Strategic Autonomy in the Global Tech Order: A study of European Union's Pursuit of Technological Sovereignty vis-à-vis US and China

August 2022

Glasgow Student Nº: 2573193

DCU Student Nº: 20109377

Charles Student Nº: 71707609

Presented in Partial Fulfilment of the Requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 20,570

Supervisor: Dr. Tomáš Karásek

Submission Date: 2nd August 2022

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude to: my supervisor Dr Tomáš Karasek, for his immense patience, valuable insights, and an atittude of encouragement throughout this dissertation process; the staff at each of the IMSISS consortium universities for their valuable logistic and academic support; most importantly my family and friends in India who, though physically far away, have been my strongest support system ; my flatmates and overseas friends, for the insightful conversations and for making my academic journey in Europe a memorable experience.

CONTENTS **PAGE**

1. **Introduction** **5**

2. **The evolution of technology in EU Strategic Autonomy Discourse** **8**

3. **Platform Governance & Regulation in Transatlantic Relations: A Case Study of GDPR** **19**

4. **EU's 5G Policy vis-à-vis China: Analysis of Threat Perceptions and divergent discourses** **31**

5. **Findings and Conclusion** **45**

6. **Methodology and Theoretical Perspective** **50**

7. **References** **54**

ABSTRACT

The evolution of European Union's strategic autonomy has been can be traced to its historical dependence on the United States through economic and security guarantees. However, in the last two decades, there has been a shift in EU's strategic thinking in terms of anticipating a scenario of potential American withdrawal from the continent. This strategic orientation has also been extended to the domain of technology where global interdependence on the same has been used to expand geo-strategic influence. This study traces the evolution of European Union's technological sovereignty as a part of its ambition to achieve strategic autonomy vis-à-vis the strategic technological competition between the United States and China. The case studies for this dissertation include (a) The analysis of Platform governance in Transatlantic relations and (b) EU's technological discourse vis-à-vis dependencies on 5G technologies in the domain of telecommunications and cybersecurity respectively. The study will be based on the theoretical perspective of strategic triangle angle approach in the context of EU's bilateral ties with both Washington and Beijing and discourse analysis will be methodology in practice with regards to the EU being the central object of reference for the study.

Keywords: Autonomy, China, EU, Sovereignty, Technology, USA

1.Introduction

Strategic autonomy can be defined as the agency of a state to prioritize and take autonomous decisions in the domain of foreign and security policy either through institutional, political and material co-operation with external parties, or unilaterally (German Institute of International Affairs ,2019) A high degree of strategic autonomy translates to stronger power projection to modify and influence international norms rather than obeying rules set by other players(ibid.)

Cyberspace as an arena for contestation

As cyberspace alongside technological digitalization of trade and commerce continues to become a key arena of strategic competition where the concept of sovereignty has exceeded national borders, the EU has increasingly grown concerned about its dependency on the United States and China on internet and communication technologies. The threat perception emerging from this dependency has been amplified due to the concerns over the practices of big tech companies ranging from social media platforms as well as 5G technologies, which the EU believes causes conflict over data and digital rights of its own citizens. Therefore, in order to strengthen its identity as a liberal-democratic actor in the digital sphere, the EU's emerging strategic framework is to elevate its role as a global tech regulator from a passive consumer dependent on American and Chinese big tech firms. Therefore, it is an important case to be studied as technology continues to shape strategic competition in the contemporary order.

The current discourse states that the key reason why EU has played a subordinate role to Washington in the current technological order, is that the very nature of its power projection has not been a globalist one and therefore, this explains Brussels' technological hardware and software dependencies on the United States (Fiott, 2017) This has been a major source of friction between the two and therefore, explains the change of stature adopted by Brussels. In one of his statements, the EU Commissioner for internal market- Mr. Thierry Barton, mentions that the cyberspace calls for the EU to exert full control over data and secure its connectivity as these were the fundamental pillars of digital sovereignty which were to be protected at all costs (Csernatoni, 2021) This statement is supplemented by the fact that the EU has created an institutional assemblage of technology-based research initiatives on artificial intelligence, cyber security and the most prominent one being the enforcement of General Data Protection Rules (GDPR) (Service, European External Action, 2020)

The magnitude of autonomous agency has become a degree of contention for EU's identity as a strategic actor on the global stage as its exposure to the strategic competition between the United States and China has confronted Brussels with a multitude of economic and security-based challenges. These challenges arising from this strategic competition are increasingly complex since they directly impact

global technological standards, supply chains and market exports (Helwig, 2021) The situation of possible American pull out from Europe has led to a concern regarding EU's capabilities to a achieve defensive and economic self-sufficiency, which also explains the further mainstreaming of EU highlighting its ambitions to attain strategic autonomy. It is in the development of this discourse of strategic autonomy where technology becomes a key cornerstone of achieving a more autonomous agency(ibid.)

The technological disruption that arose as a result of rapid digital transformation has led EU to identify several technological vulnerabilities regarding innovation policies concerning artificial intelligence, internet governance and 5G security in recent times (Helwig, 2021) The complex networks of interdependence have posed several geo-strategic risks as economic ties in the form of private organisations have been utilized as weaponised instruments by states such as US and China to further their geopolitical interests through coercion and creation of dependencie(ibid.) The Strategic dependencies in the domain of advanced technology have led to the development of EU's strategic orientation to find feasible solutions to achieve national security objectives and also continue receiving economic benefits of economic globalization(ibid.) The EU has taken cognizance of these global developments and to avoid subordination in a global order where technological advantage is a strategic instrument of power projection in dictating power hierarchies(ibid.) Thus, technological sovereignty assumes an important geo-strategic rationale for achieving strategic autonomy.

Considering its position in the contemporary geo-strategic environment, this study seeks to answer the following research question:

How does the EU deploy appropriate policy measures in its foreign and regulatory policy to consolidate technological sovereignty vis-à-vis United States and China in the global technological order? The research question seeks to fulfill the following aims and objectives:

a) To investigate the evolution of EU's strategic autonomy through analysing its strategic discourse on technological sovereignty. The key objective would be to frame technology as a central referent standpoint in EU's strategic culture and subsequently, evaluate the strategic and geopolitical rationales of the EU's traditional dependency on the United States and China in the case of internet and communication technologies. This would also dwelve into the changing nature of power projection practiced by EU in the realm of digital technologies and therefore deviations from traditional behaviour would also be addressed.

(b) The transatlantic security and economic alliance with the US has been a key pillar of EU's foreign policy. However, the behaviour of big tech firms has been a recent source of friction between the two.

Therefore, a key object of analysis would also address how the current institutional assemblage of EU's tech policy programmes comes into points of both collaboration as well as disagreements. With regards to its relations with Beijing, the study would analyse EU's policy goals with regards to achieving technological symmetery in 5G telecommunications through co-operation with Washington, in order to curb China's technological influence commercially across the globe.

(c) Lastly, the dissertation would also seek to analyse the geo-strategic triangular relationship between Brussels, Washington and Beijing through the measurement of both strategic convergence and divergence of policy measures to achieve its notions of technological sovereignty.

To achieve the above specified aims and objectives, the study is divided into three parts of the literature review:

(a) Chapter one focuses on the evolution of the debates around EU's strategic autonomy and how technology became an integral instrument in the development of Brussels' strategic orientation. This focuses on the rationales of external geopolitical factors that led to materialization of EU's technological discourse and how technological interdependence on United States and China shapes Brussels' threat perception. It also discusses how the policy discourse to achieve technological sovereignty is interlinked with technology being the contemporary instrument of power projection by the EU in addition to economic and normative power approaches. and how the latter seeks to consolidate its core identity as a liberal internationalist technological actor different from the United States. The chapter also explores the evolution of technological framework through techno-globalist and techno-nationalist ends of the spectrum respectively and its applicability how the EU being an exception of an institutionally collectivist identity not being a sovereign state is framed in the same. The chapter also analyses how the technological discourse on how EU's classification of defensive and offensive approaches to sovereignty shapes its policy orientation.

(b) Chapter two explores in detail the role of technology in shaping Transatlantic relations. The chapter explores debates of how the security perceptions of cyberspace differ in the strategic orientations of Washington and Brussels and how Washington legitimizing cyberspace being highly militarized differs from EU's human rights and consumer-oriented approach. The chapter also explores how the role of big tech and digital platforms being techno-political agents that carry the potential to shape domestic discourse set the groundwork for EU's regulatory framework vis-à-vis the same.

(c) The evolution of EU's regulatory framework is explored through the analysis of GDPR as an instrument of regulation and its potential to set global regulatory standards In addition to the policy divergences that arise in technological governance between the US and EU, the chapter also

analyses the emerging convergent framework between the two through the establishment of Trade and Technology council as a form of institutionalised co-operation with a mutual threat perception of China's growing technological footprint across the globe.

(d) Chapter Three analyses EU-China relations in the context of global proliferation of 5G technologies. It sheds light on contemporary factors that shape threat perceptions in regards to the discourse concerning technological governance of 5G in telecommunications and cybersecurity domains respectively. This includes EU's strategic discourse of what it perceives to be Beijing's convergent ecosystem that weaponizes tech companies as threat agents that carry out espionage and intelligence operations based on their links with the Chinese communist party. The chapter also includes analyses of EU's strategic and technical measures in regards to 5G and degree of divergence between policies of individual member-states. In addition to the same, the chapter also includes a comparative analysis of measures third countries with respect to the EU in the context of potential technological de-coupling from Beijing.

2. The evolution of technology in EU Strategic Autonomy Discourse

2.1 The Post WWII Origins of EU Strategic Culture

Strategic culture can be defined as a set of institutionalised thought process which is derived from a country's historical experience and aspirations that determine the conduct of responsible behaviour in national terms, but also incorporates an integrated system of symbols such as language, argumentation structure and metaphor in its official discourse (Anand, 2020) The usage of these symbols also elucidates strategic culture in terms of establishment of long-term strategic preferences and conceptualizes the role of military in diplomatic practices(ibid.) Therefore, it can be argued that the creation of the European Union was a result of the aftermath of World War II. It can be termed as a brutal collective historical experience that not only led to millions of deaths across the continent and widespread infrastructural destruction, but also became a point of strategic convergence where inter-state co-operation was viewed as a sole way to accelerate the post-conflict reconstruction and that a communitarian approach was the best-suited one to achieve this objective. Thus, it can be stated that the collective traumatic experience of the World War II laid the foundations of an interstate co-operation-based model, that manifested itself in the establishment of institution-based decision-making processes in form of European Economic Committee and later, the European Union.

The origins of a common European framework for a strategic culture can be attributed to François Duchêne, who put forth the identity of Europe as a civilian power that was not only a new actor in the international order with a unique role to play, but was built on the pillars of superpower détente and complex interdependence (Rogers, 2009) This intellectual framework can be perceived as one of the earliest steps to consolidate Europe's identity as a civilian centre of power that would overshadow its previous military stature and that it was a central player and that solidifying this identity of itself as a peaceful entity that could project its identity as an influential third alternative to United States and the Soviet Union at the height of the Cold War(ibid.) This notion of being perceived as a peaceful identity can be defined as one of the earliest cornerstones that aimed to establish Europe as an independent power in its own right, without the domination from Washington, whose hostility with Moscow often reduced Europe's independent agency in terms of its projection of influence. The debate has since been chronologically evolving, as a result of the rapidly evolving geopolitical environment in the wake of post-Cold War international order.

2.2 Central Facets of EU Strategic Autonomy

The discourse on Strategic autonomy in the context of EU can be defined that derives its central element of functioning through a model of policymaking that can be classified largely as institutional collectivism, where the sovereignty of Member States in terms of defense is not replaced completely by supranational policies from Brussels, and the structure of existing alliances is not weakened either (Pérez, 2019)

It is also the projection of a unified strategic vision, that success of collective policies would lead to a higher degree of enhancement in the capacities of individual member states(ibid. p82) The rationale for this framework applies often in specific operation areas that seek to establish a strong industrial base and through the facilitate economic growth individually through improved inter-state co-operation (ibid.) It is also important to highlight that the European Union's foreign policy also provides member-states a platform to adopt a dualistic approach to diplomatic practices at the operational level, through institutional collaborations and as well through autonomous channels(ibid.) The discussion is further extended into a varied expressions of power projection as multiple shifts in EU's identitarian perceptions of itself have been constantly evolving with the geopolitical environment and have shaped its decision making. These are as follows:

Economic power: The economic policies of the EU have been directed towards an orientation to maximise its geopolitical clout and have been cited as one of key central pillars regarding its discourse on strategic autonomy. This policy architecture represents an amalgamation of dualistic projection through its commitment to liberal internationalist principles by incentivising the creation of favourable business environments, alongside addressing policy gaps to enhance domestic industrial bases (Helwig, 2022) The policy that best describes this stance, is its development of the concept of what the European Commission calls- "Open Strategic Autonomy"; where the EU highlights its commitment to uphold a rules-based order that- (a) Exercises liberal market principles (b) Facilitates international trade with low barriers and simultaneously address high degree of dependencies in what it regards as strategic sectors(ibid; pp 25-26) The projection of its economic clout grants Brussels a high degree of strategic advantage to counter what it regards as investment practices of third states, which it considers to be a threat to its economic interests (Gehrke, 2022).

Thus, this dualistic approach not only strengthens the identity of the EU as a market power by projecting its economic influence to push for larger geopolitical goals that signal a more autonomous agency, but also strengthens its diplomatic alliances, especially the transatlantic partnership with the United States- a key actor that has been a leading advocate of liberal-internationalist rules-based order.

This order can be defined as an organised system of arrangements that are established by a group of international institutions, in order to govern interactions between member-states in order for the promotion of democracy and free-trade- based on liberal institutionalism and economic interdependence (Mearsheimer, 2019)

It can also be argued that economic power as an instrument also provides space for achieving strategic autonomy in terms of allowing EU to reduce institutional dependency on Washington and even develop its own identity as a separate liberal internationalist actor, whose geopolitical goals do not always converge with those of the US. Thus, projection of EU's economic and market power also serves as an instrument for strengthening its identitarian dimension of also being a realist actor. The announcement by present European Commission (EC) President Ursula von der Leyen to establish a Geopolitical Commission (GC) is an indicator about the EU's strategic posture especially in terms of managing interdependencies to achieve its goal of strategic autonomy(Helwig, 2022; p.27) The realist projection of strategic autonomy through establishment of institutions demonstrate, that the policy orientation has been designed for the achievement of self-sufficiency in a situation of potential decoupling from current alliances. Initiatives like the GC also serve as a unified instrument of power multipliers of member states, that projects a show of collective strength through integrated economic institutionalization based on integrated market systems (Hyde-Price, 2006)

Thus, the EU's projection of its identity as a market power is a central constituent to achieve strategic autonomy through achieving collective economic self-sufficiency, which accommodates interests of member-states through sharing unified collective benefits. This projection also represents an evolution of EU's foreign policy discourse, where geopolitical events in its neighbourhood and the wider world have led to the development of a chronological evolution of debates around its ambition of strategic autonomy in the last three decades.

Waves of Strategic Autonomy

The end of the Cold War was the early instance where the question of self-sufficiency in terms of achieving security was first raised, pertaining to the magnitude European military capabilities in a situation of potential withdrawal of American security cover from the continent. The Balkan Wars in the early 1990s sparked not only significant concerns about securing continental peripheries and also brought to the fore a lack of independent agency of the EU to act, but also prompted an urgent need to establish a mechanism where crisis management regarding the matters of continental defence were of primary concern, pertaining to conflicts in European peripheries (Helwig & Sinkkonen, 2022) While the Balkan conflict is said to have been a key event that triggered a strategic discourse of what is often termed as the first wave of EU's strategic autonomy, the second wave of the debate draws its rationale

in terms of transforming its ambitions from regional to global ones in wake of proliferation of conflicts in regions outside the continent such as Syria and Libya, that includes promotion of peace, security and liberal-democratic values in conflict zones beyond its borders(ibid; pp3-4) The third wave of the debate witnessed a more concrete projection of a unified vision, as the 2016 Global strategy document laid a high degree of emphasis on what it termed as an appropriate level of achieving its key geopolitical ambitions, signaling strong initial steps towards strengthening its official policy discourse about strategic autonomy(ibid.) The fourth wave of the strategic autonomy of the debate has been shaped by global impact of Covid-19 pandemic and the implications of the same has pushed Brussels towards developing a framework that addresses the governance aspects pertaining to health security, welfare and most significantly, economic recovery after the pandemic. It is during this wave that the defending its economic interests and central values in the domains of human rights and data privacy have become the EU's central priority, and the rapid digitalization of trade and service sector in the wake of intensified technological and geopolitical competition between United States and China, have prompted Brussels to take steps towards initiating an independent strategic discourse in the realm of technology. Thus, the fourth wave can also be described as a major inflection point where, interoperability forms the central determinant for a unified technological vision that is based on the discourse that an institutional approach to collective technological progress would also benefit individual member states by strengthening their respective industrial bases.

Techno Nationalist v/s Techno-Globalist Debate

The current wave of the debate pertaining to strategic autonomy extends to how the EU's strategic posture evolves in the geopolitical and technological spectrum of techno-globalism and techno-nationalism respectively. Techno-globalism defines technological innovation as an instrument of fostering deeper international engagement and seeks to promote the principle that promotes market values over state control, and that global technological governance is based on the central processes of internationalisation of industrial and commercial consumption of technologies based on transfer and diffusion (Wong, 2021) The techno-globalist thought also calls for the abolishment of trade barriers that prevent technology transfers and that research and development funds for scientific research should be institutionalised and formulated, with private individual firms being the central agency to establish standards and norms for commercial technology development(ibid; pp22-23) When viewed from a lens of diplomatic practice, the techno-globalist framework of governance elevates the position of individual firms as- (a) One of the key parties for negotiations with national governments (b) Creates dependencies the private organisations as the chief agencies for acquiring and diffusing technologies(ibid; p.23)

Techno-nationalist orientation of governance defines technological strength as a key instrument of national power in a fiercely competitive geopolitical environment and autonomy in a state's technological domain is crucial to its apparatus in order to contain threats to its national security (Erickson & Johnson-Freese, 2006) Techno-nationalist policy orientation also differs significantly from the techno-globalism by the justification of a rationale that follows: The former conceptualizes a state's technological capacity in terms of development of domestic industries, that can withstand hegemonic market behaviour and competition from established multinational foreign enterprises and therefore, regulating market access is essential to sustain their domestic industrial base(Wong, 2021; p.24) Techno-nationalist states also seek to regulate processes generating not only technical expertise, but also extend this practice vis-à-vis the standards that govern design and manufacturing(ibid.) The promotion of idea of supremacy of autonomy and self-sufficiency over technological dependence from foreign entities is conceptualized through (a) Diffusion through a primarily domestic consumer base and (b) Disseminating knowledge, that facilitates and enhances domestic scientific and technological capabilities (Nakayama, 2012)

The divergence between techno-globalism and techno-nationalism is witnessed in the following differences: (a) Techno-globalism seeks to consolidate national power through expansion of economic influence by maximizing international market share for disseminating technologies and (b) Techno-nationalism on the other hand employs an insular approach through measures of technology protectionism and seeks to maintain a technological advantage over other nations(Wong, 2021; p.24) The measurement of this spectrum is explained as Techno-globalism as a liberal periphery of international political economy and techno-nationalism being classified in the realm of realism(ibid.)

The evaluation of the EU's strategic discourse of its technological dimension, in the pursuit of strategic autonomy can be conceptualized as a projection an institutionally unified vision of pan-European strategic framework, which underlines its orientation towards being a techno-nationalist actor. However, it also stands out as an exception where unlike a singular state, it represents an example of collectively instituitionalised entity in the reference of techno-nationalist framework. However, the transatlantic alliance with the United States also makes the EU as a key element in Washington's sphere of technological and economic influence, due to its dependencies on the latter for the same.

It can be stated that technological competition in the contemporary era is a central element in shaping the contemporary Geo-economic order and structure of this order dictates the direction and nature of technological exchange and regulation at the global level. Geo-economic Order can be defined as a structure based on macro-level changes in the strategic relationship pertaining to security and economics with regards to the rules of international system and its impact on governance matters of international trade and investment law (Roberts, et al., 2019)

The profound change that impacts this order, are the functioning dynamics of how power is perceived by major players in the system (China and USA being the present-day examples) in-order to attain their economic and geo-strategic ambitions and therefore, this new order tends to focus more on relative economic gains over the absolute ones (ibid; pp659-660)

The domains of contention in the present geo-economic order include a high degree of security threat perceptions due to a high degree of economic interdependence and digital connectivity that has created a strong global competition for technological development and thus, has fostered protectionist tendencies(ibid; p.657) While technological interdependence might play a vital role in accelerating economic efficiency, it can also transform into a potential source of strategic vulnerabilities and diminish geo-strategic interests of the states through dependence on foreign states for critical technologies (Farrell & Newman, 2019) Since many of these technologies are categorized as necessary instruments to enhance strategic depth, but it can also generate strategic vulnerabilities in terms of- Dependencies on foreign states for the supply of critical technologies necessary to the economic advancement and military capacity of great powers(Roberts, et al., 2019; p.659) This transition from economic to a security-based strategic re-structuring signals that states have taken cognizance of these vulnerabilities and thus, have prompted greater calls for self-reliance(ibid.; p.660) Thus, it can be argued that the emergence of techno-nationalism can also be viewed as one of the concrete steps towards an increasing securitisation of techno-globalism in the current geo-economic and security order.

The threat perception of weaponised technological interdependence has been a concerning matter for the EU to seek technological self-reliance and thus it has moved swiftly towards establishing an independent framework for what is now categorized as “Technological Sovereignty”. Technological sovereignty can be defined as capability of a single country or a federation of states to develop and provide technologies that it classifies as a critical component to achieve welfare and competitive objectives (Fraunhofer Institute for Systems and Innovation Research ISI, 2020) In addition to the latter, technological sovereignty also seeks to provide a higher degree of autonomous agency in terms of developing and sourcing technologies from multiple economic areas, without creating a unilateral structural dependency(ibid; p.2) In its official policy discourse, the EU has defined European technological sovereignty as the ability for Europe to attain self-sufficiency in terms of development, protection, provision and retention of critical technologies that are integral to: (a) Ensuring welfare and prosperity for European citizens and businesses (b) Having an independent agency to secure its interests in a globalized environment (European Parliamentary Research Service , 2021)

It can be stated that the EU's rationale for seeking technological sovereignty is stated to have strengthened first back in 2016 with the cyber security being stated as one of the central pillars of its Global Strategy Document. The development of a unified cyber infrastructure to mitigate threats in its strategic discourse lays a key emphasis in providing assistance to member states in building cyber defence capabilities and ensure that the safety along with free and easy access of internet in cyberspace is ensured. The strategic discourse also entails mitigation of threats through increasing resilience of critical infrastructural networks and services for reducing cybercrime (European External Action Service , 2016) In order to attain this objective, the EU also seeks to prioritise innovation in Information and Communication Technology systems that defend Europe's digital space through creating appropriate policy framework to secure data storage and establish a certification system of digital products and services(ibid; p.21-22)

The 2016 Global Strategy document also considers integration of technological sovereignty in the Common Security and Defence Policy (CSDP) missions essential for institutional efficacy in its technological functioning as a collective unit (ibid; p.22) The collective cyber policy co-operation extends not only to cyberspace governance between member-states and EU institutions, but also seeks to strengthen cyberspace co-operation with US and NATO, both of them being long-term security partners. In addition to the co-operation with member-states and transatlantic institutions, the Global Strategy document also mentions the importance of forging public-private partnerships as a key constituent of its emerging framework of governance in cyberspace(ibid.)

It can be inferred that the EU's policy orientation regarding the involvement of private sector in the technological domain stems from its recognition of how crucial is the role of private big-tech firms, such as social media and e-commerce companies from the likes of Amazon and Facebook in dictating the norms that influence governance in the cyberspace. Thus, the global strategy of 2016 also conceptualizes the ambition of achieving technological sovereignty by the development of a common cyber strategic culture that is based on a co-operative framework based on three levels i.e.- between member-states, transatlantic institutions and private sector respectively. The second rationale that has been at the standpoint of EU's strategic discourse on technological sovereignty, is how it perceives its position in the midst of the technological dimension of US-China strategic competition and seeks to craft a framework where its technological projection can attain an autonomous position within the global technological order. Thierry Breton, in his speech mentions what he calls- a long-term technological war being waged presently by Washington and Beijing and that the EU cannot afford to have a subservient position in this confrontation and that laying a strong foundation is crucial if the strategic ambitions of achieving technological sovereignty are to be achieved in the next twenty years (European Commission, 2020)

It is also important to note that while achieving technological sovereignty is constantly stressed upon as a strategic objective, the EU does not wish to achieve to do the same through isolationism, but through continued global engagement. However, the nature and orientation of the engagement must be in primary consideration of the future of EU citizens, and that the aim of achieving autonomous agency in the technological domain is not possible without the development of European technologies and their alternatives(ibid.) The strategic focus also views technological sovereignty in terms of computing power, control over data and securing connectivity channels(ibid.)

US presidency under the Donald Trump administration that was in office from January 2017 till January 2021 and during this period, strategic rivalry between Washington and Beijing embedded itself in the technological domain (Odegaard, 2021) The aspect of central contention was the one regarding the standardizations governing boundaries for technological usage, especially the type as well as restrictions on access to the same outside of the established boundaries(ibid; p.1) The concerns pertaining to security threats presented by Huawei regarding data access to the Chinese government and dominance of American big tech firms like Facebook(ibid.) Standards is one theme that is at the centre of strategic competition, especially the geographical jurisdiction of regulation regarding the inflow of data where, the EU has increasingly scrutinized behaviours of both American big tech firms such as Facebook on collection of social media data and as well as Huawei regarding its telecommunication and network practices on the suspicion of data access to the Chinese government (ibid.)Thus, the EU has conceptualized that in order to take the first step towards achieving strategic autonomy, cognizance must be taken about a high degree of dependency on external actors from the likes of United States and China and take policy measures to reduce what it considers as over-reliance alongside establishing instutionalised regulatory mechanisms.

EU's approach to laying the fundamental framework to seek autonomy in its quest for strategic autonomy is demonstrated by emphasis of identifying dependencies in what it defines as critical sectors, with technology identified as one the latter. The strategic dependencies report defined dependencies as the sectors on which the EU relied upon a limited number of actors where data infrastructure and technologies were categorized as areas with a limited capacity for internal production (European Commission , 2021) In this report, technology was sub categorized as a sector of strategic dependencies that is differentiated from other dependencies through a specific mention of critical sectors, that included the latter alongside security, safety, health and digital transformation(ibid; p.7-8) In the global context, the EU makes a clear distinction between external and internal dependencies, where the former categorises countries and firms that operate outside the EU single market on which Brussels fulfills its requirements (ibid; p.8) The report analyses the EU's performance index in the domain of Key Emerging Technologies (KETs) that highlights the it's geo-strategic vulnerability in the technological domain.

This is further re-enforced by the report's findings in relation to EU's competitive position, which it states to be weaker than the likes of United States and China in the particular digital ecosystem of Artificial Intelligence, High Performance Computing, Big Data and cloud services (ibid; p.41) These inadequacies can also be revealed as the key driver of EU's strategic policy discourse towards strengthening its critical digital infrastructures as a key constituent of its strategic ambition to attain technological sovereignty.

EU Approaches to Technological Sovereignty

In order to address these dependency gaps, EU has conceptualized a multitude of approaches to push forward with its vision of technological sovereignty that (a) Seeks to expand its global technological footprint through an external projection of its market power of its ecosystem and (b) Adopts institutional norms to ensure that European firms are accorded a level-playing field and are accorded favorable operational conditions that allows them to thrive domestically. To achieve these goals, the EU has sought to employ a mix of offensive and defensive approaches to technological sovereignty. The offensive approach consolidates the vision by a combined institutional effort of promoting research with industry that seeks to reduce dependency on third countries through mastering and bringing about strong innovation in key emerging technologies that include- (1) Advanced Manufacturing, (2) Nano Materials, (3) Life Science Technologies (4) Micro/Nano Electronics and Photonics (5) Artificial Intelligence (6) Security and Connectivity Technologies (European Parliamentary Research Services, 2021; p.3) Assuming the role of a global standard setter in technological governance and establish a strong industrial technological base to adapt to future vulnerabilities and therefore, views the latter as a means of enforcing strategic autonomy(ibid.) While securing a strong technological and industrial base is highly emphasized, the EU seeks to influence tech co-operation in terms of how it defines its economic and geopolitical interests and avoids any strategic discourse that tendencies of technological isolationism. It seeks to transform its role in a globalized interconnected environment from solely a consumer to a major player whose decisions carry enough weight to influence technological policies across the world in co-operation with other international partners.

Brussels' defensive approach to technological sovereignty seeks to ensure protection for Europe's indigenous firms and technological systems developed by member-states, which stems from the long-term of critical digital sector by non-European players(ibid.) The attempt to curb digital hegemony of firms such as Apple, Google and Amazon by launching anti-trust investigations and pushing for a strong regulation of EU's digital market through stronger norms for to ensure secure data governance(ibid.)

A striking feature of the defensive approach, is also that the strategic discourse strongly re-iterates a disdain isolationist tendencies similar to an offensive approach and the rationale for the former is suggested to be the retaliatory measures from the third countries(ibid.) Thus, the element of anti-isolationist restraint in approaches to technological sovereignty demonstrates the limitations in current technological ecosystem as transfer of technical knowledge is still essential to bring about a balance that not only leads to a stronger power projection in the digital and technical sphere, but also ensures that Brussels continues to be a beneficiary of knowledge transfer that could strengthen EU's pan-continental technological influence. One of the most significant developments in recent years that reflects a high degree of assertion in EU's strategic discourse concerning global technological governance, is an increased frequency of documents relating to its policy framework that highlights a policy orientation where the ambition of autonomy has been the most reflective of Brussels' offensive and defensive approaches to technological sovereignty.

Some of these initiatives and policy projects include the General Data Protection Rules (GDPR) Cybersecurity strategy and the White Paper for Artificial intelligence. The White Paper on Artificial Intelligence seeks to establish a regulatory framework that seeks to uphold human agency and its respective oversight, improve technical robustness to improve operational safety and ensure that a high degree of transparency and accountability are maintained and the data governance norms of Artificial Intelligence conform to EU's fundamental right to privacy (European Commission, 2020) The paper also mentions the incorporation of these norms to build an ecosystem based on trust and excellence demonstrates not only a pro-active engagement in the technological governance, but also illustrates the magnitude of intent in the offensive approach in assuming the leadership to export this values-based technological system globally(ibid; p.3-4)

In addition to the White Paper on AI, the EU's instituitionalised discourse on cybersecurity does convey a similar discourse about demonstrating a high degree of commitment to a free and open cyberspace, it also stresses upon building an autonomous ecosystem of network and information ecosystems through the establishment of Digital Innovation Hubs and assume technological leadership (European Commission ,2020)

Since reducing dependency has been a central standpoint of the discourse regarding strategic autonomy, there also have been calls for diversification of external trade and in case of addressing external dependencies, availability of multiple trading partners is integral for the development of a strong technological base in the wake of bi-polarity in technological competition, the nature of this engagement provides a strategic opportunity to strengthen the existing functional market(European Commission, 2021; pp.42-43) On the other hand, the EU should strengthen its own capacity in strategic areas where necessary, building on the strengths of a fully functioning Single Market with open and competitive markets. In the external dimension of its industrial policy, it has also been recommended

that the diversification of import sources is a key element when it comes to increasing the EU's resilience in a context of global uncertainty and growing international tensions (ibid.) A strong EU engagement in multilateral cooperation and coordination mechanisms is important for this, including when it comes to preparing for a future crisis. At the same time, companies themselves play the key role in this regard as they are able to assess risks and take action so that they are able to tap into a sufficiently diversified and environmentally sustainable set of suppliers(ibid.)

Thus, the diversification of trading partners provides an ambiguity between offensive and defensive approaches that is not only able to reduce dependencies arising from hegemony of a few dominant players in the technological domain, but also simultaneously demonstrates an image projection of the EU's continued engagement through multilateral institutions and is able to downplay the magnitude of protectionist rhetoric in the same. The Multi-lateral Policy measures to address external strategic dependencies can be diverse

3. Platform Governance & Regulation in Transatlantic Relations: A Case Study of GDPR

European conceptions of Technology Through 3C's

One of the key pillars that influences EU's approach to technological sovereignty, derives its source from its cultural perception of technology, where its image projection is based on the rationale of Europe being a different actor from other parts of the globe requires a proactive approach in defending its values and market regulations- especially in the matters of data protection rights (Bauer & Erixson, 2020) Thus, a key constituent of this strategic outlook is digital regulation, where the human rights occupy greater precedence over business and interests(ibid.) The second aspect that underlines this approach to strategic autonomy, is the command-and-control views of technology- which believes that the orientation of policy instruments to govern practices in digital economy and cyberspace should either be in a collectivized control of EU as a supranational organisation and alternatively, member-states be granted agency in domain of intervention pertaining to usage of digital devices by citizens and companies alike(ibid; pp.13-14)

The command-and-control perception has also acquired a political dimension that dictates the policy for scrutinization vis-à-vis establishing a regulatory framework especially regarding the behaviour of digital platforms that collect data generated from EU territory(ibid.) The rationale for this framework has also been derived from a high degree of reliance of EU citizens and businesses on foreign firms, which is also considered as a threat that undermines European data integrity, with domestic forms and public institutions being at the receiving end of this threat(ibid.) The lack of a domestically designed digital platform ecosystem is also stated as one of the key reasons for this over-reliance and therefore, state-led interventionist approach to digitalization is being viewed as an instrument to ensure accountability, with the EU's adopting a collectively institutionalist mechanism in its regulatory framework(ibid.) While the digital revolution has led to the proliferation in the mass usage of communication technologies, the EU believes that the latter has reduced the global competitiveness of technological capabilities of its member-states in comparison to other actors (HEIKKILÄ, 2020) As a result, this adds to Brussels' concerns that potential subordination due to reduced capabilities in order to influence global markets and technological is detrimental to its position in the global order(Bauer & Erixson, 2020; pp13-14) This is highlighted especially in the case of blue-chip firms, who have a high degree of dependency on data and other services from foreign businesses(ibid.)

The fundamental structure of EU's technological governance, can therefore be conceptualized through a rational that digital regulation is a key instrument in ensuring that business operations by firms and third countries adhere to the human-rights based agenda. This can also be interpreted in terms of addressing dependencies especially in the matters of platform governance, where the EU has a degree of dependence on American platforms, which in recent years have been categorized as the Big Tech. This has significant implications on Transatlantic ties between Brussels and Washington, as EU's assertion of technological sovereignty in its regulatory framework has also been a source of friction between the two, especially on the matters of data sharing.

Divergent Positions on Data

In the Transatlantic relationship, this clash arises due to a highly divergent position of how the EU and US conceptualise their fundamental rationales of technological governance- with one of the key domains being their respective approaches to cybersecurity. The EU approach to cyberspace can be viewed as a legalistic one that seeks to counter cybercrime through which it legitimizes its needs for Cyber Defence and thus, integration of cybersecurity as an instrument of soft power projection, leading many experts going as far to define EU's technological credentials as a civilian cyber power (Christou, 2016) In addition to the same, the EU's rationales for the development of its cyber infrastructure as not in terms of offensive capabilities and defending its cyber perimeters(ibid.) This represents a contradiction in regards to its offensive approach to technological sovereignty that conceptualized innovation and investment in creation of autonomous digital ecosystems as a key constituent of the latter approach. Instead, the approach comprises of a framework that advocates flexibility in terms of ecosystem operations and differentiation of regulatory responsibilities between multiple stakeholders(ibid.)

Thus, the emphasis on regulatory mechanisms vis-à-vis Transatlantic relations demonstrates that EU has adopted a defensive approach to technological sovereignty vis-à-vis its technological relationship with the United States. The American perceptions of cybersecurity have been defined in terms of (a) Protection of important information systems as a constituent of critical infrastructure from cyber threats. (b) Enhancing the ability to improve identification and responsive capacities (c) Engagement with international partners to uphold internet freedom that is achieved through a secure cyberspace with a high degree of interoperability (d) Protection of federal networks by ensuring accountability of agencies while achieve cybersecurity targets and lastly (e)- Investment in developing a strong cyber-oriented workforce in designing an architecture through joint public-private partnership(ibid.) Thus, the sources from which Washington derives this intended policy framework can be traced as: (1) Complete government approach (2) Prioritisation of Network Defence (3) Ensuring privacy and upholding civil liberties in the digital sphere (4) Public-Private engagement (5) International co-operation and engagement. (ibid.)

American Rationale for Securitisation of Cyberspace

While the official American policy in regards to cyberspace projects the incorporation of cybersecurity governance based on institutionalised co-operation between public and private actors that seeks to defend critical infrastructure, the divergence becomes evident through the US establishment's dominant perception that dictates cyber policy is derived from threats to national security(ibid.) The strategic discourse that first highlighted this divergence was the Commission on Cyber Security in its 2008 report that mentioned cybersecurity as a national security concern and subsequently re-enforced under the Obama Administration, which institutionalised cybsersecurity in equivalence to military security by incorporating pre-emptive attacks(ibid.) This is reflected by the convergence of previous task forces into what is now known as the US Cyber Command (USCYBERCOM) and as a hierarchical system of functioning, USCYBERCOM had to report cyberspace matters to US Strategic Command.

The USCYBERCOM functioned in a defensive capacity through the Computer Network Defence operations that were established to co-ordinate defence operations against Cyber Attacks and (B) Cyber Attack Operations for the purpose to enhance offensive capabilities(ibid.) In the strategic discourse concerning aggression, the American strategic objective achieving deterrence in cybersphere is based on creating a climate of fear through institutional militarization of cyberspace through enhancement of capacity as well as strength, in addition to the lack of feasibility that exists to differentiate between what can be termed as attribution or retaliation(ibid.)The extent of militarisation of cyberspace in the Washington's strategic discourse on cybersecurity can be demonstrated by establishment of 13 teams of cyber agents whose sole objective is to mount offensive cyber-attacks against states and actors that carry a high degree of threat perception. Some examples that demonstrate that further demonstrate the development of US offensive capabilities in cyberspace include reports of the National Security Agency (NSA) exploiting what are called zeroday vulnerabilities and subsequently injecting specifically designed malware to strategically disrupt adversarial internet infrastructure(ibid.) To further exploit the vulnerabilities, the US security establishment has deployed mechanisms to specifically circumvent encryption standards to increase the efficiency of the offensive cyber capabilities(ibid.) NSA has bought and exploited 'so-called zeroday vulnerabilities in current operating systems and hardware to inject NSA malware into numerous strategically opportune points of Internet infrastructure' (Ibid.)

In addition, it has also been revealed that US government resource deployed to crack existing encryption standards has contributed further to the very vulnerability of those encryption systems(ibid.) This also caused a heated domestic debate in relation to the impact on intelligence gathering practices with data collection by the US government and security agencies in particular, in their justification of cybersecurity being a serious national security threat(ibid.)

Therefore, it can be stated that the conceptualization of how Washington has developed its technological capabilities in the digital sphere, is based on a high degree of securitisation of cybersecurity compared to the European Union. In addition to the same, it is important to highlight a key difference that is reflected in how the EU and US conceptualise offensive capabilities in cyberspace in their strategic discourse. While the EU's offensive approach to technological sovereignty as reducing dependency on third countries for establishing an autonomous digital ecosystem. Its cybersecurity strategy does not make an explicit mention of launching offensive cyber capabilities and instead asserts a high degree of emphasis on prevention, deterrence and responding to aggression in cyberspace (Christou, 2016)

The hierarchical interlinkage of U.S-based digital platforms with the American intelligence agencies demonstrates a high degree of securitisation of civilian digital spheres which lies in complete contradiction to EU's framework of digital governance, that consider civilian liberty as paramount object of reference in its objective of achieving technological sovereignty. In addition to the high degree of securitisation of cyberspace by the American establishment, the EU's assertion of strengthening its regulatory framework can also be derived from a high degree of global dependence on American digital platforms as online communication mediums that remain highly concentrated in the US. A key reason behind the cause of friction in Transatlantic relations in domain of internet governance arise from EU's perception of functioning of American digital platforms and the nature of threat imposed, concerning the matters of Data sharing and privacy.

Role of Platforms as Techno-Political Agents

The functioning of platforms tends to acquire a multitude of commercial identities, where they are said to possess features of both firms and markets that facilitate a simultaneous process of production and exchange (Dijck & Nieborg , 2019) This has been a gradual evolution in cyberspace where having performed the initial role of connectors, these were also able to circumvent regulatory frameworks and since many have also expanded their global operations in a short span of time, many have also built multi-sided platforms(ibid.) However, the concentration of a selected few firms tended to concentrate market power and create a digital arena which often mirrored the behaviour of an oligopolistic market structure. These mediums are also described as corporate platform elite that have assumed primary control of gateways to digital markets(ibid.)

What has also been subjected to as one of the key reasons about how the digital platforms have been able to transform as important strategic players on the global stage, is the capacity to rapidly develop and establish technological and economic standards that govern platform mechanisms(ibid.) In addition, the development of these platforms is also strategically designed to accumulate power by leveraging global diffusion(ibid.)

Platforms as Gatekeeping Agents

While these advantages enable platforms to increase their operational efficiency in regards to maintaining a transnational presence, it also has been a matter of widespread concern with regards to the platforms to dictate the flow of data and use the same as an instrument to recombine and re-use for algorithm-based innovation(ibid.) Since these platforms have already established a dominant oligopoly in the digital market, they also tend to wield a high degree of power in terms of managing gatekeeping roles and subsequently dictate the direction of online traffic(ibid.) The oligopolistic dominance also tends to govern connective infrastructures, creating a high degree of dependency in the process for online activities and subsequently cause an interference in the society. This dependency also extends to platform linkages with reliant stakeholders such media outlets, application developers and advertisers, leading to imbalanced business relationships that require strict adherence to guidelines set by these platforms(ibid.)

Transnational Influence and Role of Platforms as Extended Arms of State Intelligence

Thus, technological relations with Washington represent a multi-faceted challenge for the EU which manifest themselves in the form of (a) The divergent approach to digitalization mentioned previously, describing the militarized securitisation of cyberspace which establishes linkage between American firms and US Security Agencies (b) The digital dominance in cybersphere being concentrated by the presence of American social media platforms, whose operations extend beyond US borders and facilitate the access of personal data of international users to the government. The EU also perceives that these corporations also act as extensions of US Government and those unregulated operations of the firms hinder digital safety of its citizens. Platform governance is an important domain in how their role has become increasingly vital in the global arena, since they have become mediums that facilitate exchange of information, networking, trade and commerce. They have also become increasingly embedded as an instrument of political influencing by consolidating their identity as a collective infrastructure of freedom of expression but also present a major limitation in terms of an operational sphere- that of them being private governance systems that the factors that influence their operations arise of a conflict between local, national and supranational factors of influence (Gorwa, 2019) The regulation of the social media platforms also arose due to discovery of PRISM, which was a tool

deployed by the NSA to collect private data from social media platforms and service providers such as Apple, Gmail, Facebook and others (Sottek & Kopfstein , 2013) Concerns regarding privacy were heightened when it was also reported that the NSA had direct access to the servers of these tech corporations and hence as a result, the debate regarding this practice also questioned the privacy ethics in the domain of data collection beyond US borders(ibid.) This event also provides an insight into the overlaps of the factors of influence mentioned by Gorwa, with the supranational nature of digital platforms being dictated according to the highly securitized perceptions of the US establishment and these perceptions being extended globally as well.

Measuring Platform Power Through Discourse Regulators

EU's official discourse also frames platforms as intermediary agents between contemporary politics and the civilian population and exercise a high degree of influence in restructuring public sphere (European Commission Expert Group For the Observatory on the Online Platform Economy, 2021) Digital social media and streaming platforms like Facebook, Twitter, Instagram and YouTube being viewed as gatekeepers has been derived from the behaviour of these platforms as custodians of a massive and heterogenous public sphere, also leading to claims that a selected few private companies from the Silicon Valley being the determinants of how global public spheres are maintained(Ibid; p.20-21) The influence is described through the dimension of how public discourse is shaped with terms of service and community standards being the instruments to exercise the influence(ibid.) The terms of service and community standards are also categorized as norms of technical, social and a contractual architecture, which functions as an agent that seeks to both enable and restrict public speech.

While digital platforms can be credited for maximizing outreach of both news media outlets and as well as user-generated content, this is possible only if both adhere to the terms and conditions enforced by the platforms. This agency is further weaponised by the platforms not only through personalizing content, but also through allowing the content to be viewed on the platforms and due to this process, the platforms have challenged the dominance of traditional mass media(ibid.) This has allowed platforms to present themselves as transformative agents that wield enough power to influence public opinion by capitalizing on the dependence of news media outlets using algorithmic calculations that determines relevance of the content. Since a very large demographic of the outlets' younger audience have an online presence on these platforms, the latter are able to create dependency that is able to influence operations of news media according to their terms of service to maximise the outreach (ibid; p.22) Hence, the transformation of online platforms as digital intermediaries due to the above-mentioned dependencies have also ignited concerns about the erosion of reporting ethics and subsequent weakening of editorial principles(ibid.)

Since these platforms also have a large consumer base, it allows them to mobilise attention towards amplification of discourse on certain topics, demonstrating a high degree of discretion in shaping online discourse through algorithmic tools of persuasion(ibid.) Thus, the EU's strategic discourse terms these digital platforms as political actors in their own right due to the high degree of influence that they exercise in shaping the public discourse(ibid.) Thus, the regulatory dimension of EU's technological sovereignty can be viewed from standpoint that perceives dependence of media outlets on digital platforms as external agents that interfere with domestic political discourse and undermine institutional legitimacy of state bodies through monopolizing their gatekeeping prowess and subsequently threaten press freedom by reducing the sphere of expression without restraint mechanisms in how the visibility of online content is determined.

EU Data Strategy as a Regulatory Instrument of Information Sharing

In order to ensure high degree of transparency, the EU has crafted its official data strategy that seeks to enforce regulation vis-à-vis data flows between businesses and state institutional bodies while protecting privacy and creating a feasible business environment. The first one is Government-to-Business Model (G2B) of data sharing (European Commission, 2020) Since the production of data is made available due to public funds, the sole aim is to maximise the benefit of the society. Initiatives such as Open Data Directive19 have been of immense benefits to small and medium enterprises (SMEs), alongside civil society organisations and scientists and regular reviews through evaluating public policies(ibid.) A major limitation that has been posed, is the unequal availability of quality datasets across member-states which makes the lack of accessibility for the SMEs (ibid.) It is also worthwhile to note that data-sharing of governments with big-tech companies has not been addressed in this institutional discourse, further enforcing EU's threat perception vis-à-vis foreign companies that also wield a high degree of economic power. The lack of mention of big tech also demonstrates ambiguity and the cognizance of a situation where policy framework can be perceived as confrontational by foreign firms and potentially harm European business interests. This mechanism also highlights a differentiated regulatory approach, especially in regards to SMEs and Big Tech, further re-enforcing the threat perception as a rationale to pursue technological sovereignty. Since certain datasets also tend to carry a high degree of sensitivity to be made available to businesses for research purposes, the EU's data strategy stresses upon regulatory mechanisms, to establish checks and ensure compliance with respect to data privacy (European Commission, 2020)

The Business-2-Business model of data sharing is often considered to have strong economic potential, but has not been widely successful at a larger scale due to lack of economic incentivization to convince companies to do the exchange data, due to the fear of losing a market competitive edge(ibid.)

Alongside the apprehensions about loss of market share, the imbalance is prevalent due to the terms of negotiating power with economic operators and misappropriation by third parties and ambiguity in legal framework regarding usage of data, especially concerning the set generated by Internet of Things(ibid.) The Internet of Things (IoTs) can be defined as the network comprised of physical objects embedded with sensors, software, and other technologies, for the facilitating data exchange with other devices and systems on the internet (Oracle , n.d.) The official policy in this model does not highlight the nature of data exchange between the scale of enterprises, but makes an inference with regards to the presence of third-parties and also demonstrates the cognizance taken by the EU about the presence of third-parties and IoT networks functioning outside of its geographical and legal jurisdiction (ibid.) The model can also be understood as an instrument that is highly beneficial to the EU's digital ecosystem through informed insights obtained by data shared from dominant companies from third countries. Therefore, the business-2-business model of data sharing can also be understood as pathway to achieve economic parity vis-à-vis non-European competitors, that could also provide future policy framework for the member-state governments for aiding the development of a private industrial European digital ecosystem that is robust and autonomous to challenge contemporary oligopolistic market dominance of U.S. big tech firms.

Lastly, the Business to Government model (B2G) has been framed keeping in mind the lack of datasets obtained from private sector, that could be regarded as a valuable asset in terms achieving of evidence-based effective policy evaluation in the wake of contemporary societal developments (European Commission, 2020) This model also demonstrates that the EU has taken strong cognizance of influence exercised by foreign businesses and using the rationale of securing data of its citizens who use services of foreign firms, to normalise what it terms as a data-sharing culture and thus enforce accountability(ibid.) In its policy discourse, the EU frames the establishment of a regulatory system as utilisation through re-using privately-held data for what it defines as public good(ibid.)

GDPR as Institutionalised Data Regulation in Cyberspace

Deriving the rationale from the concerns presented in the models that demonstrate the nature of data-sharing between governments and businesses, one of the most ground-breaking policy frameworks that the EU has recently undertaken in recent years to curb the influence of social media platforms, is the GDPR-Which is defined as the General Data Protection Regulation. Considered the toughest privacy and security law in the world, it places multiple obligations on organisations irrespective of their location and subject them to mass public scrutinisation when their data collection practices are targeted towards EU citizens (Wolford, n.d.)

First implemented in May 2018, the regulation has sought to levy harsh fines in situations where corporate organisations are found violating the privacy and security standards(ibid.) The EU derives the GDPR's framework to establish privacy standards from the 1950 European Convention on Human Rights that gives every individual the right to privacy in the personal, familial and residential aspects of their lives. The aspect of regulating foreign businesses has been addressed in the Article 3.1 of the regulation that applicability of GDPR extends to firms and organisations that run their operations in EU territory even the data is stored outside the latter(ibid.) Article 3.2 also extends GDPR for scenarios where organisations not running operations from EU territory provide goods and services to EU citizens or are involved in monitoring online behaviour (ibid.) This demonstrates that geographical influence of Big Tech especially in terms of influencing public discourse online is a key element that has shaped Brussels' threat perception regarding Big Tech enterprises.

Article 5.1-2 of the GDPR has drafted seven core principles of regulation to ensure protection and accountability that (a) Emphasize that the processing of data subject must be conducted in a manner that is lawful, fair and transparent (b) The data processing must be conducted for the legitimate purposes as specified explicitly to the subject during the time of data collection (c) Data collection should not cross the required threshold mentioned for necessity and should not be excessive (d) Accuracy of the data should be maintained at all costs and be updated regularly (e) Storage limitation should apply- that identification of data should not be stored beyond the completion of the purpose (Wolford, n.d.)

US Govt and Big Tech Backlash Against European Data Regulation

While the current data protection and privacy measures introduced by the EU have garnered mass support among its citizens, these rules have also been subjected to mass criticism from Washington, which has accused Brussels' framework of data protection measures being protectionist in disguise. American enterprises have added to the criticism of regulatory policies as well, citing what they term as unreasonable restraints on their business activities, especially in regards to the compliance costs that now have to be added as an adaptation process to the measures (Bradford, 2020) These compliance costs have arisen in terms of extra labour and financial investments, with the key example of Google stating that it had to invest hundreds of hours of extra human labour to make the organizational and operational spheres more compliant with the GDPR regulations(ibid.) It was also reported that American companies in Fortune 500 group incurred an expenditure of 7.8 billion US Dollars in their operational adjustments as a part of their compliance with the regulations as well(ibid.)

While the financial expenditures and extra labour investments alongside criticism from the American political and business establishments demonstrate a certain degree of discontent, the adjustment of operational and organizational policies in compliance of the data and privacy regulations to European norms highlights the importance of EU as highly strategic instrument in terms of economic and regulatory power projection(ibid.) The criticism of GDPR can also be framed as second divergence that stems from differentiated depths of regulatory divergences present in a multitude of business and technological spheres in both the US and the EU. Taking into account this differentiation, the American legal framework on data privacy is categorized to be far weaker than that of Brussels, since the magnitude of state regulations remain restricted to certain public and some classified sensitive sectors that include healthcare alongside banking and other financial infrastructure (Bradford, 2020) The privacy policy framework in the private sector is guided solely by self-enforcement through self-defined industrial norms and individual organisations are granted liberty to create privacy policy as per their own norms and the contract between consumers and the companies on the level of privacy desired becomes a domain where the state does not interfere between the negotiated consent between both parties(ibid.)

The US government in the view of its technological governance, has not established a separate institution that can exercise independent regulatory authority to enforce privacy rights like the EU has done. Alternatively, the issues pertaining to data and privacy have been broadly been assigned to mandate of Federal Trade Commission which undertakes responsibilities of consumer protection and acting against unfair practices regarded as deceptive and unfair that have the potential to impact commerce (ibid.) This divergence again re-enforces the differentiated policy perception of data that shapes the American and European strategic framework with regards to privacy respectively. EU's policy framework concerning privacy has been designed around a rights-centered discourse where individual identities as data subjects have been guaranteed a high degree of protection (Bradford, 2020) In contrast, the discourse in the US is designed to be marketplace oriented and where consumer rights are commercially oriented around data commodification- which means that the individual consumer has the liberty to trade personal data as a commodity without strict public scrutiny by state institutions(ibid.) This is also a marked difference from EU's approach where right to privacy is considered fundamental to an extent that Brussels considers it to be one of its key identitarian facets of its governance model and through enforcement and compliance of GDPR, it seeks to assert the same norms into the wider digital and cyberspace domain.

Beijing's Technological Rise as an Alternative Player

While there have been differences and divergences between Brussels and Washington regarding a mutually agreed framework of data and privacy, the convergence in transatlantic alliance on the matter of technological governance is showing signs of strengthening due to one common factor- That is, China's rapid rise in the global technological order and the mutual threat perception of Beijing emerging as a potential hegemon and posing a strong challenge to Washington and Brussels in the contemporary technological landscape. Beijing has launched a series of initiatives that demonstrate its global technological ambitions that have caused concerns in the Transatlantic alliance. As a key component of its Belt and Road Initiative, the Digital Silk Road Project was launched by China in 2015 and has generated close to 15 trillion US Dollars to enable Chinese companies in acquiring strategic advantage in the Middle East, Africa, Latin America and Eastern Europe (Torreblanca & Jorge-Ricart, 2022) A key reason that dictates EU to seek technological co-operation with Washington, is the perception of Beijing's economic power projection in Eastern Europe- representing a threat to its geo-strategic influence in its peripheral region and potentially presenting a challenge to its economic enlargement project(ibid.) Washington and Brussels have also been strongly criticised due to their negligence that allowed Beijing to build its own digital sphere of influence by providing assistance to countries in the Global South in terms of developing communication infrastructural systems and specialised Artificial Intelligence surveillance capabilities with Huawei alone being the provider of AI-based technology to fifty countries(ibid.) In addition to the latter, China has also provided training to impart technological expertise in terms of censuring and monitoring internet in real time. Through its industrial initiatives such as Made in China 2025 and China Standards 2035- Beijing has sought to project its strategic ambitions to become a powerful player by creating and subsequently dominating global technological standards by achieving technological independence from the Western world(ibid.) Internationally at the state level, China has also demonstrated its strategic ambition to attain a strong influence in international bodies such as International Telecommunication Union (ITU) and United Industrial Development Organisation (UNIDO), signalling an intent to also position itself as a global regulatory power in technological regulation(ibid.) Thus, these initiatives reflect Beijing's strategic ambition of asserting itself as a global technological player at a multitude of levels by- (a) Expanding its digital sphere of influence through creation of technological dependencies in the developing world, where the private sector is a key strategic instrument in advancing its global technological projection. (b) Establish a strong industrial base to attain technological autonomy from the West and establish norms based on self-devised technological standards for industrial production to challenge Western hegemony in the domain (c) Export its defined norms by asserting its position as a global regulatory power in the international technological order through acquiring a high degree of influence in multilateral regulatory institutions in the matter of technological governance(ibid.)

Trade & Technology Council as a common Transatlantic Forum and an Institutional Response

The EU has anticipated the challenges that would be posed by China's rise in the international technological order, especially in regards to its geopolitical influence through technology and this has prompted Brussels to seek greater co-operation with the Washington to counter the same. While threat perception of China in its strategic discourse is not explicit, the EU has sought a collaborative approach with Washington to assert its technological leadership while simultaneously tackle the strategic challenge posed by Beijing. A major step towards institutional convergence was taken through the establishment of the EU-US Trade and Technology Council (TTC) The establishment of TTC has been described as a common forum for the EU and the US to co-ordinate policy approaches to trade, economics and technology domains and enhance the existing Transatlantic alliance based on mutual values of liberal democracy (European Commission, 2021) Among its working groups, the ones specialised in technological governance are categorized as : (a) Technology standards cooperation (including AI and Internet of Things, among other emerging technologies) (b) Data Governance and Technology platforms (c) Promoting SME (Small and Medium Enterprises) access to and use of digital technologies (d) Misuse of technology threatening security and human rights (ibid.)

Institutional Co-operation alongside divergences

The establishment of TTC demonstrates EU's strategic ambition to assert technological leadership through initiating a dialogue with the United States. This includes the global development of secure 5G infrastructure alongside ensuring security for digital supply chains through formulating a framework of objective risk-based assessments (Commission, 2020) Brussels also states that a shared interest with Washington in cybersecurity co-operation building through situational awareness, information sharing channels and building mechanisms for preventing attributed attacks from what it calls third countries. Brussels also seeks to extend this co-operation in the domain of AI technologies by furthering what can also be perceived a collaborative strategy for standardization(ibid.) To materialize the same, the EU has also proposed a Transatlantic AI agreement that adopts what it calls a humancentric approach to advance a collaborative leadership in establishing blueprint models for global technological standards modelled on shared democratic values(ibid.) The mention of shared democratic values is an important standpoint since the latter can be framed as a source of legitimacy for the collaboration, by projecting China's values in contradiction with EU's human rights agenda that takes a firm stand against securitisation of free expression and asserts the right to privacy as a fundamental tenet.

While, there is an acknowledgement of policy divergences on the issue of data governance, Brussels asserts its commitment to the Transatlantic partnership to create constructive solutions to overcome these differences through multilateral regulatory mechanisms. The EU makes a direct reference to online platforms and extends the possibility of collaboration with Washington by proposing a transatlantic strategic dialogue regarding their role, projecting a sense of mutual threat posed them to their democratic systems. It can be inferred that the EU has crafted a strategic discourse that deploys a persuasive approach to Transatlantic diplomacy, by legitimising the threat of unregulated digital platforms of manifesting them through harmful market behaviours that undermine existing liberal and democratic norms.

EU's 5G Policy vis-à-vis China: Analysis of Threat Perceptions and Divergent Discources

The initial period of bilateral relations between China and the European Union in the twentieth century were based on limited political and economic interactions, leading both parties to consider themselves as distant neighbours at best (Yahuda, 1994) While Beijing established official diplomatic relations in 1975, it was only in 1998 where common forums with Brussels were regularly shared and a major development in diplomatic relations occurred in 2000 when the EU conducted successful negotiations with China to facilitate its accession in the World Trade Organisation (WTO) (Liang, 2021) Soon after Beijing's accession to WTO in 2001, bilateral ties witnessed massive growth as the two announced the establishment of a "Comprehensive Partnership", that was further upgraded to the status of a "Comprehensive Strategic Partnership" in 2003(ibid.; p.52) Since then, the EU has elevated itself to become Beijing's leading trading partner, with Brussels being one of the highest contributors of Foreign Direct Investment (FDI) along being its largest supplier of foreign technology and equipment(ibid.) Economic relations continued to prosper as bilateral trade between the two grew at an annual average of 40% with this translating into a greater outlay through exploration of other common interests alongside cultural and diplomatic visits(ibid.) This also sets the framework for what can be classified as evolution of China- EU relations over the years. The period from 2003 to 2004 is often regarded as the Honeymoon Period for China- EU bilateral diplomatic ties as relations witnessed upgradation to a status of Comprehensive Strategic Partnership (Li et. al, 2017) In one of his visits to EU headquarters in May 2004, Chinese Premier Wen Jiabao addressed the EU headquarters and subsequently stressed that the comprehensive partnership between Beijing and Brussels extended to a wide-range of multiple domains and the strategic importance of the partnership was built for long-term and would bring about stability(ibid.) He also emphasized the mutual benefits of bilateral and as well as multilateral co-operation where both China and EU work as equal partners to achieve these goals(ibid.)

End of Honeymoon Period and EU's mistrust of Beijing

The time period from 2005 to 2008 is often described as the period of strategic adjustment in bilateral relations. From 2005 onwards, the EU had begun to harbour suspicions of China's increasing strength and its global standing and began to shift its policies towards a tougher diplomatic stance, leading to increased frictions in the relationship (Zhou, 2009) It is during this period when the EU mentions China as a fellow competitor in addition to being a partner, signalling a stark contradiction from previously viewing China as a strategic partner(Li et.al; pp 37-38) The documents published in October 2006 titled EU-China: Closer Partners, Growing Responsibilities and EU-China Trade and Investment: Competition and Partnership in the form of a communication alongside a working paper re-iterated a

strong commitment to bilateral relations and the avenues for bilateral co-operation, but also stressed on the presence of competition and laid emphasis on China's responsibilities in the framework of bilateral ties(ibid.) To highlight strain in economic relations, the EU also published a policy paper stating that China's Trade and investment policy presented a strong challenge for Brussels and that main cause of this was the barriers imposed by Beijing regarding access of foreign firms to its domestic market, its policies on intellectual property, environment etc.(ibid.) It is also worthwhile to note that technology transfer is also mentioned as a key area of contention causing friction between Brussels and Beijing in these documents and this can be understood as a starting ground for the technological differences between the two.

5G technologies and Bilateral Ties

The element that is shaping up the contemporary strategic debate about EU's technological sovereignty and industrial policy vis-à-vis China, is the issue of 5G technologies. 5G can be understood as the fifth-generation standard that governs the technological framework for broadband-based cellular networks (Kenyon, 2020) It is an upgradation from Fourth Generation technological standard that also enables the integration of other next-generation technologies such as Internet of Things to accelerate speed of connectivity and volume of information exchange over broadband networks(ibid.) The umbrella of 5G technologies extends beyond inter-handset and data communication and has been equipped with the capability to facilitate data transfer between a large volume of devices such as CCTV cameras, refrigerators, cars etc, making them highly interoperable in the process of data and information exchange (Hoffmann, et al., 2019) It has also been termed as the technical foundation of the upcoming future that would become increasingly integral for daily life and would enhance the nature of contemporary political participation in the society (ibid; p.7)

Huawei as a Security Threat

While 5G is considered to be a major technological milestone in terms of enhancing internet connectivity across the globe, it has also sparked a debate about the security concerns regarding sensitive data sharing, especially regarding Chinese suppliers of the technology and their links with the Chinese Communist Party. The case of Huawei is a major subject of debate around Chinese market share of the 5G technologies. The US government has put forth a major accusation that Huawei along with ZTE- both being major communication equipment manufacturers, of carrying out espionage for the Chinese government and thus were classified as security threats as per a report that was published in 2012 by US House intelligence Committee (The Washington Post, 2022) These concerns were further elevated in the US national security discourse when the administration under then-president Donald Trump prevented a takeover that supposedly would have been detrimental to US investments in global wireless technologies and would have increased Huawei's global market share in 5G technologies disproportionately(ibid.)

Therefore taking the potential implications of data collection on a large scale, the US Federal Communications Commission in 2020 officially designated the companies to be potential national security threats and ordered American carriers to remove both Huawei and ZTE from their network operations(ibid.) The rationale behind the heightened threat perception of Huawei is converging one between multiple governments(ibid.) That is, they are highly apprehensive about the deployment of foreign-based technology that overseas manufacturers allow installation of backdoor channels for making sensitive data accessible to potential spies or be under legal obligation to hand over data to the respective national governments(ibid.) It was reported United Kingdom-based carrier Vodafone had discovered pre-installed backdoors in its Italy-based operations in 2011 and 2012 and while it was unknown whether this discovery was accidental or was the vulnerability deliberately planted, it can be understood as a major reason for Huawei to be considered a security threat for national governments(ibid.) This it can be stated that the EU's approach to technological sovereignty vis-à-vis China can be conceptualized as a part of the global backlash against Huawei. The EU's convergence with other countries on the basis on national security concerns serves as a major policy rationale for developing its technological policy in the domain of 5G Technologies.

Dependency and Risk in the context of 5G Technology

A key rationale that shapes the global threat perception in the Western world, is the potential weaponization of technological dependency in an oligopolistic market, where selected firms dominate the market share with lack of alternatives available (Radu & Amon , 2021) The technological system of 5G networks tends to function by enhancing existing legacy-based 4G infrastructure and in the contemporary times, and this grants a small number of service providers asymmetric competitive advantages in the deployment of communications equipment needed to establish upgraded networks (ibid; p.2) While 5G technology has been projected to have more security than its predecessors, it has also inherited a significant proportion of vulnerability from previous generation networks (Newman, 2021) While it is significant to note that no suspected breaches and potential equipment has been found to be publicly proven by Chinese private companies, there is an underlying assumption that guides this threat perception, that is- about China's rapidly growing global influence in the domain of ICT infrastructure and links of these companies with Beijing's intelligence agencies that causes security concerns(ibid.) 5G technologies have deploy a risk governance model that is based on comprehensive monitoring in the context of emerging technologies that present a new variety of threats, where the magnitude of risk is a key element that are taken into consideration for determining the proportion of protectionist measures implemented (Radu & Amon, 2021; pp2-3) The new threats presented in terms of 5G infrastructure presented tend to be unknown since technological upgradation at a constant pace, with many of them cannot be easily anticipated and avoided and recognition of this fact in the context

of industrial risk management can be countered through the integration of resilience and mitigation models to diffuse potential threats and protect important national assets (PwC, 2016)

Sources of Vulnerability in 5G Technologies

Since, the threats posed by 5G technologies tend to impact national security architecture of countries in a multitude of ways, politicization of these technologies is a product of threat perception that accompanies the rationale for determining the extend of political decisions. A key component that informs decision making in the context of 5G technologies, is the formulation of standards that are built and developed for deployment through software, hardware and other digital services (Hoffmann et. al, 2021; p.9) These standards are also designed based in the context of measures taken for public welfare that includes designing networks through an operational base of converging technologies, creation of legal framework to uphold standards of intellectual property and this also extends the policy architecture in terms of internet neutrality, regulation mechanisms for compliance in market competition and security concerns (ibid.) Since 5G-based technological networks connected a large number of devices on a mass scale and also facilitates data flows through different connecting equipments, it also increases the probability of events such as large-scale data and increases the susceptibility of espionage by external agents. Majority of the political discourse of governments around the world regarding 5G has been upholding confidentiality, integrity and enhancing the network efficacy in terms of information and resilience and in addition to the same, an increased focus has also been on ensuring protecting the services that 5G facilitates. It can be argued that a large variety of 5G-based connected devices also extends the threat perception in the form potential vulnerabilities that could be harmful for the civic infrastructure. Since physical network components, internet protocols and cloud-based technological systems form the basic building block of 5G technologies, these being placed at a lower stack level increases the vulnerability of 5G-based technological systems, compared to other communication networks. 5G technologies are designed on the convergence of computing and communication-based networks that are maintained by data centers which carry out configuration operations to maximise efficiency by making the networks to be highly responsive instead of static. This pushes network intelligence at the edge of what is defined as the core network, increasing the threat of censorship through exerting control of specific network segments. This is achieved by not restricting access to the internet in its entirety, but through the isolation and targeting specific locations, institutions and business both in civilian, public and private infrastructural domain.

5G networks have made carriers transition to business models in the internet and mobile sectors in terms of replacing physical infrastructures with cloud-computing systems that are connected by fiber cables and radio waves. In addition to the same, the operations of 5G networks will be under the control of more Software Defined Networks (SDNs) and data processing centers that are run by other private players. Here, business-to-business (B2B) service models are given more emphasis over individual consumers and therefore, increase the risk of certain companies getting unfair advantages over others in terms of speed and service, increasing the threat of potential erosion of consumer rights.

Competition policy is a major determinant of the 5G governance framework in terms diversification of services provided to consumers and as well as providers. As service provider roles have begun to assume more economic importance over network providers, this has led to the creation of vertically integrated business models where operations between hardware, software and network management services are regulated by an organisation that serves as an operator. This virtually removes the demarcation between differentiated services. Since Huawei is considered to be economically strong enough to deliver both network connection services and sale of specialised devices that enhances its market standing both in terms of business and consumer-oriented services. Since asymmetry exists in terms of market power projection for different firms in terms of investment for improving infrastructural capabilities, this shift also poses a threat to re-enforce monopoly of a few selected firms in the global 5G market share. In this scenario, the multi-dimensionality of the services delivered by the operator also has been accorded the discretion in terms of reducing effectivity of other players that they might see as potential competitors in certain sectors.

The Opaque Nature of Chinese Public & Private Organisations

Chinese government's policies in regards to providing support for technological innovation, management of its domestic markets has often been scruitinsed as a part of its wider policy of what is often termed as political engineering (Hoffmann, et al., 2019) China's authoritarian single-party system is also reflected in its approach to managing internet, which often constitutes of highly pervasive surveillance systems that has also been touted as the government's micromanagement of the internet(ibid.) As a part of its digital ecosystem, industries and government's co-ordination with each other is often conducted in a very opaque manner, blurring the lines between civilian and military interlinkages(ibid.) Huawei is often projected to be significant market player that also acts a carrier for Beijing's policies on data and cloud-based infrastructure and accounts for 40 % proportion of the domestic market share. The degree of coercion that shapes China's authoritarian approach to internet governance, is meant to be an instrument of coercion for firms that do not demonstrate adherence to the Communist Party's framework of internet which causes the government to apply pressure to support other competitors(ibid.)

The case of Lenovo initially choosing to vote for Qualcomm that is American-origin technology, but later backtracking from it illustrates the Beijing's influence on industrial decisions and projection of Huawei's standard can be viewed as a policy that higher degree of industrial adherence in digital sphere for companies is rewarded by an increased market share to transform a firm into a dominant actor(ibid.) Another factor that further makes the line between public and private enterprises further invisible, is investment of financial capital through the channel of state subsidies and multiple funding outlets in the form of venture capital, private equity-based investment and capital generated from stock market(ibid.) These alternative sources of funding also use their financial clout as a soft-power influence to influence decisions taken by private firms and therefore, this has also ignited concerns about business climate in China with regards to covert mechanisms being deployed to grant asymmetric market advantages that also has the potential to impact Beijing's diplomatic ties with the Western world(ibid.)

Taking cognizance of these suspicions, Huawei has sought to quell this narrative by regularly releasing statements about the demographics of its workforce and the company not having any government officials in its core board in its attempt to deny links with the Chinese government(ibid.) However, these claims have been contradicted strongly as the findings of Huawei's investigation by US government in 2012 showed that the company's internal documentation was classified as state secret and there was indeed a presence of a Chinese Communist Party committee within the organisation (Hoffmann, et al., 2019) In addition to the same, China prevented a review by World Trade Organisation (WTO) about its market economy status in 2019, which has further increased Western skepticism towards the secrecy that surrounds the interlinkage of private and public entities, making it increasingly difficult to decipher the separation between the two(ibid.)

The growth of the private enterprises in China can be understood as a result of a series of strategic policies undertaken at the national level that have sought to provide a feasible environment for fostering promoting and protecting the tech sector over the last two decades(ibid.) The protectionist policies in particular have sought to promote the supremacy of local enterprises by creating market barriers(ibid.) This is also accompanied with support to develop an emerging technological ecosystem that includes the likes Artificial Intelligence, facial recognition and Internet of Things (IoTs) alongside 5G technologies, with these industries having strong implications with regards to data access and privacy. A continuous flow investment has contributed to Beijing's innovations to develop a technological ecosystem that also enabled several Chinese tech companies to gain strong influential positions at standard development organisations (SDOs) (ibid.)

To achieve this objective, Beijing's key strategy has been to enhance its innovation in the current market which it has achieved through obtaining intellectual proprietary rights through investment in research and development, acquisitions and mergers, establishing collaborations through joint partnerships and independent technological standardization(ibid.)

Chinese strategy of localization to attain parity with foreign competitors

With regards to containing foreign technological influence China deploys a two-thronged policy- (a) Beijing regularly puts forth the rationale of national security to promote dominance of local firms and extends the same norms with regards to its integrated overseas projects (Hoffmann, et al., 2019) (b) Having invested in building internet infrastructure, the government has enacted a National Cybersecurity Law in 2017 that places restrictions on data flows and mandates data to be localized and in addition to the same, requires, stringent reviews of hardware and software for information technology companies(ibid.) Thus, in order to obtain approval to implement their operations, foreign firms have to collaborate with local data providers or build their own local databases and are subsequently required to submit proprietary information pertaining to data alongside hardware and software devices for review and this heightens the risk of erosion of privacy and loss of intellectual property(ibid.)

Strategic Roots of China's Technological Power Projection

Western threat perception stems from how the evolution of China's strategies have been viewed in terms of achieving technological superiority. This can be traced from as early as 2006, when the long-term technological strategy of achieving the ambition of indigenous innovation and achieve a high threshold of decoupling from the West (Kaska & Beckward, 2019) In presenting a challenge to Western dominance, Chinese companies have benefited immensely from direct financing and state subsidies to present themselves a competitor that is not only technologically efficient, but also an economically viable alternative to Western players(ibid.) The strategic foresight of acquiring Western technological and infrastructural firms has also heightened the risk perception among American and European regulators. Another rationale that dictates this perception, is the risk posed in terms of espionage through the rationale of technology manufactured by Chinese firms is a potential object to misuse by the country's military and intelligence agencies for spying on users worldwide (Kaska & Beckward, 2019) According to NATO, the history of Beijing carrying out espionage operations for acquiring technological secrets is a common practice and this is done through organisations that are in a collaborative arrangement with the Chinese government and its industries through targeting academic spaces, industrial and government facilities(ibid.) In 2013, Mandiant- An America cybersecurity firm published a report about People's Liberation Army (PLA) launching an Advanced Persistent Threat (APT) campaign, that revealed details about a systematic data theft from 140 firms hailing from different industries(ibid.)

China's strategy of achieving technological decoupling also deploys a strategy of developing domestic legal framework is used as an intelligence instrument to facilitate the process obtaining sensitive information(ibid.) In 2016, the Chinese National Intelligence Law was enacted that mandated all firms operating on Chinese territory to be compliant in terms of providing assistance to national intelligence policies and maintain secrecy of any intelligence inputs that they are aware of (Kaska & Beckward, 2019) In return, the Chinese state guarantees protection and in the 2014 Counterintelligence Law, the obligations are similar in terms of directing what it calls relevant individuals and firms to provide information, facilities and other forms of assistance(ibid.) The law explicitly mentions for them to not refuse co-operation in these matters and this also exposes the rationale of national security by the Chinese state as means of justifying this coercion.

EU's 5G Threat Perceptions

As a part of its ambition to achieve a status of a major player in the realm of data rights and privacy, the EU has conceptualized possible threat perceptions emanating from the complex convergence of infrastructures that constitutes the basis of 5G technologies. Thus, as a part of its technological sovereignty, the EU has also sought to strengthen GDPR regulations vis-à-vis the domain data governance in the context of 5G technologies. Transboundary data flow and 5G: The deployment of 5G technologies are based on a convergence of virtual and physical infrastructures and in the process, also involves co-operation between European providers and those located outside the EU (Service, 2022) Enforcing of GDPR in regards to transnational data flows is derived from the threat perception of data processing in third countries which do not have privacy safeguard standards considered acceptable by the EU. Thus, the regulation 2016/679 extends EU's territorial jurisdiction borders in regards to these data flows(ibid.) High Speed Data Rate: A key feature of 5G communication technologies is high data speed and lower latency, leading to high volumes of data to be accumulated (Service, 2022) In this scenario, the risk becomes threefold- that is, volume, velocity and variety of data processed presents challenges in the amount, variety and the speed of data that is under processing(ibid.) Here, the velocity aspect escalates the threat perception since it threatens erasure rights in the absence of a consent obtaining process and also risks a possibility of circumventing notifications in the cases where data has been breached(ibid.) Threat regards to Location Based Services (LBS): The mobile applications make extensive use of location information to provide personalized services to consumers and in the process, the monitor consumer activities and preferences on a constant basis to deliver effective customer service (Service, 2022)

Since 5G technologies also utilize the Multiple-in Multiple-Out (MIMO) function, it also facilitates the accuracy achieved in device localisation due to higher frequencies which in turn, aids in revealing locations of the intended subject(ibid.) However, the potential of excessive information being available to service providers about personal and social details of consumers has also been classified by the EU as an avenue for potential misuse, since location is also classified as metadata in the privacy regulations of GDPR(ibid.)

Large number of connected devices (IoT): The Internet of Things (IoT) digital ecosystem has played in increasing the accumulation of data since 5G technologies represent a high degree of interoperability by facilitating data flows between different devices (Service, 2022) The access and flow of data from different devices also increases vulnerability since it leaves the possibility of correlation and data matching, since inferences can be generated through the derived information and could result in collectively targeted discrimination of individuals, as well as communities and institutions(ibid.) Accountability in such a situation will also become a complex challenge to address due to a large number of parties involved in terms of device manufacturers and service providers and make it harder to monitor privacy threats(ibid.) In relation to State and State-backed actors, a particular threat stems from cyber offensive initiatives of non-EU countries (Group, 2019) Several Member States have identified that certain non-EU countries represent a particular cyber threat to their national interests, based on previous modus operandi of attacks by certain entities or on the existence of an offensive cyber programme of a given third State against them (ibid.)

5G Toolbox: EU's emerging Strategic policy instruments for 5G Governance

The EU has highlighted the deployment of regulatory instruments in order to ensure protection of its telecommunication and other networks. Some of these initiatives include (a) EU Telecommunications framework grants the member-states power to impose obligations on telecommunication operators and providers in the situation where the latter operate on their national territory respectively (NIS Co-operation Group, 2020) The objective here is to ensure that member states manage technical and organizational measures to ensure integrity and security of the communication networks(ibid.) Thus, member-states have been granted the autonomy to enact authorization measures against what they conceptualise as unauthorized access in order to ensure confidentiality of communications through undertakings from providers in order to ensure domestic compliance(ibid.) The European Electronic Communications Code (EECC) is a strategic initiative, that has sought extend network security in the context of 5G technologies to the domains of policy measures to handle security incidents, ensuring continuity of business to prevent impacting trade and commerce through regular auditing, monitoring and testing and ensuring international standards are complied with (NIS Co-operation Group, 2020)

It is important to note that this framework has excluded equipment manufacturing and service providing companies with regards to communications supply chain networks(ibid.) The Cybersecurity Act of 2019 has been designed to enact a regulatory framework through certification schemes that extends to products, processes and services. The strategic objective of the certification is to ensure compliance from producers, through establishing standardized norms in the context of demonstrating the inclusion of specific security features in early stages of product development and design (NIS Co-operation Group, 2020) This is intended to not only provide a level of 5G security deemed consistent by EU standards but also contribute in terms of research and innovation to respond to contemporary 5G equipment market(ibid.)

Strategic and Technical Measures of 5G Regulation

Apart from technological standardization and compliance, EU's 5G regulatory framework also extends to domain of trade policy where Foreign Direct Investment Screening Regulation has been a vital instrument in monitoring and subsequently addressing potential security risks with regards to overseas investments in the EU (NIS Co-operation Group, 2020) The screening regulation also seeks to address technologies and infrastructures that are categorized as critical and seek to tackle EU's dependencies in these respective sectors through regular monitoring of investments made by foreign firms in the EU's 5G market (ibid.) The trade policy also seeks to promote a competitive industrial base through preventing subsided and dumped imports and this policy also seeks to establish grievance addressal mechanisms in case of complaints received from EU producers, but also extends the autonomy for the EU take appropriate action without the complaints as well (NIS Co-operation Group, 2020) The Security Toolbox also seeks to influence policy decisions of member-states by encouraging them to prioritise achieving adequate standardizations in environmental, labour and security domains and seeks to grant member-states autonomy in preventing market entry of firms from third countries which do not have market access under specific international trade arrangements(ibid.) The rationale of protecting self-defined national security interests is further re-enforced for the justification of preventing the entry of service providers in the domestic market of the member-state.(ibid.)

In the context of constantly evolving geopolitical dynamics that concerns 5G technologies, the cybersecurity toolbox classifies the regulatory approach into strategic and technical measures respectively (NIS Co-operation Group, 2020) Strategic measures take into consideration, about granting relevant authorities present at the EU level and as well as national organisations of member states additional regulatory powers to rectify vulnerabilities of non-technical nature and this makes a direct mention about external interference from a third country and the development of sustainable and diversified sources of 5G supply to prevent risks arising from long-term dependencies (NIS Co-operation Group, 2020) These measures also call for audits to be regularly performed on operators and gain vital information about their operational capabilities and in addition to the same, the measures

also call for stronger background checks of potential suppliers with regards to their risk profiles and enforcing appropriate restrictions for risk mitigation of key assets accordingly (NIS Co-operation Group, 2020)Diversification of suppliers to fulfil the technological and logistical needs of individual organisations through adequate multivendor strategies, along with simultaneous identification of significant assets to develop a 5G technological ecosystem based on strong industrial bases with national resilience and application of this strategy to lay a strong foundation to develop and maintain diversity in technologies of the near future(ibid.)

Technical measures by the EU on 5G can be conceptualized as a policy framework to enhance the security of existing 5G networks and equipments through a collective re-enforcement of security of technologies, processes, personnel and other physical factors (NIS Co-operation Group, 2020) There is a key emphasis on fulfilling baseline security requirements through establishment of an architecture with secure network designs alongside regular evaluations of security measures in accordance with present 5G standards(ibid.) Technical strategies lay a key emphasis on establishing secure networks with strict access controls, that also offer adequate protection to virtualized network functions through ensured network monitoring and operational management. Regular upgradation of physical infrastructure alongside maintaining software integrity is also essential in raising the quality of standards with regards to encouraging suppliers by creating favourable conditions for the procurement of equipment(ibid.) Technical measures also seek to expand EU standardization norms through enforcement of certifications in customer equipment, network components and supplying processes and also seek to extend this standardization in the convergent technological network to non-5G ICT technologies for longer term plans(ibid.)

Divergence in national policies of EU member-states and Third Countries in Huawei's case

Australia and the US have mitigated the perceived risk from Huawei by banning it in 2012 and 2013 respectively (Radu & Amon, 2021; pp.2-3) While Australia restricted the company from bidding on its national broadband network, virtually almost forcing it out of the market, Washington placed a strong ban on all purchases by the government of technology from companies that showed linkage to China through ownership, operations and subsidiary funding (Chergwin, 2012) (Muncaster, 2013) The United Kingdom after Brexit, has also followed an aggressive stance by banning Huawei from its infrastructural development plans and in the process, also published a report in justification of the same stating that Huawei does not meet the cyber security standards defined (Murphy & Parrock , 2021)

The EU on the other hand, did not immediately follow suit with Australia, US and the UK with regards to policy measures and took a far more ambiguous approach by (a) Directing member-states to have a unified concerted approach to 5G technology and therefore carry out national risk assessments and (b) Reviewing existing measures and simultaneously prepare adequate tools to direct further policy measures.

However, there has also been a divergence in policies among member-states themselves that have imposed varying kinds of restrictions, signaling the lack of unified action among the EU bloc. While Sweden has followed Washington by excluding Huawei's 5G equipment completely from its network space, Central and Eastern European states such Poland, Czech Republic, Latvia, Estonia and Lithuania have also adopted a hardline stance in excluding the company from their respective networks (Murphy & Parrock, 2021) France and Germany's policies have more nuanced in comparison- While France has permitted Huawei to supply the 5G equipment, it has done so under a stipulation by imposing operation restrictions by granting security agencies the power to veto the company's infrastructure policies at their discretion(ibid.) Germany on the other hand is highly divided on the issue; while Berlin has created a legal framework by approving an information security law in 2022 that stipulates detailed infrastructure reporting requirements for tech companies to tighten information security, it has adopted a cautious approach to be not openly confrontational to harm its economic ties with Beijing in the process(ibid.)

Findings and Conclusion

It can be inferred that the technology has changed the dynamics of how EU perceives it sovereignty, as this discourse serves a point of departure where potential withdrawal of American security cover was earlies scenarios to be put forth by the EU. The role of technology in the evolution of EU's strategic autonomy can be termed as a transformative instrument that diversifies the nature of its power projection. It can be stated that technology in EU's framework for strategic autonomy has become the central point of reference in dictating its normative and economic power respectively. This can be attributed to the fact while technology had already begun to be granted space for institutional prioritization in EU's official discourse, the increased global dependence on digital mediums during the covid-19 pandemic accelerated the process of elevating technology to be one of the central referent objects in the context of attaining the ambition of strategic autonomy. While it is difficult to place Brussels in a single spectrum of the extreme ends of Wong's framework, it can be inferred that the EU has deployed regulatory mechanisms as an instrument of techno-nationalist framework to achieve its long-term techno global ambitions of achieving parity with global dominance of United States and China. Since the EU is not a single sovereign state but an institutional collective identity of individual member-states, it also turns out to be an exception in the techno-nationalist and techno-globalist framework respectively. While the EU's identity as a technological actor might contradict the categorization solely in terms of techno-nationalist and globalist spectrum, the discourse asserting defensive and offensive approach to technological sovereignty can be classified as nationalist and globalist respectively, since the former emphasizes regulation to sustain domestic industrial base. The offensive approach to technological sovereignty on the other hand can be categorised as techno-globalist since it calls for the EU build its own autonomous digital and technological ecosystem to reduce its technological dependencies on external actors.

The EU's technological discourse also acquires the context of securitisation where the rationale to regulate and exercise a high degree of control is derived from the high degree technological dependencies that are weaponised as an instrument of coercion for expanding geopolitical influence. The rationale to securitise acquires even more legitimacy since the threat perception of potential subordination due to technological dependencies is greater than the benefits of globalized economic structures. Hence, EU's assertion of a liberal-democratic identity that is different from the United States is driven by a realist logic where domination by a powerful ally is viewed as an act of what can be termed as technological subjugation. It can be inferred that in order to project a high degree of assertiveness in the global technological arena, the technological discourse needs to be brought in the

institutional synchronization by justifying that the benefits brought about by the enhance technological capabilities would prove beneficial in other sectors as well. This is demonstrated by the EU calling for joint collaboration between member-state and Transatlantic institutional bodies to collaborate with private sector with respect to the development of Key Emerging technologies (KETs) Thus with a view of making the European industrial base to be globally competitive, the EU's technological discourse, can also be understood to convey benefits of collaboration through offering member states a unique opportunity to enhance their individual technological and digital capacities as well. It can also be deciphered that the EU is cognizant of not appearing to be an isolationist actor when it comes to enforcing its defensive approach and that wants to continue the level of global engagement, but it wants to do so in a mechanism so that the consumer benefit and the development of local industries become the central referent objects while pursuing this policy objective.

The technological divide in Transatlantic relations reflect highly divergent views that dictate the strategic rationale of how Washington and Brussels perceive cyberspace. It can be inferred that EU's difference with the United States comes from a threat perception about American digital platforms being entrenched with US national security and intelligence architecture. Brussels considers Washington's digital policies to cause a high degree of militarization of cyberspace, which it infers happens to be in contradiction with its model that prioritizes human rights and consumer protection. The recent regulatory approach of GDPR demonstrates EU's opposition to US hegemony over the internet since what it calls as excessive securitisation is contradictory to the liberal-democratic values of free expression, which the Transatlantic partnership strongly believe in defending in their identity as liberal internationalist actors. This also demonstrates a gap in technological capabilities between the two actors as US hegemony over cyberspace has also equipped it with offensive capabilities that also grant it enough power to unilaterally change the norms for internet governance and potentially launch cyber-attacks to weaken the actor it perceives as a potential threat to national security.

Since Washington's offensive capabilities also wield the potential to weaken network infrastructures across the world, EU's regulatory mechanisms derive their legitimacy from securitisation of American digital platforms that are perceived to be an extended organ of the US Intelligence agencies and the transnational operative nature of these platforms increase the threat of privacy violation of European citizens who use these platforms and potentially misuse their data. Thus, justifying the policy clause of EU's data protection regulations that place restrictions on non-European firms processing data of European citizens irrespective of their geographical location of functioning and in addition to the same, mandate localized data processing to appropriately handle any potential incident of data theft.

The PRISM incident of 2013 can be understood to have heightened EU's threat perception regarding the same and provide a rationale pretext for promoting its regulatory framework that securitises overseas digital platforms. The threat perceptions regarding digital platforms are further extended, since they are viewed as techno-political agents and the monopolisation of the digital markets grants them a high degree to influence domestic political and societal discourses of other countries due to their respective gatekeeping power, that could potentially create situations of social unrest by undermining the domestic political institutions of the nations on whose territory these platforms run their regional operations from. Digital platforms have also created dependencies on media outlets to maximise their audience outreach, hence the EU's regulatory framework demonstrates a high degree of threat perception due to their potential to undermine press freedom in any of the member-states. However, it can also be observed that despite the EU displaying a high degree of assertiveness through projecting its data-based regulatory framework, Brussels demonstrates the defensive approach to its discourse on technological sovereignty. Despite the heightened threat perceptions regarding digital ecosystems from the United States, the EU does not undertake an offensive approach of its technological discourse by aggressively pushing for development of indigenous European social media digital platforms.

This infers that while the EU acknowledges the privacy and security threats that arise from a highly weaponised dependence on American digital platforms, it also carries the risk of undermining the Transatlantic partnership since an offensive approach to technological sovereignty with regards to its bilateral ties with Washington. Since Europe is also viewed as a technologically geo-strategic market sphere of influence by the US, a situation of any potential European-developed platforms posing a competition could essentially threaten the American security guarantees and economic investments in the continent. In addition to the same, there are not any studies that demonstrate a high public demand in Europe for domestically developed digital media platforms being preferred over American ones. Since EU lacks offensive capabilities in the current times in its capacity to develop an autonomous digital ecosystem, innovation-centered research and development collaboration with Washington with regards to digital platforms could continue facilitating the exchange of technological expertise to lay a strong foundation for an indigenous digital ecosystem. Since several domestic businesses rely heavily on social media networks to expand their regional outreach, the magnitude of risk posed by a scenario of Big Tech companies reducing their operational capacities in Europe could create a domestic political backlash for member-state governments.

While the differences continue to persist in the Transatlantic partnership with regards to rules-based governance in cyberspace, the technological convergence is reflected through the establishment of Trade and Technology Council, which can be perceived as a common Transatlantic forum for both Brussels and Washington to project their image of liberal-democratic technological actors which have a firm commitment towards protecting freedom of expression. Coupled with China's rapid rise, the convergence is driven by mutual threat perception of Beijing in terms of the threat perception it presents through the expansion of its infrastructural Digital Silk Road project that challenges Western technological standards.

Lastly, EU's threat perceptions vis-à-vis China in the context of 5G technologies stem from a similar threat perception that arose via the United States i.e; the nexus of business companies with intelligence agencies. The opacity regarding the demographic information of board members in the case of Huawei elevate the threat perception of Chinese government attempting to carry out industrial espionage and subsequently resulting in technological and intellectual property theft. Due to single-party authoritarian nature of the Chinese government, the militarization of 5G telecommunication and cybersecurity networks reduce the probability of accountability to consumers compared to the United States, which is a democratic state. Since 5G networks also cover interconnected Internet of Things (IoTs) network, the volume of data is immense and thus presents a greater risk of being vulnerable to abuse and requiring enhanced infrastructural capabilities to secure. While the EU in its official discourse on 5G technologies did not directly project China to be a security threat, compared to scenario that concerns the dependency on digital media platforms, it's strategic discourse explicitly mentions the diversification of vendors in order to prevent security risks arising weaponised dependence. However, the magnitude of threat perceptions differ from different member states in terms of restrictive measures applied in the case of Huawei, reflecting the economic dependence on Beijing that has prevented a fully unified plan of action against the company. A key difference that stands out in the comparative policy perspective adopted in the context of digital media platforms and 5G communications, is greater degree of autonomy granted to individual member-states in the latter domain in terms of implementing investment screening mechanisms to prevent 5G vendors from non-EU countries from entering the domestic market of the member state. To conclude, EU's strategic ambition to attain technological sovereignty in the strategic triangle with United States and China reflects a common threat; i.e. the aggressive militarization of cyberspace, with both cases of Washington and Beijing reflecting a functional nexus of private companies with intelligence agencies of both countries.

Both Washington and Beijing justify the rhetoric of national security to legitimise the militarisaion of cyberspace. The only difference being the U.S. security establishment being more transparent with its legal framework in the context of data processing from digital platforms, compared to more opaque nature of Chinese firms, where links between high-ranking company officials to the Chinese Communist Party cannot be easily ascertained. This becomes a source of securitisation and a strategic rationale for the EU to implement its respective regulatory mechanisms against technological ecosystems which do not confirm to its vision of human-rights based vision of cyber and communication spaces that seek to uphold the right to data privacy. The GDPR and 5G Security Toolbox demonstrate EU's strategic ambition of technological sovereignty to project an image of global regulatory power with an attempt to establish two policies as models to emulated. In regards to the future scope of this study, it remains to be observed if the EU adopts a similar militarization-based approach, once it has acquired equivalent cyber offensive capabilities that are at par with US and China in the future.

Methodology and Theoretical Perspective

The objective of this study was to analyse European Union's strategic autonomy in the context of exercising technological sovereignty. As a part of this analysis, the first method as to trace the evolution of multitude of factors that have shaped EU's foreign policy orientation and frame technology as the central object of reference in the evolution of EU's strategic culture. Therefore, the study progressed as a framework of analysing technology as a concentric element in EU's foreign and strategic policy as a referent object as a key factor in proceeding with the content analysis of the evolution of EU's technological strategic discourse. Therefore, in addition to defining the terminologies of strategic autonomy and the role of the latter as an instrument in the development of strategic culture, the initial analyses sought to lay a functional groundwork that lays emphasis on the chronological evolution of Brussels' foreign policy post-Cold War.

To investigate the same, the first objective to establish the approach to establish the relationship between the collective institutional identity of the EU and the functioning of its foreign policy framework, which makes it an exceptional entity from other nation-states actor since it represents a unified foreign policy of several individual sovereign states. Thus, most part of the study has been analysed with the institutionally collectivist framework being the central object, however this does create limitations later in the chapter regarding China, where policy divergences between individual member-states demonstrate a contradiction to collectively institutionalist identity of the EU which has been placed as a central object of reference during the course of this study. The analysis of foreign policy-based chronological developments in the context of strategic autonomy also aided in tracing the evolution of not only how technology became an important standpoint in the debates, but also through analysis of the factors that led to EU's expanded focus on technological sovereignty as a key security concern. The author while framing the EU as the central referent object, conducted the analysis through secondary data and literature that was available. To facilitate the originality in analysis, official policy documents published by the EU and journal articles by academics alongside thinktank reports were consulted to draw out comparisons of perspectives that shaped the analysis of EU's technological discourse.

Securitisation in the context of Technological Governance

The concept of securitisation as a theoretical perspective also explains a multitude of rationales in analysing EU's technological discourse. The theory argues that the definition of security did not restrict itself to developments of states enhancing their powers in economic and military domains, but also extend the same to other sectors such as societal, political and other domains (Kilroy, 2018) This expansion was put forth to facilitate the states a more independent degree of agency in terms of

asserting and re-framing their core identity, national interests, domestic institutions, but also use the securitising discourse to expand their international influence as well(ibid.) The agency attained in the discourse of securitisation seeks to emphasize the grave threat posed to the domain that has been the referent object to justify the prioritization of the same and urgent enactment is required(ibid.) In the context of this study, the EU's strategic discourse is based on the extension of securitisation to the domain of technologies and thus its pursuit of attaining strategic autonomy through the publications of its documents, that consistently highlight the EU lacking strategic depth in global technological arena and its dependencies on third countries poses a security threat. While the applicability of securitisation theory enables to a large extent of understanding EU's strategic rationales, it also violates one of the theoretical assumptions that securitisation often involves subordinating public debates avoiding scrutinization. Since the EU projects itself as a liberal-democratic actor and all member-states are democracies with high degree of press freedom and institutional autonomy, it cannot be stated that there is a lack of popular support for achieving this strategic ambition. The rationale of securitisation is applicable to political and societal spheres. In reference to the political sphere, there is a key emphasis on the practice of securitisation through preservation of state legitimacy and that the threat to the legitimacy can arise from a variety of groups such as ethnic and religious minorities, social movements and businesses (Kilroy, 2018) In the analysis of EU's technological discourse, the big tech companies from projected to be the threat sources due to their potential to misuse personal data of EU citizens and carry out industrial espionage respectively and could potentially undermine liberal democratic systems of member-states. Thus, policy measures such as the GDPR rules in the context of EU's strategic discourse can be viewed through a lens where regulation is enforced as an instrument of securitisation. In addition to the same, the applicability of the securitisation model in this study presents a scenario where policies are implemented in ties between allies (the EU and US) demonstrate that securitisation does not always take place solely in situations where states are openly hostile to each other.

Discourse Analysis in Contextual Assumptions and Limitations

The discourse analysis used as a methodological interface for this study also showcases the limitations that have arisen due to structural and geopolitical factors while shaping EU's strategic narratives. The methodological aspect of critical paradigm assumes the central importance as it takes into account the subject matter and socio-political issues that often extend to the dimensions of underlying set of assumptions, existing state of relations and ideological orientations that are often the key ingredients in generating policy discourse (Goutsos & Georgakopolou, 2004) In the context of this study, the limitations are posed in terms of analysing the nature of EU's projection of its technological footprint, the unit of classifying the spectrum as the frame of reference was the classification of techno-globalism

and techno-nationalism based on Brussels' projection of what it termed as offensive and defensive approaches to technological sovereignty.

The EU as a technological actor incorporates both elements from both spectrums of this technological framework and its strategic discourse makes it difficult to classify as either techno-globalist or techno-nationalist, since elements from both streams of classification are deployed by Brussels to attain its strategic objective. Since technologies are a vast field, the study specifically evaluates the case study of EU's policies regarding digital platforms to analyze its emerging regulatory framework and as well as the degree of divergence with regards to technological governance vis-à-vis it's bilateral ties with the United States. Since China has been the focal point of global discourse regarding security concerns around 5G networks, the study was structured to analyze the development of Brussels' developing technological discourse in the context of several countries calling for technological decoupling from Beijing on the accusations of espionage. Lastly, the discourse analysis deployed for this study also evaluates the degree of overtness and covertness with which EU projects its desire for technological sovereignty, especially in regards to US and China. The rationale for covert nature by avoiding mentioning American and Chinese technological activities, reflects a discourse that seeks to project a high degree of assertion in terms of the EU achieving its technological ambitions without appearing aggressively confrontational in its projection. The limitation is reflected in terms of the security, economic and technological dependencies the EU has in its relationship with both Washington and Beijing. In the document published by the NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) titled "Huawei, 5G and China as a Security Threat", the overtness is far more in magnitude compared to other documents analysed on EU's 5G policy. Since several EU member-states are also a part of NATO, the latter can be understood as an institutional shield to facilitate an anti-Beijing discourse.

Strategic Triangle Angle

Since this study analyses strategic autonomy with regards to technological governance, the Strategic Triangle Angle provides a suitable framework to explain the trilateral relationship between the EU, US and China with Brussels relations with the two being the central object of reference (Biba, 2021) The applicability of this model is based on an underlying set of basic assumptions which state that the actors taken into consideration should be rational and sovereign, and that any actor engaging in bilateral diplomatic ties with the other must orient their policies taking into consideration the strategic interests and response of the third actor(ibid.) The model also emphasizes that the players in this framework do not always necessarily possess equal strategic depth, bilateral ties between two players within the framework will always be under a high degree of influence by their relationship with the third player.

In terms of axiomatic principles, the relationship between the three players in the triangle cannot be quantified solely in terms of positive or negative, the magnitude in terms of desirability to achieve strategic interests is also important, which can be achieved by maximizing positive and minimizing negative aspects of diplomatic ties that bring strategic advantage through economic and political gains and reduce potentially high risk of building strategic capacities(ibid.) This model has been chosen from the study conducted by Sebastian Biba that tests the applicability of the strategic triangle in the context of Germany's bilateral relationship with the United States and China and I have applied the same framework by replacing Germany with the EU to formulate the STA model in the context of technological governance between the three actors.

The applicability of the model in this study was based on EU's shared convergent interests and as well as constraints with Washington and Beijing. The fundamental assumption that has guided the formulation of the study is same as the one found in Biba's study, i.e.- the element of hostility between the US and China manifesting itself as a race in terms of global technological competition. In the context of this underlying assumption, the EU's negative constraints with Washington demonstrate in the form of disagreements over data protection and the convergence is reflected through the establishment of the Trade and Technology Council to counterbalance Beijing's influence. Concerning the bilateral ties between Brussels and Beijing, the positivist element is reflected in the nature of technological dependency for 5G telecommunication networks and the constraint is presented in terms of threat perceptions of industrial espionage, which the EU has recently started scrutinizing to a high degree. However, the magnitude of constraint between EU and China can be understood to be greater than those with Washington since directly addressing Huawei and China through NATO as a threat can be perceived as a more directly confrontational stance in the discourse. In terms of overall maximization of strategic advantage, the EU's policy objective of achieving strategic maximization is positioned in terms of maintaining partnerships with both Washington and Beijing to achieve an autonomous technological ecosystem as an end goal of its ambition of attaining technological sovereignty. The negative aspect of diplomatic ties seeks to minimize the technological dependence on both Washington and Beijing citing the potential threats arising from the dependencies that could undermine domestic institutions.

References

Csernatoni, R., 2021. *The EU's Rise as a Defense Technological Power.* [Online]
Available at: https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134

Fiott, D., 2017. A Revolution Too Far? US Defence Innovation, Europe and NATO's Military-Technological Gap. *Journal of Strategic Studies ,* 40(3), pp. 417-437.

German Institute of International Affairs , 2019. *European strategic autonomy: actors, issues, conflicts of interests.* [Online]
Available at: https://www.swp-berlin.org/10.18449/2019RP04/#hd-d14204e710

Helwig, N., 2021. *Strategic Autonomy and the Transformation of EU: New Agendas for Security, Diplomacy, Trade and Technology,* s.l.: Finland Institute of International Affairs.

Service, European External Action, 2020. *Why Strategic Autonomy Matters.* [Online]
Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/89865/why-european-strategic-autonomy-matters_en

European Parliamentary Research Service , 2021. Key Enabling Technologies for Europe's Technological Sovereignty, s.l.: European Parliament.

Anand, V., 2020. Revisiting the Discourse on Strategic Culture: An Assessment of the Conceptual Debates. Strategic Analysis, 44(3), pp. 193-207.

Erickson, A. S. & Johnson-Freese, J., 2006. The emerging China–EU space partnership: A geotechnological balancer. Space Policy, 22(1), pp. 12-22.

European Commission , 2020 . Europe: The Keys To Sovereignty. [Online]
Available at: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en

European Commission , 2020. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. [Online]
Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

European Commission , 2021. Commission Staff Working Document: Strategic Dependencies and Capacities , Brussels : European Comission .

European Commission, 2020. White Paper: On Artificial Intelligence- A European Approach to Excellence and Trust, Brussels: European Commission.
European External Action Service , 2016. Shared Vision, Common Action: A Stronger Europe; AGlobal Strategy for European Union's Foreign and Security Policy , s.l.: European Unon.
Farrell, H. & Newman, A. L., 2019. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, 44(1), pp. 42-79.
Fraunhofer Institute for Systems and Innovation Research ISI, 2020. Technology Sovereignty: From Demand to Concept , Karlsruhe: Fraunhofer Institute for Systems and Innovation Research ISI.
Gehrke, T., 2022. EU Open Strategic Autonomy and The Trappings of Geoeconomics. European Foreign Affairs Review, 27(Special Issue), pp. 61-78.
Helwig, N., 2022. The Ambiguity of the EU's Global Role:. European Foreign Affairs Review , 27(Special Issue), pp. 21-38.
Helwig, N. & Sinkkonen, V., 2022. Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term. European Foreign Affairs Review , 27(Special Issue), pp. 1-20.
Hyde-Price, A., 2006. "Normative" Power Europe: A Realist Critique. Journal of European Public Policy, 13(2), pp. 217-234.
Mearsheimer, J. J., 2019. Bound to Fail: The Rise and Fall of the Liberal International Order. International Security, 43(4), pp. 7-50.
Nakayama, S., 2012. Techno-Nationalism vs. Techno Globalism. East Asian Science, Technology and Society: An International Journal, 6(1), pp. 9-15.
Odegaard, L., 2021. Europe and the US-China tech war : Enhanced competition in the post-Trump era, s.l.: Robert Schulman Center for Advanced Studies.
Pérez, R. G., 2019. Strategic Autonomy of The European Union. In: E. Conde, M. Scopelliti & Z. V. Yaneva, eds. The Routledge Handbook of European Security Law and Policy. London: Routledge, pp. 81-94.
Roberts, A., Moraes, H. C. & Ferguson, V., 2019. Toward a Geoeconomic Order in International Trade and Investment. Journal of International Economic Law, 22(4), pp. 655-676.
Rogers, J., 2009. From 'Civilian Power' to 'Global Power': Explicating the European Union's 'Grand Strategy' Through the Articulation of Discourse Theory. Journal of Common Market Studies, 47(4), pp. 831-862.

Wong, P. N., 2021. Techno Geopolitics: Towards Novel Theoretical Framework transcending the 'techno-nationalism vs. techno-globalism' dualism. In: Techno-Geopolitics: U.S.-China Tech War and the Practice of Digital Statecraft. London: Routledge , pp. 19-50.
Bauer, M. & Erixson, F., 2020. Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls, s.l.: European Centre for International Political Economy.
Bradford, A., 2020. The Brussels Effect: How the European Union Rules The World. New York: Oxford University Press.
Christou, G., 2016. Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?. In: Cybersecurity in the European Union. London : Palgrave Macmillan , pp. 144-170.
Commission, E., 2020. A new EU-US Agenda for Global Change, Brussels: European Commission.
Dijck, J. & Nieborg , D., 2019. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet. Internet Policy Review, 8(2), pp. 1-18.
European Commission Expert Group For the Observatory on the Online Platform Economy, 2021. Uncovering Blind Spots in the Policy Debate On Platform Power, Brussels: European Commission.
European Commission, 2020. A European Strategy for Data, Brussels: European Commission.
European Commission, 2021. EU-US launch Trade and Technology Council to lead values-based global digital transformation. [Online]
Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990
Gorwa, R., 2019. What is Platform Governance. Information, Communication and Society , 22(6), pp. 854-871.
HEIKKILÄ, M., 2020. The Achilles' Heel of Europe's AI strategy. [Online]
Available at: https://www.politico.eu/article/europe-ai-strategy-weakness/
Oracle , n.d. What is IoT?. [Online]
Available at: https://www.oracle.com/internet-of-things/what-is-iot/
Sottek, T. & Kopfstein , J., 2013. Everything you Need to Know About PRISM. [Online]
Available at: https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet
Torreblanca, J.-I. & Jorge-Ricart , R., 2022. The US-EU Trade and Technology Council: The State of Play, Issues and Challenges for Transatlantic Relationship, s.l.: Esade EcPol-Center for Economic Policy.

Wolford, B., n.d. What is GDPR, the EU's new data protection law?. [Online]
Available at: https://gdpr.eu/what-is-gdpr/
Chergwin, R., 2012. Huawei banned from Australia’s NBN: reports. [Online]
Available at: https://www.theregister.com/2012/03/25/huawei_nbn_ban/
Group, N. C.-o., 2019. EU Co-ordinated RIsk Assessment of the cybersecurity of 5G networks, s.l.: NIS Co-operation Group.
Hoffmann, S., Bradshaw, S. & Taylor, E., 2019. Networks and Geopolitics: How Great Power Rivalries Infected 5G, s.l.: Oxford Information Labs.
Kaska , K. & Beckward, H., 2019. Huawei, 5G and China as Security Threat, Talinn: NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE.
Kenyon, M., 2020. Huawei and 5G explained. [Online]
Available at: https://citizenlab.ca/2020/12/huawei-and-5g-explained/
Muncaster, P., 2013. US bill prohibits state use of tech linked to Chinese government. [Online]
Available at: https://www.theregister.com/2013/03/28/us_government_crackdown_china_it_firms/
Murphy, A. & Parrock , J., 2021. Huawei 5G: European countries playing 'politics' with network bans, Chinese company says. [Online]
Available at: https://www.euronews.com/next/2021/07/28/huawei-eyes-a-place-within-europe-s-digital-future-despite-5g-bans-in-some-countries
Newman, L., 2021. 5G Is More Secure Than 4G and 3G—Except When It's Not. [Online]
Available at: https://www.wired.com/story/5g-more-secure-4g-except-when-not/
NIS Co-operation Group, 2020. Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures, s.l.: NIS Co-operation Group.
PwC, 2016. Technology Companies: In the Sweet Spot for Risk Resiliency and Agility, s.l.: PwC.
Radu, R. & Amon , C., 2021. The governance of 5G infrastructure: between path dependency and risk-based approaches. Journal of Cybersecurity , 7(1), pp. 1-16.
Service, E. P. R., 2022. Privacy and Security Aspects of 5G Technology, Brussels: European Parliament.
The Washington Post, 2022. How Huawei Landed at the Center of Global Tech Tussle. [Online]
Available at: https://www.washingtonpost.com/business/how-huawei-landed-at-the-center-of-global-tech-tussle/2022/05/20/1210e7a8-d82c-11ec-be17-286164974c54_story.html

Yahuda, M., 1994. China and Europe: The Significance of Secondary Relationship. In: T. Robinson & D. Shambaugh , eds. Chinese Foreign Policy: Theory and Practice. s.l.:Oxford University Press, pp. 266-82.

Zhou, H., 2009. The 60 Years of China-Europe Relations. Chinese Journal of European Studies , Volume 5, pp. 34-51.

Biba, S., 2021. Germany's relations with the United States and China from a strategic triangle perspective. International Affairs , 97(6), pp. 1905-1924.

Goutsos, D. & Georgakopolou, A., 2004. Duscourse Analysis: An Introduction. s.l.:Oxford University Press.

Kilroy, R., 2018. Securitisation. In: A. Masyk, ed. Handbook of Security Science. s.l.:Springer.