THE EUROPEAN UNION: TECHNOLOGY NARRATIVES AND REGULATION BEYOND THE WORLD WIDE WEB

TOWARDS A POST-SOVEREIGN DIGITAL (SECURITY) REGIME

Nicklas Lønborg Andersen

International Relations

Aalborg University

TABLE OF CONTENTS

ABSTRACT

This thesis investigates the European Union's (EU) evolving approach to digital sovereignty as a component of its broader strategic autonomy agenda in the context of global digital governance. With rising concerns over external dependencies on the United States (US) and the People's Republic of China (PRC), the EU has increasingly sought to position itself as a normative power, promoting values-based regulation and autonomy in the digital sphere. Drawing from constructivist epistemology, the study examines how the EU's digital sovereignty narrative impacts member state (MS) alignment, considering the interplay of governance challenges, Europeanisation of identity, and technological capacity asymmetries.

Through a comparative analysis of Germany, Hungary, and Sweden, three EU MSs with differing technological baselines and political identities, the study explores the extent of norm diffusion and regime compliance under strategic initiatives such as Gaia-X, the 5G Security Toolbox, and edge computing. Employing Normative Power Europe and regime theory as theoretical frameworks, it argues that the EU's success in achieving a coherent digital sovereignty strategy depends on more than formal compliance; it requires the internalisation of shared norms and collective identity across its members.

Findings reveal substantial variation in national implementation strategies, reflecting disparities in digital infrastructure, ideological commitment, and geopolitical alignments. While the EU seeks to transcend Westphalian models through a post-sovereign security regime, practical implementation is challenged by fragmented governance and uneven MS commitment. This thesis contributes to an understanding of the EU's identity construction in digital governance and its viability as a global actor in a geopolitically-contested digital order.

INTRODUCTION

Non-European cloud providers currently host the majority of European Union (EU) data a situation with significant economic and political implications for the Union (Pannier, 2021). In response, the EU has advanced its framework for (open) strategic autonomy, aimed at reducing its dependency on external actors such as the United States (US) and the People's Republic of China (PRC), whose influence extends deeply into European supply chains, digital infrastructure, and critical societal functions.

This idea of open strategic autonomy has emerged from the self-described "geopolitical" European Commission (EC), a term used to capture the Commission's transformation since 2019, marked by a renewed ambition to promote the EU's global role and uphold values such as freedom, democracy, and a rules-based international order (European Commission, 2024a).

A central pillar of this strategic autonomy is digital sovereignty, which refers to the EU's effort to assert control over its own data and digital infrastructure within the normative framework of its post-sovereign institutional reality. However, tensions have emerged between this narrative of self-reliance and regulatory leadership and the fragmented reality of governance, where implementation is shared and contested among supranational institutions, member states (MS), private actors, and other stakeholders

This raises critical questions about the coherence and effectiveness of the EU's digital strategy, particularly its ability to function cohesively across diverse political and technical environments. This study investigates **how the EU's digital sovereignty narrative shapes member state preferences and alignment with the broader EU digital regime**, where digital sovereignty is a key pillar. To answer this question, the analysis is structured around three interrelated dimensions:

1. Governance complexity: How the post-sovereign governance structures impact the implementation of digital policy.
2. Europeanisation and identity: The extent to which EU-level norms shape national digital policies and identities.
3. Capacity and asymmetry: How disparities in technological development affect collective action within EU initiatives.

This study specifically focuses on how digital sovereignty is narrated, institutionalised, and operationalised across different levels of the EU governance system. It examines key policy frameworks such as the 5G Action Plan, 5G Security Toolbox, and Gaia-X, all of which are flagship initiatives that aim to strengthen EU control over digital infrastructure and data flows. Furthermore, the lack of proper standardisation regarding the future evolution of the digital sovereignty paradigm will be assessed through edge computing policies, and the clash between EU policies and MS policies in regard to this field. The Digital Services Act (DSA) and the Digital Markets Act (DMA) will be slightly touched upon, as a means to understand the power of the EC, and when the different structures of the EU, and the strengths of when it stays less fragmented as opposed to the more post-sovereign approach of the greater digital sovereignty strategy.

To explore norm diffusion and implementation dynamics, the thesis conducts comparative case studies of three EU member states: Germany, Hungary, and Sweden. These countries were selected due to their contrasting relationships with EU governance and digital policy. Germany is a co-leader in the development of Gaia-X and has significant industrial weight within the Union. Hungary, in contrast, presents a critical case due to its increasing political divergence from EU norms and its close ties to Chinese digital and non-digital infrastructure. Sweden represents a middle ground, ideologically aligned with many EU principles, but with a strong legacy of independent digital policy and open data practices that predate the current EU framework.

Through these case studies, the research reveals how national preferences, technological capabilities, and political ideologies shape the degree of alignment with the EU's digital regime. Particular attention is paid to implementation asymmetries, regulatory compliance, and narrative buy-in, which are all key indicators of vertical Europeanisation. The analysis also evaluates how digital sovereignty is framed by national elites and how these discourses interact with the broader EU vision of a human-centric, rules-based digital order.

Methodologically, the thesis follows a constructivist epistemology, treating digital sovereignty not just as a technical policy problem, but as a social and political narrative. The study uses Normative Power Europe (Manners 2002), Norm Diffusion (Finnemore & Sikkink, 1998; Risse & Sikkink, 1999; Börzel & Risse, 2014) and Regime Theory (Keohane 1984; Krasner, 1993; Keohane & Nye, 2012; Keohane, 2018) to analyse the EU's strategy as both an expression of identity and a form of structured cooperation. Key concepts include norm diffusion, strategic socialisation, and the interplay between supranational

and intergovernmental mechanisms. Empirical material includes EU regulations, national policy documents, stakeholder reports, and public opinion data (e.g., Eurobarometer). These sources are triangulated to assess how digital sovereignty is interpreted and enacted across different governance levels.

In doing so, the thesis contributes to broader debates on European integration, sovereignty in the digital age, and the geopolitics of information technology. It also offers a critical reflection on the EU's ability to act as a coherent global player in the digital domain and to project its normative values outward, amid growing international competition and technological dependencies. Ultimately, the study argues that the EU's digital sovereignty strategy will only succeed if it becomes more than a regulatory agenda, it must be internalised as a shared political identity across member states. Without deeper alignment the asymmetries and fragmentation will continue to undermine the EU's ability to define and defend its digital future.

LITERATURE REVIEW

THE DECLINE OF THE UNITED STATES OF AMERICA'S INFLUENCE

As Fouskas and Gökay (2019) have established, there is currently a rise in what they categorise *new authoritarianism*, something which is inherently different compared to the traditional Western regimes, especially the European regime. This new authoritarianism is rooted in the decline of the Euro-Atlantic core, which occurred during two stages. First, the erosion of the American economic power due to pressure from (West) Germany and Japan, and secondly, during the rise of the PRC and India that became visible from at least the 1990s onwards (p. 38). In the case of Europe, the new authoritarianism can be classified as a form of *ordoliberalism*, primarily spearheaded by German economic history. Ordoliberalism is a form of public policy which is inspired by liberal, free market economic principles, which is operationalised through institutional authority (Fouskas & Gökay, 2019, p. 34). These free market economic principles have however started limiting external monopolies and subsidising European companies, as a means to strengthen the autonomy of European supply chains. Stemming out of a rejection of both free-market liberalism, which is considered too unregulated, and central planning, which is seen as too controlling, the EU has started to favour European companies disguised as a geopolitical means for achieving autonomy in supply chains.

During Donald Trump's first term as President, Washington's *America First* approach was seemingly inspired by Beijing's *Made in China 2025* policy (Hoffmeister,

2023, p. 669). These contemporary protectionist policies mirror a political tendency which occurred in the greater economic regime prior to the establishment and transition to the World Trade Organisation (WTO), when The General Agreement on Tariffs and Trade (GATT) was the treaty that governed the international trade regime. However, the GATT saw a rapid decline in its efficiency, as illegal trade restrictions grew towards its later cycle (Keohane, 1984, p. 185), even though it aimed to restrict unilateral protectionism (Keohane & Nye, 2012, p. 288). It is important to note, that it was argued that the US was the frontrunner, when it came to these economic regimes, and when they are failing, so is the American influence. It is however, also important to note that almost 70% of all trade liberalisation since the 1980s have been unilateral (Wandel, 2019, p. 198), it is more correct to assume it is the European culture and values that are the outlier, when it comes to the multilateralist nature of the region.

As for contemporary Euro-Atlantic relations, there has been a concern regarding the American commitment to collective defence, especially considering that the US has pivoted towards Asia. This has resulted in among others, the establishment of the European Common Security and Defence Policy (CSDP), which in return has been a concern for the Americans, as they fear it could divide transatlantic partnership as it takes away resources from their military cooperation (Arbatova, 2015). Further division occurred after the establishment of the CSDP, as the Bush administrations unilateralism combined with the economic and financial crisis of the 2000s furtherly divided the US and the EU. This decline in multilateralism was also evident during Donald Trump's first term as President, even though negotiations prior to that, such as the Transatlantic Trade and Investment Partnership, suggested deepening integration between the US and the EU (Welfens, 2020). One of the key examples of the decline in the US' influence, specifically in the realm of digitalisation, can be seen through the American data collection through the National Security Agency (NSA). The revelations of the US' vast surveillance operations sent shockwaves through Europe, stirring deep concerns over American espionage activities regarding both European leaders and citizens (Zhang, 2024, p. 249).

The polarisation of the American President Donald Trump reaches beyond the American political realm. American relations and the *America First* narrative has encouraged a distrust of any international commitment to treaties, cooperation, and alliances. Donald Trump has resurrected a hypothesis shared by ta part of the American conservative spectrum that states that involvement in the world can be a danger

(Guilbaud, Petiteville, & Ramel, 2023, p. 116). Furthermore, it can be argued that a new Cold War prevails, which will inherently challenge the US' commitment to multilateralism and free trade, in turn weakening their relations with what has traditionally been regarded as their allies. International institutions will be seen as forums for political competition and struggles for influence, rather than as places of consensus and global governance, if the "second" Cold War continues down its current spiral. This can result for the end of global multilateralism as we used to understand it since the beginning of the 1990s (Guilbaud et al., 2023, p. 125).

American influence on European strategic autonomy can be seen through the rhetoric that states the EU wants to remain "as open as possible, but as autonomous as necessary" (Schmitz & Seidl, 2023, p. 835), as it mirrors the US' political stance mirrors the spirit in the Madeleine Albright era, when she was Bill Clinton's Secretary of State where the goal was to be "multilateral when possible, unilateral when necessary" (Guilbaud et al., 2023, p 128).

THE PEOPLE'S REPUBLIC OF CHINA AND THEIR EMERGING INFLUENCE

The rise of the PRC has generally undercut the claims of unipolar stability. It is argued that the PRC is the most tangible evidence of the erosion of the US' influence and power. This is evident through the general questioning towards the American economic status and the doubts connected to the dollar's long-term hold on reserve currency status (Manners, 2002; Layne, 2012). Initiatives such as the Belt and Road Initiative (BRI), BRICS (including BRICS+, an expansion of BRICS to become a global platform to foster the group's external relations as a united association), and the Asian Infrastructure Investment Bank, regarded as a complimentary institution to the World Bank and International Monetary Fund (IMF). The PRC's global infrastructure spree has attracted widespread international attention, particularly among the liberal democracies concerned about the PRC's growing economic power, as well as in developing countries that host projects financed by Beijing (Strange, 2023).

The Chinese infrastructure initiatives is considered to undermine the model of the Western Hemisphere when it comes to development aid, governance, human rights, and environmental protection. Generally speaking, the PRC offers a new approach to the international dynamic, which differs immensely from the Western, and specifically the European model, which is bound on morals and correctness. The PRC instead offers nations under development an alternative to the conditionally-rooted aid of the West, for

the first time since the ending of the Cold War (Tan-Mullins, Mohan, & Power, 2010). This alternative is deeply rooted in loans, particularly concessional loans, which work as a key instrument for securing Chinese access to needed resources and providing credit for infrastructure development built by Chinese construction firms (Alden & Lu, 2019, p. 642). While the rhetoric of the PRC is deeply connected to non-intervention, as opposed to the more traditional powers, bottlenecks do occur for the emerging power. An example of this is the Chinese lease of the Hambantota Port in Sri Lanka, as a result of the Sri Lankan government defaulting on their loan (Carrai, 2019). Even though there are definite criticism towards the Chinese development programmes, some of which mirror the criticism that the Western hemisphere has received for their programmes in the 1970s, there is no doubt that the influence of the PRC is ever rising. The PRC has become the largest bilateral provider of development finance in the Global South (Strange, 2023, p. 1), and they would not have reached this status, if the receiving end would have been opposed to the financial aid they are receiving. The BRI is, as characterised by the PRC, within well-defined economic lines as the PRC strives to position itself as a major trade partner while laying greater stress on maintaining global free trade and communication against the rising tide of protectionism (Yilmaz & Liu, 2018, p. 265).

The stems of Chinese multilateralism have seen an interesting development in international relations. On the one hand, they are rejecting some multilateral institutions such as the International Court of Justice (ICJ), while interacting an actively trying to reshape others such as the UN and the WTO (Guilbaud et al., 2023, p. 133). The Chinese identity is carefully constructed through the liberal international order, specifically through the organisations which the PRC have chosen to partake in. Its commitment to the UN has resulted in international leverage, and the alignment with the WTO has secured material benefits. However, their refusal to join the ICJ does not weaken their position in their rivalry with the US, who is not a part of the ICJ either.

Another example of where the PRC is growing in influence is in day-to-day information technology. Applications such as WeChat and TikTok have seen immense rises in popularity outside of the PRC. This has resulted in American attempts at outright banning these two applications from digital stores throughout the US. Some of the American concerns regarding these applications mirrors the European concerns regarding both American and Chinese applications, primarily their data collection approaches, which is deemed to be able to sway election, create risk to privacy, and national security (Zhang, 2024, p. 249).

In relation to narratives, it is important to understand how political mobilisation can be accelerated through the international narratives that are constructed when it comes to the deployment of Chinese infrastructure. Deviations from the PRC's state goals as well as accidental or purposeful information failures about different Chinese actors can further fuel problematic narratives about Chinese global infrastructure (Strange, 2023, p. 69). While on the surface, it does not appear to be the strategy that the EU is actively seeking, their constructed narrative certainly has to do with discrediting, or at least questioning, the motives behind the infrastructure spree, especially when it comes to key digital infrastructure, which is deployed worldwide, and which the EU is dependent on. This is also evident through the sentiment that European states anticipate positive economic and political outcomes in relation to being more interlinked with the BRI, through the European neighbourhood of Central Asia after EU expansions in 2004, 2007, and 2013 (Yilmaz & Liu, 2018, p. 259). These positive anticipations are however primarily focused on opportunities in energy and trade with the PRC and does not solely relate to the digital strategy of the EU.

WHAT EMBODIES THE EUROPEAN UNION?

Historically, the European regime, and the EU, stemmed out of the culture of post war West Europe. Western Europe were closely intertwined with the US, in what is commonly regarded as the Euro-Atlantic space. The US helped post war Europe with funds for rebuilding and supported the (re)emergence of democracies within the continent. This American support came due to multiple reasons that aligned with the self-interest of the US. The first of these is connected to the military power of the US, especially their concern over the emerging new power, the USSR. Secondly, and also tied to the USSR, the US wanted post war Europe to steer towards democracy, as evident through the establishment of the League of Nations. A lot of the pillars of the EU is built through American soft power, which is the ability to get desired outcomes because others want what you want. Being able to achieve desired outcomes through attraction rather than coercion (Keohane & Nye, 2012, p. 216). This has also been a key aspect of the EU's power, as it is not a regime that excels through its hard power but is ideologically driven to promote common sensical attraction as opposed to coercion. In the cases where the EU has had to make use of its hard power, an occurrence which has happened more frequently since its formal conception in 1993 as opposed to its prior arrangement as the European Economic Community, it has been in internal matters, where sanctions

have been opposed upon member states such as Poland and Hungary in relation to democratic deficit (e.g., Blauberger & Sedelmeier, 2024; Harris, 2019).

The EU has outlined its internal aims to: Promote peace, its values and the well-being of its citizens. Offer freedom, security, and justice without internal borders, while also taking appropriate measures as its external borders to regulate asylum and immigration and prevent and combat crime. Establish and maintain an internal market. Achieve sustainable development based on balanced economic growth and social progress. Protect and improve the quality of the environment, promote scientific and technological progress. Combat social exclusion and discrimination. Promote social justice and protection, enhance economic, social and territorial cohesion and solidarity among EU countries. The EU external aims are upholding and promoting its values and interests, contributing to peace and security and the sustainable development of the Earth, contributing to solidarity and mutual respect among peoples, free and fair trade, eradication of poverty and the protection of human rights, as well as strictly observing international law. These values that the EU strives to uphold is: Human dignity, freedom, democracy, equality, rule of law, and human rights (European Union, 2007).

Europe has also long regarded consumer privacy and data protection as fundamental human rights, something that is rooted in the European historical, cultural, and legal contexts. Primarily concerning the region's experiences with totalitarian regimes, invasions of privacy, and human rights abuses. These experiences have shaped Europe's collective consciousness and its interpretation of personal data protection as a crucial human right (Zhang, 2024), something which is in stark contrast to both the US and the PRC. With this misalignment between the EU and the two global powers, the emergence of a pro-European, more independent, approach has occurred. External challenges such as the PRC's economic imperialism and the US' increasingly protectionist call have resulted in the EU advocating for the establishment of a European sovereignty fund, pooling fiscal resources at the supranational level to conduct a full-fledged EU industrial policy (Di Carlo & Schmitz, 2023, p. 2087). This commitment to sovereignty and strategic autonomy is generally argued to be a result of the disintegration of Euro-Atlanticism and the emergence of new authoritarianism, as the current world order is under heavy scrutiny (Fouskas & Gökay, 2019). The Euro-Atlantic partnership was based on the European commitment to both democratic politics and membership in the capitalist world economic system, including the Bretton Woods system, and through this commitment they had to reach accommodations with the US, as these

issues relied on the US for military protection (Keohane, 1984, p. 182). However, with the call to arms within the EU, following the lack of multilateral alignment between the US and the EU (especially on cases such as NATO), it is clear, that this reliance on American military protection has diminished. Another interesting development, which has occurred within the military sphere, is that the Russian invasion of Ukraine has increased the vertical Europeanisation of political discourse in the EU. This change since the invasion of Ukraine is in general part of the bigger narrative constructed by the EU, connected to the idea of the European public sphere. While nations do show this development to a varied degree, it is generally considered that there is a new emergence in political debate in the bloc, reshaping the public opinion, potentially leading to more centralised defence and security policies at the EU level (Sojka, Terraza, Crespo, & Rumín, 2025). This spillover coincidently perfectly aligns with the EU's strategic autonomy approach.

THE GEOPOLITICAL CONNECTION TO STRATEGIC AUTONOMY

A lot of the current standing trade war (especially between the PRC and the US), has resulted in a highly geopoliticised global trade. A resurgence of protectionism in trade has been accompanied by a zero-sum game mindset, which is heavily connected to the popular political trade deficit analysis (Nagy, 2019). There are over 150 members of the WTO, an evolution from the GATT, which is a trade regime, with the purpose of limiting protectionism through formalised norms. However, as evident through the contemporary political environment, these norms which the WTO promotes are being challenged heavily (BBC, 2025; Deutsche Welle, 2025). However, this competition between the PRC and the US is nothing new and is characterised by the US attempting to maintain its dominant global position by taking measures to counter, balance, or contain the PRC (Hlover & Mawuko-Yevugah, 2024). Even though this is the case, the Sino-American relations are not the only important international relations, as evident through Sino-European relations. In 2015 the PRC announced a ten-year plan, the "Made in China 2025" policy, which aims at the transforming the country from low skilled manufacturing to high-technology manufacturing. This includes electric vehicles, aerospace, engineering, information technology, telecommunications, along with other advanced technologies (Hlover & Mawuko-Yevugah, 2024, p. 597). This policy can be regarded as an action that directly challenge the US dominance in global trade. In 2015, coinciding with the *Made in China* 2025 policy, the EU and the PRC signed a key

partnership on 5G, suggesting that the EU acts in an open manner in its external relations, whether it is its relations with either the US or the PRC (European Commission, 2015). This does not necessarily mean the European partnership has drifted away from the transatlantic relations, but it is more so an instance of what the EU categorises as "open" strategic autonomy, being able to balance its dependencies on both of the hemispheres.

It is also argued that neoliberalism has been challenged by politicisation of trade and geopolitisation, this contestation of the order within the EU is evident through their shift in policies as argued by Schmitz and Seidl (2023) who have traced a push towards implementation of neo-mercantilist policies, suggesting a break with the otherwise embedded neoliberal compromise of the EU. This is also supported by Fouskas and Gökay (2019, p. 16) and their argument that the frenzy of neoliberal financialisaton and its collapse during the 2007-2008 financial and banking crisis brought Western markets to their knees and thus have supported a transition from the Euro-Atlantic core to Asian economies, especially the PRC and India.

This is also supported by the EC in its external relations. On the one hand, the Commission works on revitalising EU-US relations in the aftermath of COVID-19, with the goals of strengthening transatlantic cooperation, jointly shaping the rules and standards on emerging technologies, connectivity, and digital infrastructure, and making progress towards greener and fairer trade. However, this seems to have declined since President Joe Biden's term. On the other hand, the Sino-EU relations are focused on reducing the economic overdependence on a single country, working on more sustainable supply chains, and boosting the competitiveness and productivity of EU industries (European Commission, 2024a). Even though the EU communication suggests a healthy transatlantic relation, the policies which it produces present a different story. The DSA and the DMA both primarily concern information technology, with the DSA addressing issues of illegal content and disinformation distributed on digital platforms and the DMA tackling the lack of competition in "core digital platform markets" – with the aim to strengthen the EU tech industry. Both of these acts are primarily aimed towards American MNCs, with "gatekeeper" categories being placed on MNCs such as Google, Amazon, Meta, Apple, and Microsoft (Witt, 2023, pp. 627-628).

This complex approach to both the PRC and the US is argued to be similar, even though the discourse produced around the EU external relations varies quite a lot, depending on the targeted partner. This is evident through the blurred lines between

economic and geostrategic goals on the one hand and the normative narrative of free trade on the other. The EU has constructed digital policies, which aim to strengthen its own industries, while simultaneously weakening the American influence in cloud computing, as evident through the EU's Gaia-X initiative, and the Chinese influence in 5G technologies, evident through the 5G Toolbox. Broeders, Cristiano and Kaminska (2023) argue for three developments in EU policy-making that point to a geopolitisation of EU digital policies. "Firstly, the instrumental use of 'classic' internal market policies, such as trade and competition policy, to exert geopolitical influence; secondly, policies that aim to impose foreign policy 'requirements' and restrictions on national markets, such as the 5G toolbox; and thirdly, a new generation of intentionally hybrid digital policies in which internal market concerns, fundamental rights and geopolitical concerns are all present, such as the AI-Act and the DSA/DMA (p. 1269)." Furthermore, the whole political framework of strategic autonomy is considered to be of geopolitical nature, as evident through its ability to connect economic (and social) concerns with geopolitical ones (Schmitz & Seidl, 2023, p. 849), but also the general blur of the boundary between foreign policy and trade policy (Jacobs, Gheyle, de Ville, & Orbie, 2023, p. 16). Overall, the EU finds itself needing to distance itself from questionable policies that occur both within the US and the PRC, which do not align with the EU principles and values. This disconnect presents opportunities for crises, in which European dependencies is at stake.

Following this, the EU has generally changed its position within the cybersecurity field from being aligned with *regulatory capitalism*, where the private sector holds a privileged coregulatory position, to a *regulatory mercantilist* position in which the EC positions the private sector as something to be overseen and controlled (Farrand & Carrapico, 2022, p. 436). Given this development, and the general European conception of what cybersecurity concerns speaks for itself as the EU seeing itself as becoming a geostrategic power, especially in relation to cybersecurity. This is also highly connected to the Commission President's comments regarding her Commission as a *Geopolitical Commission*. There is a general tendency to accept the idea that the EU needs to construct itself as a geostrategic power in relation to the intensification of global power competition. It is argued that functional spillover between economic power and strategic objectives is at the root of this, especially related to the perceived loss of economic competitiveness for the EU (Farrand & Carrapico, 2022; Haroche, 2023).

METHODOLOGY

This study is a part of the constructivist epistemology, which is evident through the belief that we acquire knowledge through experiences. The research question regarding the EU's narrative regarding digital sovereignty emphasises the role of ideas, norms, and social interactions in shaping political reality. Firstly, the ideas of the EU are a construction, from the elite-driven powers of each institution – more specifically the EC in this case. Secondly, the digital governance norms which the EU are attempting to diffuse throughout their digital strategy distinguishes what is considered 'European' and what is not. Lastly, the ideas and norms have evolved through what I, along with other scholars, consider to be the disintegration of Euro-Atlanticism. As the relationship between the US and the EU has diminished, so has the shared beliefs, and thus a need for new ideas and norms have emerged within the EU. Digital Sovereignty is not solely a policy, but it is a normative narrative framing tech autonomy as part of the (future) European identity. This is also evident through how each of the other actors engage within the ideas of digital governance. The US frames it as a market competition and the PRC frames it as national security. Through the vision of the EU, digital sovereignty is considered more than laws, it is a battle to reclaim the digital identity of its MS. However, this does not explain while some MS embrace EU tech norms, while others resist, therefore the constructivist approach is strong in unveiling MS commitment to the EU, and whether they are willing to "buy into" the emerging European identity and norms regarding data governance, despite the commitments which the regime is making.

With the top-down approach within this study, it is a given that vertical Europeanisation is a key component of the operationalisation of the research question. Through case studies, the implementation of the European norms constructed through the digital strategy will be assessed in three EU MSs. These three MSs will be used to operationalise and simultaneously triangulate the reshaping of the European identity in relation to digital sovereignty. The three MSs are Germany, Hungary, and Sweden. These three nations have been carefully chosen due to their different characteristics within the EU, and especially due to their preconceived identities. Granted, vertical Europeanisation is traditionally considered to be a policy diffusion mechanic, yet it is also important to understand the different levels of commitment to the EU based on a national identity basis – so it is more so considered as the process in which EU level norms are adopted, resisted, or adapted by the MSs within this study. Some MSs are keener on transferring their independence from the US or the PRC to the EU than others.

European integration is not equal throughout the union, which is also a factor for including Hungary as one of the examples of vertical Europeanisation. Vertical Europeanisation is not solely about legal compliance however, it is also about socialisation and the internalisation of EU norms through practices among other mechanics which are not explored in this study.

Germany is considered one of the leaders of the EU, as well as the MS with the largest economy. This comes a certain responsibility, which is also evident through the fact that they are the co-founder (along with France) of Gaia-X. Hungary has been chosen due to their tumultuous past regarding assimilating with general EU principles and values as well as their democratic deficit. Finally, Sweden has been chosen due to their open-data tradition, a value and data governance ideology that predates the establishment of a common European digital strategy. With this shift, the interdependence of the MSs transfers from either the US or the PRC in a given policy field, over to a reliance and interdependence on each other. This dynamic aligns with regime theory, which emphasises the importance of sustained cooperation and shared rules in shaping state behaviour Even though the EU MSs have agreed to instrumental compliance, it is not always the case, and for the EU to assert itself as a geopolitical power, in any given field, this compliance should be more than a simple case of instrumental compliance, but a genuine shift in identity for the MS. If the EU is not able to achieve a common digital governance and security approach within the Union, it is hard to imagine, that third parties would ever subscribe to the narrative that the EU is a global player. The EU is trying to differentiate its narrative from the US, which is market driven, and the PRC, which is state-controlled. Therefore, the constructed narrative of the EU must be different as opposed to the two great powers.

Within this approach to vertical Europeanisation, socialisation plays a huge role in norm diffusion. Therefore, Checkel (2007) will heavily compliment the work of Finnemore and Sikkink (1998) while combining these normative aspects with Keohane's (1984; & Nye, 2012; 2018) plentiful works on regimes and interdependencies, and the ideas of when policies harmonise and when they find themselves in conflict. There is a preposition embedded in the whole concept of strategic autonomy, which presupposes that interdependence between MSs is better than the dependence on either American or Chinese information technology, which is heavily aligned with the ideas of regime theory. Normative power Europe (NPE) and regime theory will be paired in order to analyse the projection of values-based geopolitical identity. Through the establishment

of a global digital regime, the EU reinforces its role as a normative and institutional power, shaping its geopolitical position. The regime construction of the EU emphasises its role as a rule-maker rather than a traditional military or economic power.

The current interpolar world order has provided the EU with reason for establishing the EU Global Security Strategy (EUGS) in June of 2016. Along with the EUGS, there has been a prevalent input from France and Germany in relation to further military integration for the two nations (Deschaux-Dutard, 2022, pp. 593-594), providing a bilateral cooperation within the already multilateral framework of the EU and NATO. This falls under the normative dimensions surrounding European strategic autonomy and technological sovereignty – as it favours certain views of security and technological progress over potentially silencing others. These initiatives govern the EU future trajectories regarding defence policy and technological innovation (Csernatoni, 2022). This notion is also supported by Monsees and Lambach (2022) who have made significant research on the geopolitical imaginaries of the EU. Security comes in many forms, and they have considered aspects of digital security in a highly digitalised world, where both American and Chinese tech companies such a s Google, Apple, Amazon, Intel and their Chinese counterparts, Alibaba, Tencent, Huawei, etc. pose many threats towards the European normative identity. Aspects which these technological companies concern include privacy, data protection, media freedom, and democratic stability (Monsees & Lambach, 2022, p. 379).

The empirical data sets are a combination of EU legal instruments and policy documents, MS-level strategies, legislation, and official communications, public opinion data gathered through Eurobarometer, stakeholder reports , and secondary academic sources. Operationalisation of the data sets will occur through the measurements of governance challenges, which are accessed through the tensions between supranational regulation and national implementation, Europeanisation and identity, operationalised by the degrees of vertical norm diffusion and internalisation, and disparities in digital infrastructure and political will, which will allow for analysing the differing capacities and asymmetries of the MSs.

This study focuses on formal policy instruments and elite-level discourse, with limited access to behind-the-scenes negotiation processes or micro-level stakeholder perspectives. Furthermore, while constructivism offers powerful tools for unpacking normative and identity dynamics, it does not account for material or economic interests

in the same depth as rationalist approaches — though regime theory partially offsets this.

THEORETICAL FRAMEWORK

NORMATIVE POWER EUROPE AND NORM DIFFUSION

In 2002, Ian Manners introduced the concept of the EU as a *normative power*, as opposed to it being either a *civilian* or a *military* power. This idea of the EU as a normative power stood in contrast to the general idea that the power of Europe was "long on economic power and relatively short on armed force" (Manners, 2002, p. 236). This is rooted in a general understanding that military power or economic power is a bipolarity, which Manners challenges through refocusing away from this debate, and instead focuses on the ideational impact of the EU's identity and role as representing normative power. With this new added normative power to the equation, suddenly a bipolarity became an option of three instead.

The systematic preference of the EU presupposes that Westphalian sovereignty and norms is not a given. This ability to shape the conceptions of what is normal is where the power of the EU lies. Realists might argue that the diffusion of the EU is not dissimilar to the norm diffusion which historical empires and contemporary global powers exercise. On the other hand, liberalists may argue that the role of norm diffusion rests on the hands of the institution, which is the general position this study will take. EU's normative power comes from its historical context, hybrid policy and political-legal constitution. The EU was created in post-war Europe and the highly nationalistic political environment which preceded WWII. Therefore, the initial institutions, which evolved into the EU, were committed to pooling their resources together, an approach which promoted peace and liberty. This position has accelerated a commitment to placing universal norms and principles at the centre of its relations with its member states (Manners, 2002, p. 241). An evolution which challenges the Westphalian ideas and establishes a position of post-sovereignty within the continent. Since then, the EU has evolved into this hybrid of supranationality and intergovernmental forms of governance.

Cyberspace and digitalisation in general offer an interesting battleground for this post-sovereign EU approach and the Westphalian model of the US and the PRC. With Westphalian principles being rooted in territoriality sovereignty and the absolutely that accompanies it. With the lack of an actual territoriality of the cyberspace, this clash of

interference and non-interference is evident, especially through the EU's regulative and constitutive norm diffusion regarding the policy conflict. Granted, the EU is not the first to govern the cyberspace and execute its sovereignty in this realm but are the first to push for diffusion of norms and ideas which they establish. The US and its infamous NSA is a clear example of digital governance, where diffusion is not accompanied with the governance, especially considering the subsequent legislation of the USA Freedom Act, which limited the NSA's power (Greenwald, 2014). An example from the PRC, which is different in nature to the American approach, is the establishment of the *Great Firewall of China*, which allowed for the PRC to build and control an alternative version of the internet (Griffiths, 2021). These two examples can be more-so considered as the rights of the US and the PRC seen from their perspectives, whereas the EU wants to establish and diffuse a conception of normal. This different approach to governance also rests on the shoulders of the EU as an at least perceived normative power, whereas the military and economic powerhouses of the US and the PRC are more concerned with upholding the status quo and their Westphalian norms, than establishing new ones that may limit their powers in cyberspace.

The position of the EU is evident through its core principle guidance of "spreading good governance, supporting social and political reform, dealing with corruption and abuse of power, establishing the rule of law", which are principles that has the EU self-realising as having the *correct* ideology when it comes to its external relations (Whitman, 2011, p. 2). This assumption that the EU carries, along with its post-sovereign qualities, allows for norm diffusion to occur in a unique way within the institution. The constitution of the EU as a political entity that is a largely elite-driven, treaty based, legal order allows for norm diffusion to occur unevenly in a vertical favour due to the EU embodying actor qualities (Manners, 2002, pp. 240-241). This idea, coupled with Finnemore and Sikkink's (1998) theorisation of norm diffusion allows for a unique approach to the EU. When it comes to the EU, the discussion surrounding norms can be flipped over. Whereas it is argued that domestic norms are deeply entwined with international norms, and that many international norms begin as domestic norms and evolve through their cycles (Finnemore & Sikkink, 1998, p. 893), this is not necessarily true, especially considering the concept of NPE. The EU, has through its strong post-sovereign and hybrid polity characteristics, managed to establish itself as both a sole actor, but also as a network of its MSs. This is even evident through the EU's self-identity, specifically through discourse surrounding itself, where it often is the phrase: *The European Union and its*

Member States that is highlighted in regulations, legislations, and other formal positions (European Parliament, 2011; European Union External Action, 2023). This also ties in with the aforementioned notion of the EU as a more multilateral actor/organisation. Even though Finnemore and Sikkink's approach to the interplay between domestic norms and international norms does not translate that well to the EU their *norm life cycle* offers an interesting power dynamic for the EU, especially coupled with this idea of the EU as a normative power.

The following table represents the stages of norms (Finnemore & Sikkink, 1998, p. 898), and after the table, an explanation for these different dynamics in a European context will be provided:

	Norm emergence	Norm cascade	Internalisation
Actors	Norm entrepreneurs with organisational platforms	States, international organisations, networks	Law, professions, bureaucracy
Motives	Altruism, empathy, ideational commitment	Legitimacy, reputation, esteem	Conformity
Dominant mechanisms	Persuasion (coercion)	Socialisation, institutionalisation, demonstration	Habit, institutionalisation

Dissecting the table row-to-row offers the best approach to coupling the norm life cycle with the power of the EU, however a column-to-column dissection would also allow for an approach more focused on norms and their different characteristics and evolutions. The EU's power lies primarily within formalised norms, especially within the two categories of formalised norms, specifically regulative norms and constitutive norms (more on these specific norm categories will be explained later in the section). The EU is unique in its sense, that its *norm entrepreneurs* can be rooted in both the EU-elite, which have a loyalty towards the EU, but also the member states. All of these EU-elite with a shifted loyalty, however, does already have access to the organisational platform of the EU, and can thus boost their norms without larger cries for collective action within the union. However, the rest of the actors category is also embodied within the EU, so that countries begin to adopt these (formalised) norms in accordance with their commitment

to the EU, and internalisation is executed thus, as both a union/regime-level and at a state level. *Motives* for the norms are also all within the realm of the EU, as within the norm emergence stage there definitely is an overlap with the EU as a regional organisation, which has a concern for its partners as the interests of the member states are intertwined, due to the large interdependence on each other, combined with spillover effects – especially as sovereignty is pooled together in the union. This is clearly evident through the history of crisis of the union, specifically cases such as the Eurozone Crisis enlighten how states' interests are also the interest of the EU. However, on a EU-level, it is important for the legitimacy of the EU to have the formalised norms established evenly within the region, thus the internalisation of the norms play a critical role in ensuring the upholding of these ideas the norms are established from. One of the key principles for NPE is also tied together with the *dominant mechanisms* of the norm stages. The EU is able to exercise all of the mechanisms for efficient norm diffusion. However, it is important to consider whether norm diffusion occurs due to a genuine belief in the norms that the EU are pushing, or due to a regulatory pressure from the position of the EU, which would weaken their international stance.

Wendt (1999) argues "that states are actors whose behaviour is motivated by a variety of interests rooted in corporate, type, role, and collective identities (p. 223)". Related to the individualistic perception of the EU it is not hard to see certain "corporate-like" tendencies of the Union. Certain policy areas result in subsidiaries such as Gaia-X, the 5G deployment, and edge computing. The whole of EU's digital sovereignty agenda carries characteristics similar to that of corporations; however, the EU carries a certain power that extends beyond MNCs.

Granted, the power of MNCs should not be understated. The EU is able, as delved into through norm diffusion, to establish formalised norms which either constitute or regulate behaviour. While these norms are sometimes differentiated, it is important to consider the fact that norms which often constitute the identity of an actor, is often also the same which regulate their behaviour (Wendt, 1999, p. 165). This is also evident through the initiatives such as the DMA and DSA, which both constitutive the identities of the categorised (digital) gatekeepers it also regulates the behaviour of these MNCs. This is naturally also true for the establishment of European subsidiaries such as Gaia-X and similar ventures that pool together resources in the name of common goods.

The EU is able to constitute the identity of the infrastructure and simultaneously regulate its capacities, so that it aligns with the European digital governance strategies.

However, this only occurs successfully when MSs adopt and invest in it fully. Furthermore, the EU is also able to construct its own identity based on these constitutive norms, a construction which also aligns with the European ideas, further internalising the digital sovereignty agenda. These characteristics and strengths further support the idea of NPE, as it expands past a solely economic or civil institution.

As now established, the norm stages of the EU are all interlinked. While it is a very complex network of dynamics they strengthen the idea of NPE and allows for the EU to further develop itself in this grey zone between military and economic power. However, two things need to be added. *Strategic social construction* and *cognitive prior(s)*. Both align themselves with the interaction of (an)other actor(s). Strategic social construction is the term for the rational means-ends calculations which one actor makes about how to achieve their goals. One aspect of it is the utility maximisation which is tied to the changing the Others' utility function and thus provides the geopolitical context to regulations aimed at limiting American or Chinese influence. This lends itself well to rationalistic game theory which in turn is highly compatible with regime theory (Finnemore & Sikkink, 1998, p. 910). The cognitive prior is the underlying assumption of an existing normative framework, something which is interconnected with the idea of European strategic autonomy. The concept of strategic autonomy suggests a dependence on the US and the PRC; this is the cognitive prior that the EU's narrative surrounds when it comes to strategic sovereignty. These are established norms which the EU is actively trying to abandon, and to further understand this (inter)dependence, it is important to apply these understandings to the concept of the preexisting ideas. These preexisting ideas are often connected to prior choices (Acharya, 2009, pp. 21-23), which are highly connected to the international regimes which the EU have been a part of for all of its existence, dating all the way back to the European Communities and its dependence on the US.

Börzel and Risse (2014) have presented four social mechanisms that play a role when it comes to diffusion mechanisms following the direct influence model. This is important due to the compatibility between European institutional change and the direct influence model. The four categories, which Börzel and Risse have unveiled are (p. 7):

1. Coercion
2. Manipulation of Utility Calculations
3. Socialisation

4. Persuasion

The fist mechanism concerns voluntary adaption. This is typically in regard to the internal diffusion following the obligation of a MS to comply with EU law. The second mechanism concerns diffusion through manipulation, in other words, the EU provides negative and positive incentives to diffuse. The third mechanism works through normative rationality and is in regard to social expectations in a given solution. This results in a MS redefining its interests and identities, which will be interesting in the cases for Hungary and Sweden, which have different outlooks on both the EU, and data governance. Lastly, and closely related to socialisation, is the case of persuasion, which is based on communicative rationality or the logic of arguing. This will be important for the case of Germany, as they are the co-founder of initiatives such as Gaia-X and therefore have to lead the way for the digital strategy (Börzel & Risse, 2014, pp. 7-9).

One of the key aspects of the digital security regime, is the socialisation that occurs in the diffusion in relation to MS compliance with the EU identity. One specific type of socialisation that is interesting in the case of identity change is Checkel's (2007) *Type II Socialisation*. This in in contrast to *Type I Socialisation*, which concerns actor strategies and roles (p. 107). *Type II Socialisation* presupposes that preferences are shaped over time (evident through the newly emergence of a European digital strategy that aims to reposition the EU in accordance with its new understanding of the US and the PRC), that cohesive organisations are better at socialising agents than fragmented organisations, that there is an interplay between international (perhaps more regional in the case of the EU) and national socialisation, and to what degree norms differ in their openness towards socialisation, as norms are not equal. Finally, Checkel also argues that it is important to consider the influence of self-selection, selective recruitment, and utility maximisation in order to fully grasp the concept of socialisation (Checkel, 2007, p. 67).

REGIME THEORY AND THE EUROPEAN DIGITAL SECURITY REGIME

In order to assess the EU digital security regime, it is important to first establish a definition of regimes. Krasner (1993) has defined regimes as a "set of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations (p. 2)." Bradford (2007) defines regimes "as the occurrence of cooperation among States by focusing on [...]

mitigating international anarchy and overcoming various collective action problems among States (p. 1)." When these States band together, a general sense of obligation among the actors is cultivated. Through this cultivation, common-sensical expectations and behaviour patterns are established. While these definitions are generally wide-ranging, it is also important to consider the fact that regimes exist in differing forms within the domain of international relations. Some of the more commonly referred to regimes are the UN and NATO which are collective security regimes, the IBRD, the IMF, and the WTO, which all three are economic regimes. Noticeably, the EU embodies both characteristics of a regime, such as shared norms and principles, rules and decision-making processes, convergence of expectations, and issue-specific cooperation. However, it also has structures which fall outside of what a regime generally is, namely, its supranational nature, political integration, the broader scope of the EU, and its unique political identity and legitimacy which is embodied through direct elections. Nonetheless, the EU and its MSs are still part of other regimes, where effects from these regimes trickle down into the European norms and principles. Regime theory provides a useful lens for analysing certain aspects of the EU, but it cannot fully capture the EU's distinct nature (Hiavac, 2010; Leal-Arcas, 2006).

Narrowing in on the European digital security regime, it is important to understand the implications of the US-Soviet bipolarity on European integration. A key argument during this period, was that the broader European regime would decline as a result of either of these polarities collapsing, however, as evident through history, this did not happen, and it is commonly agreed upon today that institutionalised cooperation can indeed sustain in the absence of a hegemony (Keohane 1984; 2018). This study even has the understanding that the EU has elevated its position since the collapse of the USSR.

The notion of hegemony, and even absence thereof, is key in understanding the current geopoliticised world, where two new polarities are at the forefront of international relations, namely the US and the PRC. Interdependencies within the world order is not a new phenomenon, Keohane and Nye (2012) argued for an era of interdependence all the way back during the Cold War. Whether it be in the form of military interdependence or in something as common as the nationalisation of MNCs and their increasing power in the 21st century. They argued that "contemporary world politics is not a seamless web; it is a tapestry of diverse relationships (p. 4)," which aligns with the European position on sovereignty and interdependence. The balance between discord and cooperation is interlinked with the globalisation of the contemporary world

of politics. With increased interdependence and governmental intervention more possibilities for policy conflicts arise (Keohane, 1984, p. 6).

Cooperation exists within global political economy when common interests exist, and conflicts arise when these common interests are not present, or when they shift from either of the cooperating parties. The latter of the two instances of conflicts, is what is currently happening, and is the root cause for the EU to push for a digital security regime.

For the better half of the 20th century and so far within the 21st century the advanced market economy countries have held similar views in regard to proper operation of their economies (Keohane, 1984, p. 6), however, within the last decade, an erosion for this can be seen, which can be connected to the prisoner's dilemma. The prisoner's dilemma is a game theory where individual decision-makers are incentivised to choose in a way where the most optimised choice for either individual party is overlooked, as a means to gain the most mass gain for both parties involved. The idea behind the prisoner's dilemma is that a reward (R) is given in case of cooperation between actors, a benefit (T) is given in the case that one cooperates (the benefit goes to the cooperating party), while the other is receives the sucker payoff (S). In case that both parties' defect, they both receive a punishment (P). In order to translate these into numerical values, a benefit is worth the maximum of 4 available points, a reward is the second-highest yielding outcome worth 3 points, punishment is worth 2 points, and finally, sucker payoff is worth a sole point. A table to visualise the row and column's choices have been included below, where the outcome left of the comma refers to the row and the outcome right of the comma refers to the column (Hasenclever, Mayer, & Rittberger, 2004; Keohane, 1984):

	COOPERATE	DEFECT
COOPERATE	R, R	S, T
DEFECT	T, S	P, P

Applying this to international politics is important to understand the implications of the policy conflicts of the US, the EU, and the PRC. As all parties are sovereign, there are rarely cases where the three of them engage in the "game", so it is primarily a game of two actors, with roots in either Sino-American, European-American, or Sino-European relations. In isolated cases, cooperation is very unlikely, as whatever either party does,

it will always yield a higher pay-off by defecting. Therefore, established common interests have to be present, in order to achieve mutual prosperity (Hasenclever, et al., 2004, pp. 31-32). Cooperation is also seeing problems related to international uncertainty, specifically related to their partners. When states are uncertain about potential partners, which results in governments missing out opportunities of striking these mutually beneficial bargains, which is an even more common occurrence during the very much tense, geopoliticised contemporary world politics (Hasenclever, et al., 2004, p. 33). These issues are evident through both the disintegration of the Euro-Atlantic alliance and the imbalance between the traditional Western Hemisphere and the Asian emerging powers of the PRC and India. Furthermore, it is an important aspect of conceptualising the dependencies of EU MSs, and whether their dependencies are likely to be shifted from external actors to internal MSs.

The suggestion of the Prisoner's Dilemma, in relation to vertical Europeanisation, is that compliance with set commitments is reasoned through social pressure, exercised through linkages among issues. If compliance with the digital strategy does not occur, MS behaviour will be evaluated within the broader context of the European governance regime, possibly even resulting in retaliatory actions such as sanctions (Keohane, 1984, p. 103).

In relation to cooperation and the idea of *asymmetrical information* new policy conflicts may also arise. While one party may know more about a situation than their counterpart(s), a presumption that bargaining would be unfair forces the party with less information to be reluctant to make agreements with the party with more information. This is essentially based upon the belief, that awareness that others have greater knowledge than oneself allows for manipulating the relationship, or even engagement in successful deception and double-crossing, which is a barrier to agreements (Keohane, 1984, p. 93). A prime example of this in relation to European relations, is both the case of cloud computing (where the US is more informed) and the 5G network (where the PRC is more informed), instead of relying on these advanced (information) technologies from outside of the EU, the EU strives to pool together its capabilities and establish both cloud computing (Gaia-X) and autonomous 5G networks, while also researching on the future 6G networks (further security threats and dilemmas for these two initiatives will be delved deeper into). Generally speaking, there is the presumption that actors are self-interested and goal seeking when it comes to their commitment to regimes. Theories of international regimes agree on the fact that these actors are rationalist (or utilitarian).

This comes with the assumption that actors' preferences are fairly stable over time (Hasenclever, et al., 2004, p. 23).

For the EU to successfully establish its digital security regime, Woo and Verdier (2020) argue that rewards and sanctions are functionalities, that help to grow compliance within the MSs (p. 235). This is one of the bottlenecks for the EU in relation to establishing the new 'digital identity' of the EU. Is compliance occurring simply because of incentives such as funding when it comes to alignment with the EU's digital strategy, or do MSs widely adopt this new narrative and construct a new identity that compliments the call for digital sovereignty? This is at the root of including NPE to the regime theory approach. These incentives may act as benefits that will be rewarded through compliance within the digital strategy (the Prisoner's Dilemma), therefore, it is presupposed that MSs will, at least to some degree, comply with the digital strategy, as incentives and utility maximisation are strong in regulating behaviour in a way that exceeds regulatory compliance.

THE EUROPEAN NARRATIVE

DIGITAL SOVEREIGNTY REGIME: DATA GOVERNANCE AND IDENTITY

In 2020, the President of the EC, Ursula von der Leyen, stated: "Europe must have to make its own choices, based on its own values, respecting its own rules. This is what will help make tech optimists of us all", a sentiment that resonates with the overall strategic autonomy approach, which von der Leyen's Commission has made one of its key objectives during her tenure. Furthermore, she stated that "we believe that the digital transformation can power our economies and help us find European solution to global challenges. We believe citizens should be empowered to make better decisions based on insights gleaned from non-personal data" (von der Leyen, 2020). These quotes stem out of the constructed rhetoric and narrative in the backdrop of the implementation of GDPR. The European technology narrative, have since then, evolved almost as rapidly as technology itself has, at an attempt to govern and regulate the digital realm.

The EC's digital strategy has outlined a couple of principles for Europe to achieve, in order to prepare for what they have coined the "digital decade". The digital decade policy programme is a cooperation cycle, that is set to prepare the EU for the 2030s. Along with the Digital Decade Policy Programme 2023, certain general objectives have put in place, those are among others (European Union, 2022a):

- Promoting a human-centred, fundamental-rights-based, inclusive, transparent and open digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values and are accessible to all, everywhere in the Union
- Developing a comprehensive and sustainable ecosystem of interoperable digital infrastructures, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity work in convergence, to promote their uptake by businesses in the Union, and to create opportunities for growth and jobs through research, development and innovation, and ensuring that the Union has a competitive, secure and sustainable data cloud infrastructure in place, with high security and privacy standards and complying with the Union data protection rules.
- Improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity.

As evident through the selected general objectives, the narrative of the digital sovereignty regime is evidently overlapping with the already established narrative of the EU promoting human dignity, freedom, democracy, equality, rule of law, and human rights. Furthermore, the development of interoperable digital infrastructures along with the promotion of human-centred, fundamental-rights-based, inclusive, transparent and open digital environment seems to suggest, that the EU constructs a narrative, where the current system does not live up to their principles and values. Therefore, a solution needs to be developed. This solution furthermore has to be developed within the Union, this is a notion which is evident through the fact that it is a general objective to ensure the EU has a competitive, secure and sustainable data cloud infrastructure in place. The focus on the European solution being competitive, suggests that there currently is an imbalance and dependence on foreign technology, which is supported by the fact that the EU subsidises information technology initiatives, and furthermore wants to double both the current amount of EU technology unicorns and the semiconductor production. Finally, the improvement of resilience to cyberattacks hints at two aspects of the digital decade programme. First off, there is the fact, that the current dependencies on deployed technology does carry a certain risk when it comes to digital security. Secondly, it suggests there is an information gap within the citizens of the Union, and

therefore, it is valid to question the intense rollout for a digital strategy, if public and private organisations do not already possess *at least basic levels of cybersecurity*. It is safe to assume there is a discrepancy between the EU digital strategy, and the EU citizens based on this framing. Based on the Digital Economy and Society Index (DESI), the EU average of all individuals with "at least basic digital skills" is just shy of 56%. For the countries that we monitor in case of the digital strategy implementation, Sweden and Hungary both exceed this average (they are at 66.44% and 58.89% respectively), while Germany falls below the average at 52.22% of all individuals possessing at least basic digital skills (European Commission, 2024f). These findings from the DESI naturally establishes the presumption that Sweden and Hungary will be further along in the digital transition than Germany.

Tying together EU external relations with the prisoner's dilemma acts as a way to explain this development within the Union. On the one hand, with the US as a counterpart we have a dilemma primarily focused on services (or in this case cloud computing). On the other hand, we have the telecommunications dilemma, with the PRC as the counterpart. The EU has been involved with the two parties in numerous ways in relation to each dilemma. However, cooperation and defection have panned out in both cases, which we will argue to be the driving force behind the sudden change in the European digital strategy. Furthermore, the dilemmas that are bilateral between the EU and the opposing parties also trickle down to a civilian level within the EU. These cases can be evident through the fact that European businesses can take up contracts, that are free when nations such as Sweden ban Chinese technologies in their 5G telecommunications technologies. A case portraying the contrast is when a MS such as Hungary is heavily reliant on Chinese 5G technologies for running their mobile data network. Finally, an example of the prisoner's dilemma is also evident in a nation such as Germany that has approximately 50 Gaia-X hubs, ensuring private businesses alignment with the data governance strategy of the EU, in turn allowing for these businesses to store sensitive and critical EU data on their sites.

In relation to EU external relations with the US, there are numerous declarations that have the aim to coerce the US MNCs to comply with European values and principles. These declarations, among others the DMA and DSA, have often singled out specific American MNCs that yield the privatised infrastructure and influence to affect narratives. The concern over privatised infrastructure is regarded through the DMA, incorporating the categorised gatekeepers into compliance through possible sanctions through

various consequence measures (European Union, 2022b), establishing a one-sided prisoner's dilemma for the gatekeepers in relation to their operations in the EU. The possibility of affecting narratives is clearly embedded in the DSA, regarding the prevention of the *spread of disinformation* (European Union, 2022c), adding to the overall narrative regarding digital sovereignty and the influence from, and dependence on, external factors.

Looking at the Sino-EU relations and narrowing it down on the 5G technology, we see a shift from 2015 till 2025. In 2015, a joint declaration on strategic cooperation in the area of the fifth generation of mobile communication networks (hereinafter referred to as "5G Joint Declaration") was finalised. The 5G Joint Declaration strove to reach a global understanding on 5G and establish mutual cooperation in the area of 5G through facilitation of bilateral participation of enterprises in both EU and the PRC. At the time of the finalisation, the EU even referenced to the 5G Joint Declaration as a milestone agreement (European Commission, 2015). However, the subsequent European 5G toolbox of 2020 allows for more agency for each MS, and with this agency, they have been allowed to both restrict and outright ban Chinese influence in their telecommunications networks (European Commission, 2020a). A large portion of the 5G Toolbox regards the risk assessment in relation to the 5G network. This sudden shift within a mere five-year period, is a great reflection of one of Keohane's argument regarding the dynamics between two parties with asymmetrical information. With this asymmetricity, the EU portrays itself as being afraid of manipulation of the relationship, deception, and double-crossing in regard to the PRC, Huawei, and ZTE. This has been an ongoing process, and the latest development even bans lobby groups with connections to Huawei (Associated Press, 2025), as they are concerned that Huawei bribes EU lawmakers.

Each of the three MSs also have had different outcomes, based on the 5G Toolbox, in their domestic policies when it comes to the Chinese influence on domestic 5G networks. Sweden outright banned Chinese suppliers, Hungary has strengthened their bond with the PRC following plenty of investments and is fully dependent on Chinese suppliers and components for their 5G networks . Finally, Germany is undergoing the process of phasing out Chinese suppliers and components in their domestic 5G network (AboutHungary, 2023; Reuters, 2019; 2022; 2024). This is yet another case of how the European data governance regime is not solely a top-down regime, but there indeed are agency to the MS, and therefore diffusion needs to occur, in order for the digital strategy to be successful. However, the top-down regime is clearly

evident through issues regarding the DMA and DSA. Therefore, the data governance regime embodies the already established qualities of the EU with the interplay between the supranational and intergovernmental allowing for the strengthening of the post-sovereign nature of the EU.

The European narrative on the digital strategy and digital sovereignty is an intense network of different directives and regulations that highlights the interplay between the two, and the importance of digital sovereignty for the overall digital strategy. However, there are certain directives and regulations that are leaning more towards digital sovereignty than others. Based on a European Parliament briefing, the parliament has categorised the notion of digital sovereignty as the notion of European leadership in the digital field – hinting at the geopolitical nature of it. Furthermore, technological innovations such as 5G and cloud computing have become major strategic assets for the EU economy, therefore, there is more than a simple geopolitical nature to the strategy. The narrative, however, is deeply rooted in the identified *potential* dependence on foreign technology that presents a risk to Europe's influence, once again emphasising the geopolitical nature of digital sovereignty as part of the digital strategy (European Parliament, 2020).

Within regulation such as the Data Governance Act, the rhetoric, while not explicit in the sense it takes stabs at the PRC or the US, hints at the discontent with the current digital ecosystems and how there are certain visions and principles of the EU that are not fulfilled through the current dominant digital ecosystems. The European digital strategy is in stark contrast to the US Big Tech, which is evidently very market driven, as well as the Chinese state-backed services which they are heavily promoting. Each of the two opposing digital ecosystems carry their own characteristics, which both strengthen them in the international market, but to a certain degree also weaken them, as evident not only through the European treatment of the ecosystems, but also the American response to the Chinese model and vice versa. This is directly evident through the language of the Data Governance Act (European Union, 2022d):

> "It is necessary to improve the conditions for data sharing in the internal market, by creating a harmonised framework for data exchanges and laying down certain basic requirements for data governance, paying specific attention to facilitating cooperation between Member States. This Regulation should aim to develop

> further the borderless digital internal market and a human-centric, trustworthy and secure data society and economy."

The framework, which the EU refers to here, supports the broader European approach to treat data as a strategic asset, contributing to the EU's broader security regime and its expansion into the digital realm. A lot of the emphasis in this section of the Data Governance Act also paves the way for a more integrated EU, with a large focus on the agency of MSs. Another aspect which this excerpt of the Data Governance Act concerns is the importance of the European single market, hinting at the economic and material aspects of the digital security regime, hinting at the fact that it is more than solely a normative regime, but there is also an economic dimension to the broader strategy. This is also evident through the Recovery and resilience plan (RRP), which is a temporary, economic instrument, which is at the centrepiece the EU's plan to emerge stronger and more resilient from the "current crisis" as the EU phrases it (European Commission, 2024e). While the instrument gained its validity under the coronavirus, it is now largely used to build a more digital and more resilient future.

Another emphasis is the establishment of a human-centric and trustworthy process that is evident in the Data Governance Act and the emphasis of human-centred, fundamental-rights-based, inclusive, transparent and open digital environment within the Digital Decade Policy Programme lends itself to the normative sphere as opposed to the models employed by the US and the PRC. The European narrative strives to reshape and contextualise the current relations between the MSs and external partners. This builds on the socialisation aspect of norm diffusion. This is the weakest part of NPE, as MS socialisation cannot be forced aside from shaping and contextualising the EU dynamics. MSs therefore have to adopt the narrative which the EU is pushing, in order to legitimate the broader security regime that is heavily based upon the idea of a post-sovereign Europe, where sovereignty is pooled together among MSs to build this heavily value-based digital strategy. The importance of the European narrative lies within the fact that a commonsensical and common identity have to be constructed, in order for the MS compliance in the digital transformation, and invest MS resources into gaining this digital sovereignty within the Union as opposed to going with the established, dominant digital opportunities which are offered by the US and the PRC, that do not align with the framed European principles and values.

STRATEGIC INITIATIVES AND NARRATIVES SURROUNDING THEM

The digital regime that the EU is pushing for, relies heavily on regime theory mechanisms such as rules, incentives, and normative appeal. A lot of the rhetoric surrounding the digital sovereignty narratives ties a lot of directives, decisions and declarations together. One of the clearest examples of this is the connection between the DMA, DSA, and cloud computing services. In contemporary times, software, digital platforms, and infrastructure is often encompassed in service models, where they are sold as services, either directly to consumers as is the case of a lot of paid subscription services such as Spotify, Netflix, etc., or directly to businesses, Amazon Web Services for instance, and sometimes even a hybrid, as is the case for instances such as Microsoft's Office and Google's workspace services, cloud storing services such as Dropbox, as well as plentiful of other examples. One of the key principles of the DMA is to minimise both the dominance of certain services and minimise unfair practices that are accompanied in their business models. This, to some degree, transcends the efforts of the EU in the sense that the narrative is focused on both lessening the dependence on foreign information technology for both consumers within the institutional market as well as the civilian market, emphasising the economic and material aspect of the European digital security regime. The opposing goes for the DSA, naturally, an instrument which encompasses key goals for citizens, businesses, and society at large, but is important for the European values, principles and norms to thrive. Something that inherently is connected to NPE. Both of these regulations overlook MS commitment to the digital security regime, as the EC is left with the power of regulating, executing, and upholding the rules, acting as a benchmark for what EU MSs should do in their given digital transformation.

GAIA-X & CLOUD COMPUTING

One of these services that still needs to find its place in the vast digital space is Gaia-X, a service that, according to its own narrative, *empowers businesses, individuals, and governments with secure, transparent, and sovereign control over data through a decentralized cloud infrastructure. By participating, you gain access to a trusted ecosystem and the community that fosters innovation, collaboration, and scalability across industries, all while ensuring compliance with European and local regulations. Participants benefit from driving data privacy innovation, interoperability, and the ability to shape digital transformation* (Gaia-X, 2025b). Gaia-X brings together an international

industrial, academic, and political community with the aim of building a common standard for transparent, controllable, and interoperable technologies. It is *open to anyone* and aligned with the *European values* (Gaia-X, 2024d). In less abstract terms, Gaia-X provides a holistic data governance approach that is connected to European digital regulation. The

Gaia-X is a federated cloud computing service and digital ecosystem that aims to mitigate the interplay between cloud users and cloud providers in accordance with jurisdictions and domains within the EU, supported by several architectural, compliance, and trust frameworks, that aims to provide a clearer playing field for users and providers alike, as a means to help navigate within the European digital security regime, that is currently quite complex and immensely dynamic, in the sense that current development of the regime is occurring at rapid pace. Gaia-X attempts to standardise and institutionalise European data storage, that aligns itself with the European digital regime, with a streamlined way of connecting, spreading, coordinating, and consolidating European data, primarily within the EU, so that European data can remain sovereign. Gaia-X is voluntary for businesses and users to use and become part of, and thus it rests primarily on the digital sovereignty narrative, as a means to gain traction.

The notion of interoperability, hints at the importance of MS commitment to programmes such as Gaia-X. In order for interoperability occur within the Gaia-X framework, the aforementioned notion of hubs is a central piece in the interoperability puzzle. Currently, there are 19 European hubs within the Gaia-X framework, and these are also supported by 5 global ones. The European hubs are located in: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Hungary, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Switzerland (Gaia-X, 2025a). This shows general commitment to the framework, as two EEA country, in the case of Norway, and seventeen EU MSs have established Gaia-X hubs – alongside the internal commitment, the five global hubs suggest, that the normative power of the EU does also work to some extent as well, as the five global hubs based in South Korea, Japan, Texas, California, and Washington D.C. will need to adapt the European approach to data, potentially allowing for the European norms and values, in the digital realm, to diffuse into the South Korea, Japan, and the US. Furthermore, four EU MSs are currently in the progress of adapting to the Gaia-X framework, these being Czechia, Estonia, Sweden, and Ireland. In regard to global expansion Africa (more ambiguous, as Gaia-X

does not provide which African nation states they refer to) and the UK are currently preparing for adaptation of Gaia-X as well.

Gaia-X provides three key principles as to why compliance matters. These three principles align with European values, ensuring secure, transparent, and sovereign data infrastructure. The fundamentality of Gaia-X compliance is narrowed down to (Gaia-X, 2024a):

1. Openness and Transparency
2. Security and Data Protection
3. European Sovereignty

These three principles of the ecosystem ensure adherence to rules that are in line with the European values regarding digitalisation, fostering the relationship between the broader EU digital regime and businesses. In order to address the asymmetrical and uneven digital characteristics of each of the EU MSs, as well as accompanied businesses in each of the MSs, a differentiation system has been constructed through the Gaia-X framework. This labelling system allows for the differentiation of data storage ensures a universal level of security and compliance across all sectors, while simultaneously allowing for a tiered ecosystem where hosting of data is dependent on the importance, criticality, and sensitivity of the stored data, while also determining the compliance-level of the hosting service, and whether said data is safe to be stored at the provider. This tiered system adds three levels to standard compliance with the framework. The first tier is the entry-level compliance with the *European standard* of data protection and security which follows European laws. The second level concerns higher-level data protection, which also follows European laws, yet is based on certification given by the Gaia-X programme. Lastly, the third-tier concerns services requiring exceptional data handling, security, and legal control, and is exclusive to European providers. Level 2 and level 3 differentiation bears the caveat that data is processed exclusively within the EEA, and the highest-tier of differentiation even makes it impossible to access data outside of the EEA (Gaia-X, 2024b; Gaia-X, 2024c). Gaia-X's placement in the data regime, that the EU is currently pushing for, finds itself borrowing a lot of the normative rhetoric, and the belief that data protection is an essential human right in the contemporary society. The initiative is heavily linked with rules, incentives, and normative appeal as its means of attraction to users and providers alike. The Gaia-X

Trust Framework report is the most evident report, that illustrates how data providers store their data, while also highlighting the characteristics of said provider, in order for the user to get a clearer overview of their own data. This trust framework is directly linked to the aforementioned tier-system. Providers are ranked through indexes of veracity, transparency, composability and semantic-match. These rankings allow for comparisons between offerings, promoting interoperability, and furthering trust in the greater Gaia-X ecosystem, while also allowing businesses to improve their services, ensuring their offerings are competitive and trustworthy. Actors comply when the benefits outweigh the costs, and repeated interactions, specifically through the European Single Market, incentivise long-term norm adherence with the greater goals of Gaia-X. Defecting from the federated Gaia-X, may result in businesses risking exclusion from sensitive contracts, since data is not ensured to live up to the data governance politics of the EU. The project's aim is to establish a federated interoperable cloud infrastructure, positioned as Europe's response to the American tech dominance, specifically within the cloud computing sphere of information technology. In 2020, the Gaia-X association's purpose and objective was stated to consolidate and facilitate work and collaboration within a European data community, with the association striving to expand the community beyond European borders, however they did emphasise them seeking especially new members from other EU MSs (European Commission, 2020b). The setup allows for public and private organisations within MSs to establish *Gaia-X hubs* prior to the initiatives full-scale operations.

Initiatives such as Gaia-X allows for the prisoner's dilemma to become part of the digital governance strategy of the EU, where the cooperation and defection becomes a compliance concern for data providers in order to secure contracts, that will allow them to store essential, critical, and sensitive data. Through cooperation, businesses can become a greater part of the single market and gain a competitive advantage through the European subsidisation and investments in digitalisation. Through normative alignment, businesses and the EU can build stronger relations vertically, both top-down and bottom-up. A lot of Gaia-X, as well as the general European commitment to digitalisation focuses on the single market, through identification of the strengths that accompanies it. One of the key benefits of establishing the European strategy, concerns the general globalisation of not only physical goods, but definitely also the increasingly important aspects of digital goods. Through the European subsidisation of initiatives such as Gaia-X, EU is able to promote its own standards for the exchange and sovereignty of data,

through the cooperation of businesses that adopt to the Gaia-X framework, businesses that become norm cascade networks, allowing for further socialisation and construction of the digital strategy, with a greater focus on the interplay between regulators and the *regulated* businesses and civilians alike.

Gaia-X represents an attempt at consolidating the digital regime, with a focus on cloud computing. This digital regime balances the notions of sovereignty, security, and market integration. For the Gaia-X initiative to be successful, the steps need to be achieved. Firstly, there is the vertical norm diffusion that occurs internally among MSs and businesses when they adhere to EU standards. Secondly, there is the horizontal diffusion, which occurs through the global hubs in Asia, the US, and the ones that are in progress of being established in Africa and the UK. Finally, the resilience of the regime has to be withheld in order for Gaia-X and the EU to shape the global digital order, and have it aligned with EU values.

One critique of the current efforts to drive out American cloud services or at least have them comply with the European digital sovereignty narrative through initiatives such as Gaia-X. is provided by Meyers (2023). While Meyers does claim that the concerns are valid through the European lens that "foreign governments can [potentially] force cloud companies on their territory to give them access to data, that will violate EU legislation like the GDPR, impinge on Europeans' rights, and allow industrial espionage (p. 1)", he does consider the fact, that having stored your data across multiple global data centres reduces the risk of exposure to cyberattacks (Meyers, 2023, p. 3). Another critique provided by Meyers considers the fact, that limiting the European cloud computing market, through the lens of national security and privacy concerns, would give the remaining European cloud firms fewer incentives to improve their services and reduce their prices in relation to services provided by the US and the PRC (Meyers, 2023, p. 5). Furthermore, a general tendency, that can be observed through this, is the fact that it would discredit the European single market, as its strong anti-monopolistic tendencies throughout the last three decades would stand on empty ground, if an artificial limiting of non-European services would occur. Granted, as of right now, there is nothing that keeps the dominant American services away from the European market but considering the fact that it could drive them out is definitely a reasonable consideration of the European digital sovereignty narrative. Gaia-X is in direct contestation with these overseas web services such as Amazon Web Services and Microsoft Azure. While Europe is rich in digital systems, but there are no big, large, or dominant, search engine,

operating system, or other alternative stemming out of the European continent within these technologies. Therefore, it is important to consider the critique provided by Meyers. It is also important to note whether if Gaia-X can be perceived as a protectionist initiative, as that could hinder in the horizontal diffusion of EU's attempt at shaping the global digital order. This would occur due to the fact, that it would weaken EU's normative appeal, as a lot of the rhetoric is normatively-tied to a greater discourse regarding data governance.

5G ACTION PLAN FOR EUROPE, THE 5G SECURITY TOOLBOX & EUROPEAN TELECOMMUNICATIONS

In the field of telecommunications, the EU has released their 5G Action Plan for Europe, an instrument, which allows for greater control over telecommunications within each of the EU MSs. The 5G Action Plan was announced in 2016 and not all of its goals have been achieved. Furthermore, in 2020 the EU supplied the 5G rollout with the 5G Security Toolbox, which is a set of measurements to strengthen the security requirements for mobile networks and risk assessing suppliers, limiting dependency on any single vendor, and stipulate the EU's own 5G capabilities.

One of the actions that were included in the 5G Action Plan, was the preservation of 5G Global Interoperability, with a heavy focus with regards to the standards, specifically the fostering of global industry standards under EU leadership for key 5G technologies (European Commission, 2016, p. 7). Even though this predates the development of the EC to fit into the term "geopolitical Commission", it clearly shows aspects of the standardisation which the EU strives for, specifically in diffusing the regional norms and digital regime into a broader context. While the 5G Action Plan predates the digital sovereignty narrative, it is still largely connected to it and shows the interplay between digital policies prior to the establishment of (open) strategic autonomy as a pillar for European policy. The Commission said. That there is a need to *develop the backbone of digital infrastructure that will support future competitiveness* (European Commission, 2016, p. 10), which is one of the key aspects of digital sovereignty. Whether the 5G Action Plan can be directly linked to Nokia and Ericsson's relatively great market share within the EU is hard to say, but we can only imagine, that through endorsement of supporting future competitiveness of European actors, that the EU narrative of digital sovereignty stems out of a greater context of support for the European digital industries.

The addition of the 5G Security Toolbox to the telecommunications framework of the EU is a clear example of how the focus of cybersecurity has developed immensely within such a short span, which is also supported by the development of risk assessments after the 5G Joint Declaration by the PRC and EU. This context also highlights the fact, that the EU's digital policies are dynamic and constantly being reevaluated as a result of the very contested digital realm and the fact that dependencies on third parties have been a large problem within European digitalisation.

The 5G Security Toolbox is a coordinated risk assessment of 5G network security, which identifies nine main risks in five categories (European Commission, 2020a, p. 2):

RISK SCENARIOS	MAIN RISKS IN THE SCENARIO
Risk scenarios related to insufficient security measures.	• Misconfiguration of networks. • Lack of access controls.
Risk scenarios related to 5G supply chain.	• Low product quality. • Dependency on any single supplier.
Risk scenarios related to modus operandi of main threat actors.	• State interreference through supply chain. (Non-EU-states). • Organised crime exploitation.
Risk scenarios related to interdependencies between 5G networks and critical systems.	• Significant disruption of infrastructures and services. • Massive network failures based on e.g. electricity supply.
Risk scenarios related to end-user device(s).	• Exploitation of the internet of things, handsets, or smart devices.

These nine risks and the five categories outline the greater both external and internal risks. While no specific actors are mentioned within the table, it is clear that the EU suggests the PRC as the main producer of high-risk suppliers, aligning the 5G Security Toolbox with the general narrative of strategic autonomy. *The European Council called on the EU and the MSs 'to make full use of the 5G cybersecurity toolbox and to apply the relevant restrictions on high-risk suppliers for key assets* (European Commission, 2020a, p. 1). This is based on the fact that Chinese firms dominate the telecommunication

industry. This is also supported through MS actions, where there have not been any cases of foreign involvement and influence being banned within the 5G rollout outside of the cases where Chinese firms are involved. The ambiguous language of the Toolbox does however suggest any non-EU country to be at the receiving end of the toolbox. The toolbox requires MSs to *assess the risk profile of suppliers, i.e. risk of interference by a non-EU country*, yet still leaves the power to determine if a supplier should be banned to the individual MS. This arguably fragments the EU, in the fact that if one country finds that the PRC, for instance, can interfere through their telecommunication firms it only is determined by a single MS, unless similar cases persist throughout the EU. Arguably, if one MS determines that there is a risk of foreign (non-EU country) interference from a supplier, then one must assume that this is the case for all EU MSs, and not just a sole case in an individual MS, that has come to that evaluation. It is great however, to also have MSs take an active role in determining their risk assessment, but if interference can occur within one MS, the digital ecosystem of the EU as a whole has already been compromised based on the interoperability of the digital regime. It is also clear that the EU considers the subsidisation of European technology enterprises within the field of telecommunications similarly to what occurred in the case of Gaia-X. The Commission's role is outlined in the toolbox to *maintain a diverse and sustainable 5G supply chain in order to avoid long-term dependency.* This can be achieved through foreign and direct investment screening, trade defence instruments, competition, as well as strengthening the European capacities in the 5G (and post-5G) technologies (European Commission, 2020a), strengthening the overall (open) strategic autonomy narrative.

The technocratic nature of the EU has also led to establishments of certain organisations that work in accordance with the European goals. One of these organisations is the Network and Information Systems Cooperation Group (NIS Cooperation Group) which was established to ensure cooperation and information exchange among MSs. The NIS Group released a coordinated risk assessment of the cybersecurity of 5G networks prior to the 5G Cybersecurity Toolbox. Within this risk assessment, shortcomings and challenges were outlined to become part of the European telecommunications strategy. In general, the risk assessment is closely tied with the power which MSs received following the 5G Cybersecurity Toolbox and explicitly states the concerns of the EU and MSs may face in the advent of 5G networks. It is argued that *technological changed introduced by 5G will increase the overall attack surface and the number of potential entry points for attackers,* that *reliance of mobile network*

operators on third-party suppliers will increase and following this increasement that *the increase of the number of attack paths could be exploited by threat actors, in particularly non-EU states or state-backed actors*. As a result of this a concern over *a major dependency on a single supplier* has simultaneously evolved (The Network and Information Systems Cooperation Group, 2019), which contributes to the geopolitical dimensions of telecommunications, and the ban of Chinese-telecommunication firms in certain MSs. Furthermore, the report also reported that there is a lack of specialised and trained personnel to secure, monitor, and maintain a European 5G network – whether this is still reflective for cases such as Hungary, which is heavily reliant on Chinese industries to uphold their 5G networks will be assessed later in this study.

Another institution that has explicitly commented on the European strategy is the 5G Infrastructure Association. They have outlined the framework for building an ecosystem where driving firms acknowledge their dependency on other firms to achieve 5G growth. This framework heavily emphasises trust among these firms and also acknowledges the fact that mutual benefit and profit are of paramount importance, mirroring the concepts of regime theory and the prisoner's dilemma. The Infrastructure Association outlines that predictability in sharing of roles and revenues is important, and parties must demonstrate their willingness to leave parts of the market revenues to others, in order for 5G growth to organically occur within the EU. Furthermore, the ability to impose sanctions, and the acceptance of it as a governance mechanism, is also outlined and endorsed (5G Infrastructure Association, 2021, p. 16). A large aspect of the Infrastructure Association's report also considers the interplay between regulation and market growth (5G Infrastructure Association, 2021, p. 56). The fact that regulation is a key component in avoiding monopolies and the dynamic nature of digital regulation points at admittance that the current market is not strong enough to carry the European load, yet this is in stark contrast with the EC that Nokia and Ericsson are viable replacements of Huawei following the potential sidelining of the Chinese firm in relation to security concerns (Euronews, 2020).

Critique of the 5G telecommunications strategy is unveiled by da Ponte, Leon, and Alvarez (2023) as an asymmetrical problem within the EU. *The very high concentration of capacities in Germany, France, [...] and Ireland reveals imbalances that have exacerbated the impact of the lack of a unified regulatory framework as well as financing instruments that can compete with those implemented by others such as the US and [the PRC]* (p. 13). This imbalance in capacities would have a MS like Hungary

relocate their dependencies from one foreign nation state to another, the only difference would be the fact that the new dependencies would primarily be shifted to be inside of the EU borders, but that is not necessarily as appealing to a MS that lacks capacities as opposed to a more mutual dependency network of two high-capacity MSs. Furthermore, critique is presented by Koenig and Veidt (2023) as they argue that legal uncertainty in relation to EU's data governance strategies fosters an environment where European Internet Service Providers suffer from lack of investment and innovation in relation to the legal uncertainty (p. 6). Furthermore, it is argued that the EC acknowledges this but does not do enough to address the legal uncertainty regarding highly quality-sensitive content, applications, and services delivered via the 5G network (Koenig & Veidt, 2023). Without adequate investment in the security of the internet service providers, sensitive end-user data that is exchanged through content and application providers can be intercepted, as the national regulatory authorities have asymmetrical approach to their case-by-case basis of regulating the data. This can, and will, furtherly widen the information technology gap among the EU MSs.

EDGE OBSERVATORY & EDGE COMPUTING – TYING IT ALL TOGETHER

Edge computing, a relatively new and emerging technology, is the processing of computation and data storage closer to the sources of data. In the case of the European narrative for the digital regime, this is the idea that European data should be stored within the EU borders, so that the data stored is ensured to be processed, governed, and accessed in accordance with the data regulation which the EU has decided upon. The current European rhetoric regarding edge computing strongly emphasises the general digital sovereignty narrative through the ideas that data storage should be decentralised (in this case moving it from distant data centres to proximate locations) (European Commission, 2023e, p. 24). The application of edge computing can boost the European digital sovereignty in many different ways, even ways that exceed the two policy fields which are represented in this study.

In relation to this the European Edge Observatory has been established. The Edge Observatory *monitors the evolution of the climate neutral and secure edge node landscape and ecosystem across the EU Member States, mapping the deployment of nodes, investigating the use cases of edge nodes, and assessing the development of the EU edge node market* (European Commission, 2024f). Furthermore, it has published their *Edge Employment Data Report*. Within this report, the budgets, projected

deployments of edge nodes, and comments on national tendencies are included. Regarding budgets it shows the limitations, which no common strategy involves, as enterprises within each of the MSs invested the following in 2022 (Ferrer, et al., 2023, p. 19):

SPENDING AMOUNT (2022)	GERMANY	HUNGARY	SWEDEN
€0	57%	NA	73%
€10,000-€49,999	7%	NA	0%
€50,000-€99,999	10%	NA	0%
€100,000-€999,999	7%	NA	0%
€1M to less than €5M	7%	NA	0%
€5M to less than €10M	0%	NA	3%
€10M to less than €25M	3%	NA	3%
€25M to less than €50M	0%	NA	7%
€50M or more	10%	NA	13%

These budget reports, while excluding Hungary, shows the importance of general industrial capacity, as it is solely the more digitalised countries that have enterprises which have agreed to participate. Furthermore, the report projects deployment the following (Ferrer, et al., 2023, p. 76):

	2025	2026	2027	2028	2029	2030	TOTAL
GERMANY	344	426	396	341	233	105	2,405
HUNGARY	9	13	14	15	13	7	82
SWEDEN	45	56	52	45	31	24	319

Despite the uneven funding in Germany and Sweden from the former table, it is interesting to think about the capacities that are not related to solely investing and funding of edge nodes. Germany will deploy more edge nodes than Sweden, and despite Hungarian funding not being incorporated in the former table, they are still planning on deploying edge nodes.

The report notes that spending (budget) is highly dependent on approaches to data sovereignty and compliance is related to resilience against unforeseen disruptions

in the digital security regime. The report furthermore notes this reflects differing regulatory and data handling norms, potentially driven by legislative frameworks governing data and privacy (Ferrer, et al., 2023, pp. 16, 40, 81).

Tying edge computing with cloud computing is important, as *hyperscalers headquartered in the US* (Amazon, Microsoft, and Google) *controls the global public cloud infrastructure*, with these three taking up approximately 80% of the competitive positioning on the EU27 market, and it is argued that 90% of the European cloud market is currently dominated by non-EU players (European Commission, 2023e, pp. 9-10). Through the establishment of edge computing, the EU can at least seize control over the data, if these non-EU data providers can be regulated in a sense that European data needs to be hosted within the borders of Europe, taking back control over the data that is stored in the cloud. The EC found that *Europe can take benefit of the strengths of the European industrial ecosystem across the professional value chain and adopting a collaborative approach to face the competition of the non-EU giants* and through this the European Alliance for Industrial Data, Edge and Cloud was founded in July 2021 (European Commission, 2023e, p. 11). The European Alliance for Industrial Data, Edge and Cloud outlined in their roadmap the importance of the interplay between edge computing and cloud computing:

> "It is important that data are appropriately protected in accordance with European values and regulations. A huge amount of European data is currently available to and processed by a few non-EU companies based in countries with different legislations, making it difficult to apply and enforce European legislation and to preserve European privacy and security standards (European Alliance for Industrial Data, Edge and Cloud, 2024, p. 46)."

This underlines the importance of increasing the European storage capacities, and with the interplay between European cloud computing and edge computing solutions. If the European cloud computing alternatives does not have the capacity to be hosted within the EU, it can first and foremost not align with the general digital sovereignty goals of the Gaia-X programme, and secondly, the data cannot be insured to live up to the European standards. Furthermore, regulation cannot be put into place, that regulates non-European companies to host European data within the region, if the capacity is not great enough in accordance with the supply of European data. Therefore, if a MS finds the

appeal of European privacy and security standards to be an important political aspect, it is important for the individual MS to take part in edge computing, which will strengthen cloud solutions as a spillover effect.

The same is also true for the telecommunications narrative. Mobile edge computing brings computing capabilities closer to the user, while allowing for localised data processing and analysis, ensuring the hosting of data and interconnectivity of user devices (European Commission, 2023e, p. 35). Furthermore, the great interplay of edge computing and 5G infrastructure is also important for the digital sovereignty narrative based on the great position of Nokia and Ericsson (European Commission, 2023e, p. 134). The idea of edge computing and its importance for digital sovereignty, is referenced to by Ericsson as *all potentially sensitive data could be kept locally* (Ericsson, 2024). Ericsson also argues that a benefit from edge computing is indeed data sovereignty, they are able to *comply fully with jurisdictional data regulations and sovereignty laws by allowing data to be processed locally, or within a particular geographic region* (Ericsson, 2024). Based on this, it is therefore important for the EU MSs to push for edge computing not only in relation to the cloud capabilities of the EU, but also for EU data to be processed locally, ensuring the European standards are being uphold.

In general, commitment to edge computing reflects deeper layers in commitment to telecommunications and cloud computing, offering more depth to MS commitment to digital sovereignty, as it is the gateway for ensuring that data can be hosted in a manner, which allows for preserving European privacy and security standards.

Furthermore, edge computing provides a look into the future for the EU MSs. Whereas the race within both cloud computing and 5G telecommunications is hard to get back in, edge computing offers an opportunity for the EU. It is considered that the *EU ecosystem has developed strong expertise at multiple stages of the value chain needed to master managed edge platforms, giving it a competitive advantage over its main competitors* (European Commission, 2023e, p. 45). If the EU MSs surely support digital sovereignty, they have to invest in emerging technologies, where the market is still open enough for the EU to become a dominant player in the field. It is imagined that edge computing will be one of the key drivers of growth for information technology businesses by 2023, and therefore the EU and its MSs has to capitalise on this trend in order to regain some of the market share in information technology which it has lost in the last two decades.

MEMBER STATES AND THEIR IMPLEMENTATION OF DIGITAL SOVEREIGNTY

One of the key benefits of the EU approach to establishing a digital security regime is the fact that it strengthens opportunity of avoiding potential fragmentation, that could be resulted by individual national regulation from each MS. Even though this fragmentation is a concern, that still surrounds the bottom-up compliance and alignment with the greater European digital strategy through the fact that differentiated integration is definitely occurring through the asymmetrical relation and knowledge each EU MSs has to digitalisation. Digitalisation is not an even distribution, as is evident through the sample countries for this analysis. Sweden is uncontestably the sample MS that has undergone the greatest digitalisation prior to a common data regime, Germany, is traditionally a great power within the EU, however digitalisation has always been a struggle for the large economy to adapt to, and finally, Hungary overcomes it general laggard-labelling and exceeds the EU average when it comes to digitalisation.

The EU has several ways to categorise the digital transformation of its MSs, such as digital decade reports in relation to each individual MS, Eurobarometer, that reflects the general commitment in the population of each MS, but these models has an oversight in their approach to commitment to the digital strategy in a way that regards national jurisdiction, therefore the EU-provided models and scores cannot stand alone, and need to be paired with the initiatives on a national level, as opposed to solely regarding the digital regime and the post-sovereign nature of MS alignment, to avoid solely regarding the norm diffusion that occurs through compliance of regulatory norms. Socialisation will therefore need to be assessed through measures that stem out of national policies and commitment that allows for greater transparency regarding vertical Europeanisation.

Each of the three MSs that will be used in this analysis have received different monetary incentives, in accordance with the idea of common goods, that has been granted to each MS out of the RRP in order to incentivise EU MSs to achieving the Digital Decade targets. Each of the three MSs has received different allocations that is devoted to the digital transformation of each of them. The nations have received the following amounts (European Commission 2023a; 2023b; 2023c):

- Germany: €11,995,000,000
- Hungary: €1,200,000,000
- Sweden: €650,000,000

These RRP allocations also come with recommendations regarding the individual MS's digitalisation efforts from the EU's point-of-view, which grades the implementation of the digital policies within the MS. Alongside these recommendations from the EU, national digital decade roadmaps are also available, which grants access to KPIs in relation to the national strategies, allowing for a broader perspectivation of each individual MS's efforts in cloud computing, advanced telecommunication networks, and edge computing, along with other parameters.

The asymmetry that the post-sovereign model contributes to is also evident through different statistics from each of the three MSs, specifically in regard to the differing public opinions in each of the three MSs (European Union, 2020; European Union, 2024a; European Union, 2024b):

QUESTION EUROBAROMETER	**GERMANY**	**HUNGARY**	**SWEDEN**
What is the willingness to share personal information to improve public services?	57%	58%	88%
Would you like to take a more active role in controlling the use of your personal information? (Answer: Yes).	37%	16%	51%
To what extend to you agree or disagree with the following statements: You consider yourself to be sufficiently skilled in the use of digital technologies. (Answer: Totally agree and tend to agree pooled together).	81%	67%	87%
How high or low a priority is cyber security in your company? (Answer: Very high and fairly high pooled together).	76%	61%	71%
How many positions in cyber security currently need to be filled in your company if there would be appropriate candidates? (Answer: One or more open spots).	14%	5%	4%

The large, asymmetrical gap between the MSs show the reality of how unevenly knowledge and industries are distributed among the three (and thus the broader

European region), and unsurprisingly, it is generally agreed upon that Sweden is the most advanced of the three when it comes to digitalisation, especially considering their size relative to the other MSs. This is also evident through something like their amount of unicorn companies in Sweden in comparison to the two Germany and Hungary. Naturally, it is safe to assume, that with better digitalisation and differing views (more positive in relation to digital transformation), that Sweden would put in greater effort in relation to digitalisation on its own, whereas Germany would presumably focus more on the industrial production aspect of digitalisation.

GERMANY

Germany is being advised by the EU to *accelerate* its efforts in the area of digital skills, its efforts on connectivity infrastructure, and its efforts to digitalise public services. They are, being commended for their commitment to implement policies in the area of digitalisation of businesses, which is a policy area in which the EU recommends Germany to continue its current trajectory.

In the German case of cloud computing, a progress of 10.0% has been observed from 2023 to 2024, moving the current standing of the German KPI in cloud computing up to a 38.5% achievement, being stagnant with the EU performance indicator that is at 38.9%. Gaia-X is one of the largest contributors to the German support of an EU-wide digital ecosystem, showcasing the German subscription and commitment to the digital security regime, that aligns with the digitalisation of German enterprises according to all related cloud KPIs (European Commission, 2024b, p. 14). This relatively high KPI brings a positive contribution to the EU's digital decade target on cloud computing and demonstrates Germany subscribing to the narrative set-up by the EU in relation to the digital security regime, and the proposed way handling, storing, and exchanging data in a way that is in accordance with the European values. The general positive contribution to cloud computing shows the German cooperation with the broader digital regime, allowing for internalisation through professions in relation to making a habit out of handling European data within the borders of the EU.

The German Gaia-X hub, has in collaboration with the Austrian Gaia-X hub, released a position paper that has highlighted three concrete use cases of Gaia-X within the German context. Firstly, there is the Energy Efficiency Data Portal, which should provide a national access point for energy-related data, through the integration of data from local governments and stake holders, ensuring both local governments and stake

holders secure exchange of sensitive data. Secondly is the *Kommunale Datenwerke* (translates to Municipal Data Facility), which revolves around sharing data and IT infrastructure in cities, and promotion of cooperation between actors. This enables secure and trusted data use in inter-municipal data spaces, allowing for decentralisation of digital ecosystems and data spaces. Lastly, the Mobility Data Standardisation in Local Governments an initiative which allows for making data more usable in several decision-making settings, without fearing the loss of said data. Gaia-X is credited with tackling the lack of harmonisation and integration of data within German cities and regions, allowing for a more factual approach to the increasing data which MSs have access to. Finally, the position paper also emphasises the importance standards should play in both the municipal and broader national sector. "Standards are the central technical factor for sustainability in social (ethics and values), environmental (resource use and energy consumption), economic (investment security and business models) and technical (interoperability and vendor independence) terms. Numerous efforts in the smart city sector therefore aim at identifying requirements for norms and standards" (Brucke, et al., 2024, pp. 10-12). Through the combination of both the national KPIs and the initiatives from local governments and municipalities to adapt to the cloud computing suggests a general commitment, subscription and diffusion that occurs within the broader digital security regime in the German context.

Germany is one of the EU MSs which adapted the 5G Security Toolbox to its policies in a manner, which resulted in the German state backtracking on their previous commitment to Chinese firm Huawei, which Germany internally has been revealed to back during their draft of security standards for construction of 5G networks around 2020. Since the short time-span since then, Germany has adopted the narrative of digital sovereignty to a greater extent, and is currently phasing out the components which are supplied by Huawei, after their installation following the first steps in the German 5G strategy (Deutsche Welle, 2020; Deutsche Welle, 2024). One of the key highlighted components to this switch is the Ukraine War, which really highlighted the German dependence on Russian fossil oils and has presumably acted as a wakeup call for the German government, that they need to invest heavily into the German supply chains, and thus the (open) strategic autonomy of the EU, with digital sovereignty being a key principle of this. The German identity is heavily reflected in this, along with the German context, therefore, it is hard to say whether the same German commitment to digital sovereignty would have occurred if it was not because of the Russian invasion of Ukraine.

However, as it is also a key aspect as the war plays a greater role in the commitment of the EC to boost the (open) strategic autonomy, and therefore, it is safe to assume that Germany has not necessarily adopted to the rhetoric and narrative of the greater EU, instead, the German position and the position of the Commission was aligned prior to this, which is also evident in the German commitment to Huawei following the 5G Joint Declaration. Type II socialisation has therefore played an enormous role in the telecommunication policies of the German state.

An interesting component in the German 5G telecommunications strategy has been outlined by Walter and Trampusch (2024) as they argued that the German telecommunication firms argued heavily against banning Huawei in the 5G infrastructure of the German state (pp. 547-548). Even though German industry was opposed to the ban, the German state opposed these claims by the industry and banned the Chinese firm in providing infrastructural components to the German telecommunications network. Through the ban the German state is heavily reinforcing the idea of digital sovereignty within the EU, especially considering the fact that Germany is the largest economy within the Union. Germany, along with the other EU MSs, is thus able to construct the policies of the post-sovereign digital regime and contribute to the "facts" of the narrative, and the concerns that the EU needs to lessen its dependencies on non-EU actors. German 5G coverage is relatively high at 98.1%, almost 10% higher than the overall coverage in the EU. It is agreed upon that the German commitment to European standards in 5G is easily obtainable (European Commission, 2024b, p. 11), and the cost of phasing out Chinese components is increasing the cost of the 5G rollout, but this cost reflects an immense support and alignment with the European digital sovereignty.

German commitment to edge computing is among the highest of MSs in the EU. Latest estimates report that 351 edge nodes are deployed in Germany, making it the leader in edge computing. The main objective of the German commitment to edge computing it to create a completely new decentralised environment allowing for a software infrastructure for the advanced use of computing resources from the cloud to the edge, which will reduce technological dependencies, as it is operated by multiple suppliers (European Commission, 2024b, pp. 9, 13). Germany is a founding member of the Important Project of Common European Interest in Next Generation Cloud Infrastructure and Services (IPCEI CIS) which is a an "important project" in the cloud and edge computing domain. It concerns the development of this overarching idea of an interoperable and openly accessible European data processing ecosystem (European

Commission, 2023d). One of the driving forces behind German commitment to edge computing regards the retaining over control. Sebastian Ritz, CEO of German Edge Cloud has said that *manufacturers such as BMW and VW are currently implementing digital production platforms on the basis of global public cloud services available from vendors such as Amazon and Microsoft. Suppliers must make their data available in a corresponding form but wish to safeguard their intellectual property. As a result, we recommend the deployment of an open edge platform that ensures they retain control over their* data (Friedhelm LOH Group, 2019). Edge computing is closely linked with another European strategy as evident through the comment from Ritz. Industry 4.0 will only be achievable through the help of initiatives such as edge computing.

Germany being the largest provider of edge nodes within the EU suggests that indeed, industrial capacities are at the forefront of digital sovereignty. Admittedly, (open) strategic autonomy, and the pillar of digital sovereignty, does indeed stem out of these dependencies which the EU has seen as a result of outsourcing its production abroad. This is evident through their many edge nodes and their fight against the hyperscalers which we see dominating data storage, where edge computing is a general opposition towards this, and enables the European MSs to regain control over the data that is stored, as external data access is minimised and mitigated through regional hosting such as in the case of German deployment of edge computing and nodes. Germany is presumably also the biggest beneficiary of edge computing, which is directly related with their commitment, as the backbone of its great economy is based on its manufacturing sector, a sector which stands to gain enormously in the presence of edge computing. A last contributing factor, which is also related to the digital sovereignty, is the increase in German cybersecurity and cybersecurity's connection to edge computing. In 2024 the German Federal Office for Information Security deemed that information technology security situation in Germany has been and remains worrying (German Federal Office for Information Security, 2024). With the German state directly hinting at their worries for the cybersecurity of the MS, it is no surprise that Germany is taking up a large quantity of European edge computing based on the role of that and their push for Industry 4.0. Edge computing is a critical piece in the German approach to decentralising data processing and enhance industrial efficiency, contributing greatly to digital sovereignty. This is also evident through the European industrial technology roadmap, which states that it is imperative that Europe takes a leading role in cloud and edge security to ensure trust and confidence in industrial data management (European Commission, 2021).

The German approach to data security and informational autonomy has long been underway. In the Digital Strategy 2025, the German approach outlined the importance of these two notions and highlighted that they are of importance to the German democracy, predating the digital sovereignty narrative. They even recognised the power of European legislation stating that *fragmented national data protection rules, legal ambiguities and possibilities for circumvention will be eliminated* in regard to data protection (German Federal Ministry for Economic Affaris and Energy, 2016).

HUNGARY

The recommendations from the EU based on Hungarian commitment to their digitalisation efforts and the digital regime, suggests the asymmetricity of information technology knowledge within the EU. In regard to digital skills and connectivity infrastructure, the EU recommends Hungary to step up its efforts. In the area of digitalisation of businesses, they are even advised to significantly step up their efforts. In the final parameter, digitalisation of public services, Hungary is recommended to accelerate its efforts (European Commission, 2023b).

These recommendations reflect the interplay between policy conflicts, bargaining, and asymmetrical knowledge. This would not explain for the Hungarian commitment to the PRC, however. Tying this to cloud services, a domain in which the PRC is not the dominant actor, Hungary is argued to bring a positive contribution to the EU's digital decade Cloud target. Even though the current numbers for cloud solutions within the MS is slightly below the EU average (37.1% vs. 38.9%), significant annual growth has occurred in the MS, heavily outweighing the EU average (34.2% vs. 7%). Hungary does indeed seem to find itself receiving positive payouts in relation to cooperation in cloud computing, even though the MS expect many businesses to rely on the use of simpler or on-site solutions (European Commission, 2024c, p. 13). Putting the national roadmap aside, looking at the Gaia-X Hub of Hungary shows another side of the story, which is probably related to the internal asymmetricity within the MS. Deputy State Secretary for Digitalisation, Dr. Károly Balázs Solymár has noted that:

> "Data has become an indispensable source of economic growth, competitiveness, innovation, prosperity, and even security and sovereignty. Strategic autonomy in Europe can be achieved by developing and, where appropriate, pooling national capabilities, an excellent example of which is the

> bottom-up Gaia-X cooperation in the field of data economy and the development of the necessary data infrastructure, which can be mutually beneficial for both the domestic data ecosystem and European cloud capabilities (Hungarian Computer Science and Control Research Institute, 2022)."

This notion is also resonated within the body that represented the Hungarian industry players at the announcement of the Hungarian Gaia-X Hub stating that *businesses, research, education, governments, and social data are some of the important areas targeted by the National Hub* (E-Group, 2022).

Even with the consideration of the Hungarian rhetoric that accompanies their Gaia-X Hub, there is still quite a gap to go for the MS's implementation of the digital ecosystem. The Hungarian Hub lacks the transparency of the other national hubs, as they do not have their own website, and do not construct any research or goals set out in position papers similarly to the German Hub. In 2025, Hulkó, Kálmán, and Lapsánzsky argued that there are two relatively big reasons for the lack of a coordinated digital innovation in a MS such as Hungary. The first of these two, is the question on national sovereignty and supranational governance. Hulkó et al. (2025) presented the fact that due to the unique political, economic, and cultural characteristics of the region nation-state sovereignty weighs higher than the post-sovereign approach of the EU and thus the digital regime (pp. 6-7). Furthermore, the lower economic capacity makes the development of digital infrastructure and the MS's regulatory capacity dependent on EU funding, yet full commitment to the idea is still hard due to the context of the MS (Hulkó et al., p. 8). This is not necessarily a bottleneck for vertical Europeanisation and diffusion of the digital regime, as one of the strengths of the Gaia-X ecosystem is the collective pooling and sharing data of data, infrastructure, and innovation amongst the national Hubs. However, it seems like the horizontal Europeanisation is yet to be fulfilled.

Sino-Hungarian relations are an outlier compared to the general Sino-European relations. Wang (2023) outlines this to be due to several aspects of the two nation states political and economic affairs. Hungary is generally considered to be the biggest beneficiary of Chinese initiatives within the Central East Europe. Due to these relations, Hungary's perception of the PRC is generally more positive as opposed to the other EU MSs (p. 57). With Hungary having beneficial relations with the PRC prior to the announcement of the 5G Security Toolbox, it is no surprise, that the MS did not limit Huawei's uptake and commitment to the Hungarian 5G network. Arguably, the

Hungarian reality is differing to that of other EU MSs, even though they are more digitalised than the EU average. The Hungarian digitalisation, and the fact that they exceed the EU average, can also be credited to their relations with the PRC. Huawei has been a large supplier of the Hungarian telecommunications since 2013, and in 2023 Hungary and Huawei announced they were deepening the strategic cooperation between the two parties further (AboutHungary, 2023). While this does not align with the overall idea and driving force behind the digital sovereignty strategy of the EU, it is safe to assume the Hungarian identity and Sino-Hungarian relations are playing a large role in the Huawei 5G influence. Granted, the EU has left the decisions up to each of the EU MSs, and therefore Hungary is not doing anything that is outside of the EU regulation, yet the strategic autonomy of the Hungarian tech sector may not be as important to Hungary, as that of Germany or Sweden.

Hungarian socialisation with the PRC has been beneficial to the MS, and therefore there is no reason for Hungary to shift their dependencies from an already beneficial bipartisan relation to a dependency on a European provider. The Hungarian reality is that excluding Huawei is the least favourable solution, and without restrictions from the EU level, it is safe to assume, that Huawei's presence in Hungary will be increasing, even though it undermines the greater digital sovereignty narrative that is constructed by the EU and supported by some of the EU MSs. Hungarian 5G coverage is also increasing rapidly, going from 57.9% covered in 2023 to 83.7% covered in 2024 representing an increase that is more than four times the increase of the EU average in annual progress (European Commission, 2024c, pp. 4, 10). With such an annual progress, it is safe to assume that Hungary is on its way to comply with the Digital Decade target. This increase also supports the sentiment that Hungary would not find it viable to switch over to European suppliers in their 5G infrastructure.

Hungary is a co-founder of the IPCEI CIS, yet this is not reflected in the MS and their current edge deployment. Hungary only offers 5 edge nodes and has not included edge node deployment in their digital decade road map. Hungary is advised to take advantage of its involvement as a direct partner in this, however, it does seem that Hungary is too ambitious for their own good in regard to both cloud computing and edge computing, as nothing of greater character can be extracted from their commitment to these aspects of digital sovereignty and the European digital regime. However, through their inclusion in these initiatives, they are definitely supporting the greater narrative

regarding collective knowledge within the EU and are thus contributing to digital sovereignty through their participation.

The commitment is also shown in the Hungarian National Digitalisation Strategy for 2022-2030, which was revised in 2024. Multiple measures refer to the European data infrastructure and the emerging innovative digital technologies. Amongst these are initiatives DA II titled *creating a data-based state* and initiative DG II *targeted and innovative development of the ICT sector and ecosystem* (Hungarian Cabinet Office of the Prime Minister, 2024). Both of these measurements aim to boost the digital readiness of businesses, fostering the integration of digital technologies and encourages the innovation in key digital solutions such as edge computing, cloud, and telecommunications, highlighting the interplay between these. Within this framework is support for domestic data centres, edge computing infrastructure, and 5G deployment, as well as the call for acceleration of these.

One of the bottlenecks of Hungary lies in terms of integration of digital technologies where Hungary ranks 25th overall amongst the EU MSs. Hungary shows the worst performance in the business segment (Hungarian Cabinet Office of the Prime Minister, 2024, p. 6), which provides a surprisingly stark contrast to that of Germany, even considering the fact that Hungary is a co-founder of the IPCEI CIS. Despite being the a co-founder, the challenges which accompanies Hungarian businesses is also evident through the Edge Observatory report. The National Digitalisation Strategy also emphasises the Hungarian priority is to support the data economy, which is also reflected through the MS's commitment to Gaia-X and edge computing, even though no road map goals have been announced in regard to Hungarian edge computing. This priority is emphasised both under the objectives of the Hungarian digital economy and the Hungarian digital state. With this vague rhetoric of the Hungarian goals, it is evident that they would like to contribute furtherly, but do not have the capacity.

SWEDEN

The high Swedish standard in digitalisation is also represented through the EU's recommendation. Based on this, the only measurement which Sweden should accelerate is the effort within connectivity infrastructure. Within the other three measurements (policies in the area of digital skills, policies in the area of digitalisation of businesses, and implementation of policies to digitalise public service) Sweden is simply recommended to continue with their current efforts (European Commission,

2023c). It is generally agreed upon that Swedish digital ambitions are very high, and that they allocate significant efforts to achieve the Digital Decade objectives and targets (European Commission, 2024d, p. 4), even despite of the fact that they are only just in the progress of joining an initiative like Gaia-X. The fact that Sweden is a latecomer to the Gaia-X project can potentially be credited due to the fact that 66% of Swedish enterprises already use cloud computing and solutions (European Commission, 2024d, p. 13), and therefore, waiting for Gaia-X to become more streamlined would undeniably be the strategy of the MS. With the lack of current European data storing solutions, it is important to note that with their commitment, they would contribute greatly to helping with generalisation and institutionalisation of European cloud services, when, and if, the majority of Swedish enterprises make the switch to European hosted solutions.

With the Gaia-X expansion into Sweden is relatively recent, the construction of it is heavily based on the idea of digital sovereignty. Johan Christensen, an initiator of the Swedish Gaia-X organisation argued the following in relation to the Swedish Hub:

> "Sweden and the rest of the EU have gradually become dependent on a small number of companies outside the EU to handle our data infrastructure. This not only impedes the potential autonomy of the world's largest economy, it also places our most valuable asset, our data, outside of European jurisdiction (Gaia-X Sweden, 2021)."

This sentiment is also emphasised at one of the largest technology companies in Sweden, Ericsson:

> **"**Europe must build data infrastructure based on values, such as openness, accessibility and the protection of privacy. In this context, GAIA-X has a key role to play in the creation of the next generation of data services in Europe. In view of the breadth of potential users of GAIA-X's data services – everything from storing personal data, such as photos and letters, to process-critical industrial data – it is crucial that GAIA-X makes available a wide range of user cases and requirements. We are therefore encouraging Swedish industry and Swedish authorities to become involved in GAIA-X and in particular in the Swedish GAIA-X hub to create user cases and requirements that can help to ensure the success of the venture from a Swedish perspective (Gaia-X Sweden, 2021)."

Despite the slow expansion into Sweden, it is clear that both initiators such as Christensen and large tech enterprises, such as Ericsson, heavily subscribes to the European narrative, and the norms that the EU try to diffuse through its digital regime. Not only is there clear that the Swedish Gaia-X Hub concerns both the openness, accessibility, and the protection of user privacy is a normative sense, they also wholeheartedly endorse the European jurisdiction of the digital regime and the regulatory mechanisms of it. This paired with the high KPI scores of Swedish cloud computing up-take suggests governance, identity, and capacity of Sweden aligns heavily with the expectations set up by the broader EU regime.

Sweden is interesting in the telecommunications context due to one of the largest European telecommunication providers being based in Sweden. However, similarly to the case of Germany, the interest of Swedish firms was not playing a role in the decision of banning the Chinese providers Huawei and ZTE from the 5G telecommunications networks in Sweden. Ericsson feared backlash from their exposure in the Chinese market and were afraid that they would see inconceivable losses as a reaction to the Swedish ban of the Chinese telecommunication firms (Reuters, 2020). Even though Sweden banned Chinese firms in their 5G networks, the Swedish 5G coverage is really high scoring in at 90.3% of the Swedish territory covered with 5G telecommunications (European Commission, 2024d, p. 4). Swedish cyber security initiatives have also been bound on the 5G Security Toolbox, which has allowed for Sweden to deploy a secure and resilient 5G network, contributing to the digital regime.

Despite the Swedish ban of Chinese firms in its 5G telecommunication network, it is worth noting that Huawei had overtaken Ericsson in capacities of the two telecommunication companies comparatively, first it was in quantity and quality measurements, and then later annual sales. This is argued to reflect that the rise of Huawei was not solely due to the Chinese government's support, but more importantly its technological strengths (Joo, Lee, & Oh, 2016, p. 38). This emergence in Huawei as a leader in telecommunications, overtaking a Swedish company, can possibly also be at the root of the digital sovereignty issues which are represented in the Swedish ban of Huawei and ZTE despite the Ericsson company advising against banning the Chinese firms. However, it would be safe to imagine, that with the way telecommunications and technologies are auctioned in relation to national deployment of them, that the larger a company is, the better their offer can possibly be.

Following the Swedish ban, it is important to note that Ericsson has slowly gained market share in different EU countries which followed suit. Ericsson have agreed on deals with other EU MSs such as Spain and Portugal when it comes to supplying their 5G infrastructure and architecture. Courts upheld the ruling on banning Chinese 5G firms, yet the geopolitical nature of these aspects still stand, as there certainly is a degree of this, that is highly related to the interplay between economics, cybersecurity, and digital sovereignty.

Swedish commitment to edge computing is relatively low, based on their generally high digitalisation. Currently Sweden is hosting approximately 34 edge nodes, while this is more than Hungary, Sweden is not participating in the IPCEI CIS, showing more nuance to the debate regarding asymmetry. One would presumably imagine that the Swedes would participate in a cutting-edge project that regards data infrastructure, both no direct commitment to edge computing has been expressed by the MS besides through their few edge nodes. However, Swedish initiatives is evident through the collaboration between the research institute *RISE* and the Swedish Lulå University of Technology. One of the key leaders of RISE has even stated that "edge is the future. It is a key technology that will be the next big arena for digital innovation. Soon there will be an edge node in every street corner (Research Institute of Sweden, 2021)." Despite this comment, it seems like the deployment of Swedish edge nodes are still not at a level which depicts the Swedish digitalisation properly. Generally speaking, it has become evident that Sweden heavily subscribes to the digital sovereignty narrative. With their large digital presence, it is surprising that Sweden only has approximately 34 of the total 1186 edge nodes in the EU. Similarly to Hungary, Sweden has not added targets for edge nodes in their roadmap, furtherly emphasising the importance of Industry 4.0 and its correspondence to the edge node deployment. However, it is worth noting that edge node employment went up with 20 nodes on an annual basis (2022 to 2023).

The Swedish commitment to edge computing should not be undermined, however. Through their competence centre Trustworthy Edge Computing Systems and Applications (TECoSA) they outline their industrial and societal relevance. TECoSA outlines the safety-critical interactions between humans and cyber-physical systems, contributing to the security narrative and the importance of data storing and governance. Within this field, it is argued through TECoSA research that technological challenges, contractual, privacy, security, liability, safety assurance, and corresponding standards are still challenges which the Swedish edge computing deployment is facing (Törngren,

et al., 2022, p. 7). This reflects both the high standards of Swedish digital transformation as well as the MS's commitment to European values and principles.

COMBINED COMMITMENT OF THE SELECTED MEMBER STATES

In general, the approach to the EU's digital regime is divided among the EU MSs. It seems like the countries that will gain from the digital sovereignty of the digital regime is more keen on strengthening their position within the European market through stricter and bigger commitment to the European digital regime, furthermore, a country like Hungary which is prepositioned in a way where a more positive approach to the PRC for instance seems to be playing a larger role in their commitment to digital sovereignty, as they are gaining net-positives from collaborating and cooperating with Huawei for instance.

The digital regime of the EU seems to be scattered all over the place, and that is largely thanks to the asymmetry in information technology knowledge. The EU has failed to address this properly, and therefore the very ambiguous and abstract ideas which they are posing in relation to the establishment of the digital regime does not consider the full context of each of the MSs, which has a say due to the post-sovereign nature of the regime. However, the regulations of the EU does contribute to the idea of NPE instead of it being a regulatory shift, due to a commitment to the EU, this is one of the strengths surrounding the narrative, as the regulations constructed by the EU does not force MSs to unfairly shift their commitments from non-EU actors to solely European actors, still maintaining a fair open market, where individual cases are regulated by security concerns of individual MSs.

The identity of each MS is peculiar in the sense that each of them differs in one way or the other in regard to the digital strategy. Germany being a co-founder of Gaia-X of courses sees the MS being a leader in cloud computing. The interesting aspect of this is the fact that solely based on the rhetoric the EU has been constructing and pushing for the last decade, MS initiatives are still part of the digital transition. An initiative such as Gaia-X is not mandatory for organisations to participate in, yet it reflects whether Type I or Type II socialisation is occurring within each MS. Another aspect which hints at secondary socialisation is the weakening of traditional alliances such as the transatlantic one, it is the clearest example of the dynamic nature of external relations being context-driven and shaped by identities and socialisation. This is also evident in a case such as telecommunications, where Hungary is an outlier based on the contextualisation of the MS.

Generally speaking, there is a commitment to the digital regime among the EU MSs, however the incentives to fully emerge and adopt to the socialisation is so individualistic, that cases will occur, where non-EU actors propose larger incentives for the MSs that already has strong, healthy, and beneficial relations with non-EU suppliers. The EU and its MSs do not have the capacity to be fully sovereign either, yet the storing of data and the governance models seem to be generally agreed upon amongst EU MSs. It is more so industrial capacity and supply chains which becomes the problem as opposed to the norms and human rights-centric approach and narrative of the EU.

The issues that are accompanied with the industrial sovereignty, which is an integrated part of digital sovereignty, is clearly outlined through the lack of commitment to edge computing. None of the three MSs that have been analysed have put edge nodes, and edge computing, into their digital decade roadmap, but the EU has. The EU target for 2030 is a total of 10,000 edge nodes within the region, and the reality is that European edge nodes are far away from the target. The lack of national instruments in regard to edge computing, besides very vague commitment to the digital transformation, supports the understanding that industrial capacity is a bottleneck for the EU MSs.

Looking back at regulations such as the DSA and the DMA presents itself in an interesting manner to the post-sovereign structures of the EU. While the DSA and the DMA are outside of the MS power, they are two regulations that are almost exclusively exercised by the EC. Even though the Commission excels at regulating through these two regulations, it is important to consider whether the European digital space will be able to innovate new services to compete with the gatekeeper-coined American MNCs, and if not, then it is worth doing a risk assessment on whether continuous regulating within the field would be able to push out the services provided by these American MNCs.

DISCUSSION

HORIZONTAL DIFFUSION: EXPORTING THE EUROPEAN STANDARD IN THE CASE OF BRAZILIAN GDPR MIRRORING

A case in which the EU has been successful in exporting its standards and norms in relation to the overall EU policies has been the case of GDPR. GDPR is a regulation that primarily emphasises the strongest arguments for European data governance, as well as most appealing aspects of the digital regime – the human-centric, open, and human-rights perception of personal data. When the EU is at its greatest, it is able to reach a

level where NPE does indeed find itself managing to be based on principles, norms, and standards of operations.

In 2020 the Brazilian General Data Protection Law (LGDP) came into place, providing a clear case of normative diffusion in a horizontal aspect. Similarly to the GDPR regulation, LGDP has extraterritorial application, and both agree on several basics when it comes to data protection. Besides not including a single definition for personal data, it is argued that the LGPD mirrors the GDPR's definition of personal data (Koch, 2023). Naturally differences in the legislations are also evident, as the Brazilian government has to tailor it to fit the needs of the nation state.

However, it is a clear case of the fact that Europe, through its NPE concept, is able to appeal to some of the right aspects of greater international norms and be a leader within digital regimes if the application of it does not find itself being too ambiguous and abstract. Furthermore, GDPR does not have the same bottlenecks as the digital regime and digital sovereignty, as it does not find itself adding constraints that exceed MS capacities within the storage of personal data, while also showing the geopolitical measurements which an extraterritorial regulation is able to excel in. When there are not constraints on the industrial capacity, and thus not internal industrial opposition, the EU can push for ambitious regulations that reshape global data and digital governance reinforcing its role as a regulatory superpower.

The strength of GDPR and its normative diffusion lies in the successful vertical Europeanisation, where the EU MSs have all adopted to the regulation successfully, and therefore, it becomes a benchmark for horizontal diffusion among EU and non-EU players.

VERTICAL DIFFUSION: PERSPECTIVATION TO THE EUROPEAN GREEN DEAL AND THE ABSTRACT NATURE OF VERTICAL EUROPEANISATION

An example of where vertical diffusion did not occur to its fullest extent is the EU Green Deal. The Green Deal, despite its singular name, is a series of projects that need to be implemented simultaneously in a relative short time span. Similarly to the EU Green Deal, the digital regime and digital strategy does not consider certain fragmentations among its MSs. Three fragmentations which the Green Deal has suffered from can be narrowed down into political, financial, and social natures (Snijders, Gimber, & Furno, 2023).

The political nature of the Green Deal became evident following the differing industrial policies of the MSs. Germany was also involved in this, as they opposed the de-facto ban of on sales of new vehicles with internal combustion engines, as a means to protect their thriving automotive industry. This brough forth similarly critique from other MSs sharing the same industrial edge in automobile manufacturing, and while a compromise was reached initially, which allowed for hybrid vehicles to continue their sales, it seems that Italy is currently attempting to push back the Green Deal again. Regarding the financial nature and its rooted fragmentation showcases the economic differences among MSs. This provides issues in regard to the green transition due to the fact that companies would have asymmetrical access to state aid based on their locations, widening the gap and divergences amongst MSs for the decades to come. Finally, social fragmentation is evident through many ways. Some MSs have identities which suffer from an uneven historical context regarding green energy, and therefore companies are divided among MSs, and the MSs that have historically been frontrunners in the green transition will thus have a leap and are more likely to be able to live up to the standards set in place through the Green Deal.

Despite the Green Deal still being pursued from an EU point-of-view, the fragmentation of MSs reflects the same industrial capacity differences which the digital regime and digital sovereignty also represents. It is too ambiguous and abstract for the majority of nation states to fully adopt to, as evident through the lack of cloud computing and edge computing deployment in a an otherwise digitalised MS. Similarly, countries that do not find itself gaining beneficial industrial incentives from the adoption of autonomous 5G infrastructure does not see any benefits in changing their technological alliances to be in favour of other MSs, when the incentives do not grant a utility maximisation. Finally, a MS like Germany, that represents multiple European sectors through its industries seems to have a greater capacity at applying digital sovereignty and the digital regime to their policies, despite the fact that the MS has historically always been bad at implementing digitalisation based off a historical context.

When the vertical diffusion does not occur, the EU will be unable to export its standards and norms on a greater scale, because it fails to comprehend the importance of the financial and industrial capacities, even though the normative aspect resonates among its MSs. The weakness of the post-sovereign approach which the EU provides fails to address the agency of individual countries based on factors which the EU cannot control or incentives properly to make a change within as a means of coercion.

CONCLUSION

The findings of this study propose that while the EU has made significant strides in establishing a normative and institutional framework for digital sovereignty, the coherence of this framework is undermined by persistent fragmentation, diverging national interests, and asymmetries in digital capacity and political will among member states.

Germany, Hungary, and Sweden serve as representative case studies to illustrate the complexities of norm diffusion within the EU. Germany exemplifies leadership and co-ownership in EU digital initiatives, notably Gaia-X, demonstrating strong alignment with the European digital sovereignty agenda. However, even Germany's initial reliance on Chinese telecommunications components reflects the persistent challenges of implementation. Sweden, with its open-data legacy, aligns ideologically with the EU's normative values, yet it maintains a critical stance toward certain EU instruments, choosing autonomy in how it operationalises policy at the national level. Hungary, by contrast, reflects resistance to EU digital norms, maintaining close technological ties with China and demonstrating limited internalisation of EU values. This heterogeneity highlights the uneven vertical Europeanisation across the Union.

From a theoretical standpoint, the combination of Normative Power Europe and Regime Theory offers valuable insight into the EU's strategy. The EU acts as a norm entrepreneur, constructing a values-based identity rooted in democratic governance, human rights, and multilateralism. Yet, the success of its digital sovereignty narrative depends not only on the capacity to project these norms but also on their uptake by MSs. The post-sovereign nature of the EU, relying on interdependence and shared sovereignty, requires more than formal compliance; it necessitates identity transformation at the member state level. A transformation that is hard to achieve, when national identities and differing governance strategies.

The study emphasises three major challenges: Governance complexity, where the EU must navigate the tensions between supranational directives and national sovereignty; 'Europeanisation and identity' which requires a shift in how states view their technological future in relation to European values; and 'Capacity and asymmetry' wherein resource-rich states like Germany can lead, while less digitally advanced or ideologically resistant states may lag or resist. These obstacles limit the EU's ability to present itself as a unified actor in the global digital order. Furthermore, external

pressures from US tech hegemony and China's infrastructural diplomacy expose the EU to a strategic dilemma: to build autonomy without closing itself off, and to maintain openness without compromising security or normative coherence. The EU's digital sovereignty initiatives, such as the 5G Action Plan, the 5G Security Toolbox, Gaia-X, and Edge Computing tying these together into more depth, embody an attempt to reconcile these tensions by establishing internal governance regimes that also shape global norms. However, as this research demonstrates, the success of these initiatives is conditional upon sustained political commitment and a shared vision among member states. Without stronger mechanisms for socialisation and incentive-based alignment with the digital regime, the EU risks digital disintegration, where MSs operate in divergent technological ecosystems influenced by competing global powers, through the lack of initiatives funded in cooperation among the MSs. Ultimately, this study concludes that the EU's attempt to forge a post-sovereign digital regime is too ambitious due to the asymmetrical EU capacities, flawed and ambiguous in its funding. It challenges the Westphalian logic of sovereignty and projects a normative model that contrasts with market-driven American liberalism and state-centric Chinese digital authoritarianism. Yet, the internal fragmentation and asymmetrical commitment among MSs undermine the potential for coherent external projection.

Without proper investment frameworks for establishing European supply chains that can actually sustain the European demand and future expansion, strategic autonomy will not be achievable and thus digital sovereignty by extension becomes nothing more than a fancy phrasing for allowing the EU to penalise external actors for not abiding by European regulation. For the EU to truly become a global digital power, its digital sovereignty strategy must evolve from a regulatory framework into a socially embedded identity shared across the Union. Strategic autonomy in the digital age requires more than infrastructure, it requires a cultural and political redefinition of what it means to be digitally European, and a mindset where capacities are shared cross-borders. This study contributes to ongoing debates on European integration, sovereignty, and global digital governance by showing that the EU's global role will depend on its ability to harmonise internal fragmentation and embed digital sovereignty as a shared value, not just a policy goal.

BIBLIOGRAPHY

5G Infrastructure Association. (2021). *5G Ecosystems: Vision and Societal Challenges Working Group Business Validation, Models, and Ecosystem Sub-Group*. Brussels: 5G Infrastructure Association.

AboutHungary. (2023, October 20). *Hungary signs new MoU with Huawei*. Retrieved from AboutHungary: News in Brief: https://abouthungary.hu/news-in-brief/hungary-signs-new-mou-with-huawei

Acharya, A. (2009). *Whose Ideas Matter? Agency and Power in Asian Regionalism*. Thaca: Cornell University Press.

Acharya, A. (2014). *The End of American World Order.* Cambridge: Polity.

Alden, C., & Lu, J. (2019). Brave New World: Debt, Industrialisation and Security in China-Africa Relations. *International Affairs*, 641-647.

Altbertoni, N. (2024). *Trade Protectionism in an Uncertain and Interconnected Economy.* Milton Park: Routledge.

Arbatova, N. (2015). Euro-Atlantic Relations in the 21st Century: Problems and Scenarios. *World Economy and International Relations*, 31-37.

Associated Press. (2025, April 24). *Huawei lobbyists banned from accessing European Parliament after bribery arrests*. Retrieved from Associated Press: https://apnews.com/article/huawei-corruption-eu-parliament-belgium-brussels-arrests-f91e918ab1057f82f33e175993ce17db

BBC. (2025, April 9). *What would a US-China Trade War do to the World Economy?* Retrieved from British Broadcasting Channel: https://www.bbc.com/news/articles/c4g2089vznzo

Blauberger, M., & Sedelmeier, U. (2024, August 12). *Why the EU has started to act against democratic backsliding - and why it may even stay the course*. Retrieved from European Politics and Policy: https://blogs.lse.ac.uk/europpblog/2024/08/12/why-the-eu-has-started-to-act-against-democratic-backsliding-and-why-it-may-even-stay-the-course/

Börzel, T., & Risse, T. (2014). *From Europeanisation ot Diffusion.* Milton Park: Routledge.

Bradford, A. (2007). Regime Theory. *Max Planck Encyclopedia of Public International Law*.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *Journal of Common Markey Studies*, 1261-1280.

Brucke, M., Etminan, G., Hofmann, D., Kraemer, P., Krins, T., Leufkes, R., . . . Schmeling. (2024). *Setting the Course: Gaia-X and the Future of Data-Centric Government*. Munich: Gaia-X Hub Germany.

Butler, G. (2021). State Monopolies and the Free Movement of Goods in EU Law: Getting Beyond Obscure Clarity. *Legal Issues of Economic INtegration*, 285-308.

Carrai, M. A. (2019). China's Malleable Sovereignty Along the Belt and Road Initiative: The Case of The 99-Year Chinese Lease of Hambantota Port. *NYU Journal of International Law and Politics*, 1061-1100.

Česnakas, G., & Juozaitis, J. (2023). *European Strategic Auonomy and Small States' Security: In The Shadow of Power.* Abingdon, Oxon: Taylor & Francis.

Checkel, J. T. (2007). *International Institutions and Socialisation in Europe.* New York: Camdrige University Press.

Csernatoni, R. (2022). The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty. *European Security*, 395-414.

da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological Sovereignty of the EU in Advanced 5G Mobile Communications: An Empirical Approach. *Telecommunications Policy*, 1-17.

Deschaux-Dutard, D. (2022). European Defence in an Interpolar Context: Explaining the Limitations of French-German contribution to European Strategic Autonomy. *Defence Studies*, 591-608.

Deutsche Welle. (2020, September 16). *Europe Will Not Follow the US 'China-Free' 5G Strategy*. Retrieved from Deutsche Welle: https://www.dw.com/en/opinion-europe-will-not-follow-the-us-china-free-5g-strategy/a-54948684

Deutsche Welle. (2024, July 11). *Germany to Phase Out Chinese Components in 5G Networks*. Retrieved from Deutsche Welle: https://www.dw.com/en/germany-to-phase-out-chinese-components-in-5g-networks/a-69632743

Deutsche Welle. (2025, April 9). *What is a Trade War and how big is the US-China One?* Retrieved from Deutsche Welle: https://www.dw.com/en/us-china-trade-war-trump-tariffs-economy/a-72183002

Di Carlo, D., & Schmitz, L. (2023). Europe FirsT? The Rise of EU Industrial Policy Promoting and Protecting the Single Market. *Journal of European Public Policy*, 2063-2096.

E-Group. (2022, May 13). *Gaia-X Landed in Hungary*. Retrieved from E-Group: Software and Beyond: https://www.egroup.hu/gaia-x-landed-in-hungary/

Ericsson. (2024, November 14). *Exploring the Edge: A Must for 5G Success*. Retrieved from Ericsson: https://www.ericsson.com/en/edge-computing

Euronews. (2020, July 25). *EU insists European companies could replace Huawei in 5G network*. Retrieved from Euronews: https://www.euronews.com/2020/07/25/eu-insists-european-companies-could-replace-huawei-in-5g-network

European Alliance for Industrial Data, Edge and Cloud. (2024). *European Industrial Technology Roadmap for the Next-Generation Cloud-Edge*. Brussels: Publications Office of the European Union.

European Commission. (2015, September 28). *The EU and China signed a key partnership on 5G, our tomorrow's communication networks*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/ip_15_5715

European Commission. (2016). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Comittee of the Regions: 5G For Europe: An Action Plan*. Brussels: European Commission.

European Commission. (2020a). *EU toolbox for 5G security : a set of robust and comprehensive measures for an EU coordinated approach to secure 5G networks*. Belgium: Publications Office of the European Union.

European Commission. (2020b). *Gaia-X: A Franco-German Pitch Towards a European Data Infrastructure*. Brussels: Publications Office of the European Union.

European Commission. (2021). *European Industrial Technology Roadmap for The Next Generation Cloud-Edge Offering*. Brussels: Publication Office for the European Union.

European Commission. (2023a). *2023 Digital Decade: Annex Germany*. Brussels: European Commission.

European Commission. (2023b). *2023 Digital Decade: Annex Hungary*. Brussels: European Commission.

European Commission. (2023c). *2030 Digital Decade: Annex Sweden*. Brussels: European Commission.

European Commission. (2023d). *Commission Approves up to €1.2 Billion of State Aid by Seven Member States for an Important Project of Common European Interest in Cloud and Edge Computing Technologies*. Brussels: Publications Office of the European Union.

European Commission. (2023e). *Study on the Economic Potential of Far Edge Computing in the Future Smart Internet of Things*. Brussels: Publications Office of the European Union.

European Commission. (2024a, October 11). *A Stronger Europe in the World*. Retrieved from European Commission: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/story-von-der-leyen-commission/stronger-europe-world_en

European Commission. (2024b). *Digital Decade Country Report 2024: Germany*. Brussels: European Commission.

European Commission. (2024c). *Digital Decade Country Report 2024: Hungary*. Brussels: European Commission.

European Commission. (2024d). *Digital Decade Country Report 2024: Sweden*. Brussels: European Commission.

European Commission. (2024e, February 23). *NextGenerationEU*. Retrieved from European Commision: https://commission.europa.eu/strategy-and-policy/eu-budget/eu-borrower-investor-relations/nextgenerationeu_en

European Commission. (2024f, November 5). *Edge Observatory for the Digital Decade*. Retrieved from European Commission: Shaping Europe's digital future: https://digital-strategy.ec.europa.eu/en/policies/edge-observatory

European Commission. (2024f). *Shaping Europe's Digital Future*. Retrieved April 2025, from Shaping Europe's Digital Future: DESI Indicators: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?indicator=desi_dsk_bab&breakdown=ind_total&unit=pc_ind&country=HU,DE,SE,EU&period=desi_2024&periodX=desi_2024&periodY=desi_2024&indicatorX=desi_iuse&indicatorY=

European Parliament. (2011, April 4). *Report ont the EU as a Global Actor: Its Role in Multilateral Organisations*. Retrieved from European Parliament Website: https://www.europarl.europa.eu/doceo/document/A-7-2011-0181_EN.html

European Parliament. (2020). *Digital Sovereignty for Europe*. Brussels: European Parliamentary Research Service.

European Union External Action. (2023, March 17). *The Diplomatic Service of the European Union*. Retrieved from The EU as a Global Actor: https://www.eeas.europa.eu/eeas/eu-global-actor_en

European Union. (2007, December 13). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007*. Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

European Union. (2020). *Special Eurobarometer 503: The Impact of Digitalisation on our Daily Lives*. Brussels: Eurobarometer.

European Union. (2022a, December 14). *Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030*. Retrieved from EUR-Lex: https://eur-lex.europa.eu/eli/dec/2022/2481/oj

European Union. (2022b, September 2022). *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)*. Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

European Union. (2022c, October 19). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)*. Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

European Union. (2022d, May 30). *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)* . Retrieved from EUR-Lex: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

European Union. (2024a). *Flash Eurobarometer 547: Cyberskills Report*. Brussels: Eurobarometer.

European Union. (2024b). *Special Eurobarometer 551: On the Digital Decade 2024*. Brussels: Eurobarometer.

Farrand, B., & Carrapico, H. (2022). Digital Sovereignty and Taking Back Control: From Regulator Capitalism to Regulatory Mercantilism in EU Cybersecurity. *European Security*, 435-453.

Ferrer, A., Dekker, R., Romeo, S., Perez, M., Branco, M., Minde, T., . . . Brinkhege, R. (2023). *Edge Deployment Data Report*. Luxembourg: Publications Office of the European Union.

Fetzer, T., & Schwarz, C. (2020). Tariffs and Politics: Evidence from Trump's Trade Wars. *The Economic Journal*, 1717-1741.

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, 887-917.

Fouskas, V., & Gökay, B. (2019). *The Disintegration of Euro-Atlanticism and New Authoritarianism: Global Power-Shift*. Charm: Palgrave Macmillan.

Friedhelm LOH Group. (2019, September 13). *German Edge Cloud Cemonstrates that Edge Computing is a Key Technology for Smart Factories*. Retrieved from Friedhelm Loh Group: https://friedhelm-loh-group.com/en/aktuelles/german-edge-cloud.asp?utm

Gábriš, T. (2021). 5G and Digital Sovereignty of the EU: The Slovak Way. *TalTech Journal of European Studies*, 25-47.

Gaia-X Sweden. (2021, April 20). *European Cloud Collaboration Gaia-X Expands to Sweden*. Retrieved from Gaia-x Sweden: https://web.archive.org/web/20210618013205/https://gaiax.se/contact/

Gaia-X. (2024a). *Gaia-X Architecture: Building the Backbone of Trusted Digital Ecosystems*. Brussels: European Association for Data and Cloud AISBL.

Gaia-X. (2024b). *Gaia-X Compliance Document*. Brussels: European Association for Data and Cloud AISBL.

Gaia-X. (2024c). *Gaia-X Trust Framework: Your Pathway to Trusted Digital Ecosystems*. Brussels: European Association for Data and Cloud AISBL.

Gaia-X. (2024d). *General Overview: Gaia-X*. Brussels: European Association for Data and Cloud AISBL.

Gaia-X. (2025a). *Together Towards a Federated and Secure Data Infrastructure*. Brussels: European Association for Data and Cloud AISBL.

Gaia-X. (2025b, April 28). *What's in it for me?: Gaia-X*. Retrieved from Gaia-X: https://gaia-x.eu

Gaia-X. (2025c, March 1). *Gaia-X Hubs: Gaia-X*. Retrieved from Gaia-X: https://gaia-x.eu/community/hubs/

German Federal Ministry for Economic Affaris and Energy. (2016). *Digital Strategy 2025*. Berlin: Federal Ministry for Economic Affaris and Energy.

German Federal Office for Information Security. (2024, November 12). *Thre State of IT Security in Germany*. Retrieved from Federal Office for Information Security: https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA and the Surveillance State.* Penguin: London.

Griffiths, J. (2021). *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet.* London: Zed.

Guilbaud, A., Petiteville, F., & Ramel, F. (2023). *Crisis of Multilateralism?: Challenges and Resilience.* Cham: Palgrave Macmillan.

Haroche, P. (2023). A 'Geopolitical Commission': Supranationalism Meets Global Power Competition. *Journal of Common Market Studies*, 970-987.

Harris, M. (2019). Punishment & Power: An Examination of the European Union's Use of Lawfare Since 1993. *Clocks and Clouds*, 149-181.

Hasenclever, A., Mayer, P., & Rittberger, V. (2004). *Theories of Internaitonal Regimes*. Cambridge: Cambridge University Press.

Hiavac, M. (2010). Less Than a State, More Than an International Organization: The Sui Generis Nature of the European Union. *Georgetown Public Policy Institute*, 1-18.

Hlover, I., & Mawuko-Yevugah, L. (2024). The Current World-System and Conflicts: Understanding the U.S.-China Trade War. *Journal of World Systems Research*, 583-609.

Hoffmeister, F. (2023). Strategic Autonomy in the European Union's External Relations Law. *Common Market Law Review*, 667-700.

Hulkó, G., Kálmán, J., & Lapsánszky, A. (2025). The Politics of Digital Sovereignyy and the European Union's Legislation: Navigating Crisis. *Frontiers in Political Science*, 1-9.

Hungarian Cabinet Office of the Prime Minister. (2024). *National Digitalisation Strategy 2022-2030.* Budapest: Digitaliske Szsegek.

Hungarian Computer Science and Control Research Institute. (2022, April 29). *SZTAKI has established the Gaia-X Hungarian National Hub*. Retrieved from Hungarian Computer Science and Control Research Institute: Computer Science and Control Research Institute

International Monetary Fund. (2025, March 3). *GDP, Current Prices (2025)*. Retrieved from International Monetary Fund: https://www.imf.org/external/datamapper/NGDPD@WEO/CHN/USA/EU

Jacobs, T., Gheyle, N., de Ville, F., & Orbie, J. (2023). The Hegemonic Politics of 'Strategic Autonomy' and 'Resilience': COVID-19 and the Dislocation of EU Trade Policy. *Journal of Common Market Studies*, 3-19.

Joo, S., Lee, K., & Oh, C. (2016). Catch-Up Strategy of an Emerging Firm in an Emerging Country: Analysing the Case of Huawei vs. Ericsson with Patent Data. *Int. J. Technology Management*, 19-42.

Jora, O.-D., & Butisecâ, A. (2024). Free Trade Semantic Disagreements: Why WTO-Style Multilateral Liberalization and FTAs Stand Much Closer to Protectionism. *Romanian Economic and Business Review*, 7-28.

Katzenstein, P. J. (1996). *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press.

Keohane, R. O. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

Keohane, R. O. (2018). *International Institutions and State Power: Essays in International Relations Theory*. New York and Milton Park: Routledge.

Keohane, R. O., & Nye, J. S. (2012). *Power and Interdependence*. Glenview: Longman.

Koch, R. (2023, September 14). *What is the LGPD? Brazil's version of the GDPR*. Retrieved from GDPR: https://gdpr.eu/gdpr-vs-lgpd/

Koenig, C., & Veidt, A. (2023). Lifting a Regulatory Millstone Around 5G Investors' Neck - 5G Network Slicing Versus EU-Net Neutrality. *Telecommunications Policy*, 1-11.

Krasner, S. D. (1993). *International Regimes*. Ithaca and London: Cornell University Press.

Layne, C. (2012). This Time It's Real: The End of Unipolarity and the "Pax Americana". *International Studies Quarterly*, 203-213.

Leal-Arcas, R. (2006). Theories of Supranaitonalism in the EU. *The Journal of Law in Society*, 88-113.

Manners, I. (2002). Normative Power Europe: A Contradiction in Terms? *Journal of Common Market Studies*, 235-258.

Meyers, Z. (2023). Can the EU afford to drive out American cloud services? *Centre for European Reform*, 1-5.

Monsees, L., & Lambach, D. (2022). Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity. *European Security*, 377-394.

Nagy, C. (2019). World Trade, Imperial Fantasies and Protectionism: Can You Really Have Your Cake and Eat it Too? *Indiana Journal of Global Legal Studies*, 87-132.

Pannier, A. (2021). The Changing Landscape of European Cloud Computing: Gaia-X, the French National Strategy, and EU Plans. *Geopolitics of Technology Program*, 1-7.

Research Institute of Sweden. (2021, June 30). *Test Bed for Edge Technology and 5G Leads the Development*. Retrieved from Research Institute of Sweden: https://www.ri.se/en/test-bed-for-edge-technology-and-5g-leads-the-development?utm_source=chatgpt.com

Reuters . (2019, November 5). *Hungarian minister opens door to Huawei for 5G network rollout*. Retrieved from Reuters: https://www.reuters.com/article/business/hungarian-minister-opens-door-to-huawei-for-5g-network-rollout-idUSKBN1XF1UT/

Reuters. (2020, October 20). *Sweden Bans Huawei, ZTE from Upcoming 5G Networks*. Retrieved from Reuters: https://www.reuters.com/article/sweden-huawei-int-idUSKBN2750WA/

Reuters. (2022, June 22). *Swedish court upholds ban on Huawei sale of 5G gear*. Retrieved from Reuters: https://www.reuters.com/business/media-telecom/swedish-court-upholds-ban-huawei-sale-5g-gear-2022-06-22/

Reuters. (2024, July 11). *Germany to phase out Huawei, ZTE components from its 5G core network*. Retrieved from Reuters: https://www.reuters.com/business/media-telecom/germany-agrees-phaseout-huawei-zte-components-5g-core-network-2024-07-11/

Rieker, P., & Giske, M. (2024). *European Actorness in a Shifting Geopolitical Order: European Strategic Autonomy Through Differentiated Integration*. Basingstoke: Palgrave Macmillan.

Risse, T., Ropp, S., & Sikkink, K. (1999). *The Power of Human Rights: International Norms and Domestic Change*. Cambridge: Cambridge University Press.

Schmitz, L., & Seidl, T. (2023). As Open as Possible, as Autonomous as Necessary: Understand the Rise of Open Strategic Autonomy in EU Trade Policy. *Journal of Common Market Studies*, 834-852.

Snijders, A., Gimber, J., & Furno, B. (2023, May 10). *The Challenges for the EU's Green Industrial Policy*. Retrieved from Fleishmanhilllard: Public Affairs & Government Relations: https://fleishmanhillard.eu/2023/05/the-challenges-for-the-eus-green-industrial-policy/

Sojka, A., Terraza, J., Crespo, F. C., & Rumín, Á. C. (2025). Russian Invasian as a European Issue: Vertical Europeanisation of National Political Debates and the War in Ukraine. *European Union Politics*, 1-34.

Strange, A. (2023). *Chinese Global Infrastructure.* New York: Camdrige University Press.

Tan-Mullins, M., Mohan, G., & Power, M. (2010). Redefining 'Aid' in the China-Africa Context. *Development and Change*, 857-881.

The Network and Information Systems Cooperation Group. (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks.* Brussels: The Network and Information Systems Cooperation Group.

TNO. (2024, June 14). *GAIA-X: A European Initiative for Increased Digital Sovereignty*. Retrieved from TNO: https://www.tno.nl/en/digital/data-sharing/gaia-digital-sovereignty/

Törngren, M., Thompson, H., Herzog, E., Inam, R., Gross, J., & Dán, G. (2022). Industrial Edge-based Cyber-Physical Systems - Application Needs and Concerns for Realization. *ACM/IEEE Symposium on Edge Computing*, 1-8.

von der Leyen, U. (2020, February 19). *Shaping Europe's Digital Future: Op-ed by Ursula von der Leyen, President of the European Commission*. Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260

Walter, M., & Trampusch, C. (2024). Economic Statecraft by Design and by Default: The Political Economy of the 5G-Huawei bans in the United States, United Kingdom, and Germany. *Competition & Change*, 539-560.

Wandel, J. (2019). Do Free Trade Agreements Promote Sneaky Protectionism? A Classical Liberal Perspective. *International Journal of Management and Economics*, 185-200.

Wang, X. (2023). Is China's Rising Presence in Hungary Since 2012 Impacting on Hungary's Relations with the EU? *Australian and New Zealand Journal of European Studies*, 47-63.

Welfens, P. J. (2020). Trump's Trade Policy, Brexit, Corona Dynamics, EU Crisis and Declining Multilateralism. *International Economics and Economic Policy*, 563-634.

Wendt, A. (1999). *Social Theory of International Politics*. New York: Cambridge University Press.

Whitman, R. G. (2011). *Normative Power Europe: Empirical and Theoretical Perspectives*. Basingstoke: Palgrave Macmillan.

Witt, A. C. (2023). The Digital Markets Act - Regulating the Wild West. *Common Market Law Review*, 625-666.

Woo, B., & Verdier, D. (2020). A Unifying Theory of Positive and Negative Incentives in International Relations: Sanctions, Rewards, Regime Types, and Compliance. *Economics of Governance*, 215-236.

Yilmaz, S., & Liu, C. (2018). China's 'Belt and Road' Strategy in Eurasia and Euro-Atlanticism. *Europe-Asia Studies, 70*(2), 252-276.

Zhang, A. H. (2024). *High Wire: How China Regulates Big Tech and Governs Its Economy*. New York: Oxford University Press.