• Article •

Entanglement Security and the Dynamic Turn of European Integration

An Peng[1,*]

[1] China Institute of International Relations, China Foreign Affairs University, Beijing, China

[*] Corresponding Authors: An Peng. Email: aanpeng1998@gmail.com

Received: 20 April 2024 Accepted: 9 May 2024 Published: 9 May 2024

Abstract: European integration during the Cold War was designed to jointly respond to threats from Soviet socialism and the German Nazis. In the process of integration, European nation-states shape national security with national interests as the center, which means that integration is a collective foreign policy formed by bargaining among governments. Its direction is to provide a basis of trust from the low political field, and then to the high political field. At present, the EU is facing the trend of alienation of security relations, expansion of competition space and blurring of security boundaries. The EU urgently needs to strengthen its own identity, compete for new geopolitical areas, shape its internal jurisdiction through technical sovereignty, and promote European integration to a deeper level. Therefore, the driving force of EU integration has begun to shift to technical sovereignty. This study takes entanglement security as the research framework, focusing on the new driving factors of the development of European integration under the new situation.

Keywords: EU; Entanglement Security; Technical Sovereignty

1. Introduction

The content of competition in the international community is contemporary and technical, subject to technological and spatial constraints, nation-states used to compete mainly in the fields of arms, trade, diplomacy, natural resources and agriculture, etc., but when the competitive resources and capabilities of competing countries tend to be balanced, they will be caught in a "competitive dilemma", and therefore need to seek new content of competition. Therefore, it is necessary to seek new competitive content in order to break the original deadlock and give new competitive vigour to the international community. At this time, the actor that takes the lead in grasping new competitive resources can seize the dominance of international competition and seek a higher status in the international community. As early as in the 1980s, the European Community, in order to strive for greater autonomy, once tried to cooperate in the field of high technology and launched the "Eureka Plan" to build a technological Europe. However, due to the legal nature of the EU and the ambiguity of "sovereignty" at the EU level, in order

to avoid ambiguities in the division of powers among member states within the EU, the EU's power as an independent actor has not been expressed in the form of "sovereignty" in the past.

With the globalisation process after the end of the Cold War, the pattern of competition between the major powers has taken on new dimensions. The search for technological mastery by different states has led to a tendency towards the securitisation and geopoliticalisation of technology, which in turn has increased technological conflict between different actors. From a practical point of view, at present, technology is used by international actors to engage in external competition, construct identities, and even trigger conflicts, and technology is no longer a purely dimensional factor of production, but has become an important force affecting international security. Under the influence of technology, security has taken on a multi-level, multi-relational and multi-spatial character, and security issues in various fields and spaces are interconnected and mutually influential, presenting such entangling phenomena as the alienation of security relations, the combination of real and virtual spaces, and the blurring of security boundaries. As security issues become more complex, the emergence of "entangled security" phenomenon, European integration needs to seek a new impetus, in this context, the EU in the field of technology to build the concept of "sovereignty", to "technological sovereignty In this context, the EU has constructed the concept of "sovereignty" in the field of technology, and returned to the political discourse system of the EU in the form of the new concept of "technological sovereignty", which has become the new driving force for the deep development of European integration in the technological context of the new era. However, this change in the elements of the dynamic has not yet been adequately studied by academics, and this paper focuses mainly on examining why there is a tendency for the EU integration dynamic to shift from traditional geo-extension and sovereignty to shaping technological sovereignty.

2. Existing Research and Its Shortcomings

In currently available research, European integration is driven by economic integration, political peace objectives, legal and institutional innovations, the challenges and opportunities of globalisation, and cultural and social oneness. These dynamics are intertwined, and together they drive European integration forward, creating a closer, more united Europe. In recent years, as the discourse of "technological security" within the EU system has increased, the study of dynamics has gradually shifted to the construction of "technological sovereignty", but there has been a lack of attention to the causes of the transformation of the EU's integration dynamics.

In the study of defence security and political stability as the driving force of integration, Feng Yiran believes that since 2016, due to the increasingly severe security situation faced by the EU, the supranationalist character of the EU's autonomous defence has become more and more obvious, and a "new security concept" has been formed on the basis of which, i.e., the resonance of traditional and non-traditional security threats, the interweaving of internal and external security challenges, as well as the development of a "new security concept". On the basis of this, a "new security concept" has been formed,

in which traditional and non-traditional security threats resonate, internal and external security challenges are intertwined, and the divergence of interests with the United States has increased, so that the EU member states have strengthened their autonomous defence cooperation, and stepped up European integration through the establishment of the European Defence Fund and the construction of the "Permanent Structural Cooperation", which is a combination of supranationalism and inter-governmentalism. In the future, integration will continue to be led by France and Germany, which will continue to promote defence cooperation within the framework of the European Union, and the structure of the European Union's security forces will become more and more important as a result of the upgrading of the status of the European Commission and the impact of the Brexit event . Fang Lexian and Di Chongguang continue to conduct further research on the "permanent structural cooperation" mechanism, affirming the EU's innovation in the decision-making mechanism, but also pointing out that the implementation of this cooperation mechanism is subject to great uncertainty .

In the study of maintaining economic, financial and market security as the driving force of integration, Li Xia and Shi Di studied the process of European financial integration since the birth of the euro from a macro perspective, which mainly stimulates the integration of European capital markets and promotes the vitality of economic development through the plan of the Capital Markets Union, adapting to the current normalisation of the global monetary policy and the post-Brexit era in the United Kingdom; Wang best studied the process of the European Central Bank's shift from technologisation to politicisation from a micro perspective, arguing that the politicisation of the European Central Bank has fuelled the development of European economic integration. The interaction of factors such as the inability of the ECB's traditional policy mandate to cope with the European debt crisis, the politicisation of economic issues due to the weak economy becoming the new normal, the prevalence of euroscepticism impeding the development of economic integration, and the urgent need for strong political leadership in times of crisis, have all led to the politicisation of the ECB. The ECB has a long way to go in the future, and will take on more responsibility for restoring market confidence, recovering the economy and promoting the deeper development of European integration .

In the study of the legal system as a driving force of integration, Zhong Yichen and Luo Yingjie take the supranational politicisation of the EU's justice and home affairs field as an example of the EU's new public administration reform. It is elaborated that the main purpose of the establishment of EU public offices is to fulfil specific tasks at the Union level, including monitoring the fulfilment of treaty obligations by member states in a certain field, facilitating the exchange of information between member states, and providing professional technical support for EU legislation. In the field of justice and home affairs and in response to the refugee crisis, the EU Office cooperates with other Union institutions and member states' administrations, highlighting its importance in the EU's comprehensive governance system, and is a key force in promoting the EU's ability to enhance its administrative and governance capacity and level of integration. With the expansion of the administrative competence and discretionary

power of the EU public office, the EU has been able to strengthen its supervision capacity of the member states and improve the overall level of administrative and judicial cooperation .

In the study of responding to the challenges of globalisation as a driving force for integration, Lian Bo studied the dilemma of the EU's energy security strategy integration from the contradiction between intergovernmental and supranational, the contradiction between autonomy and dependence, and the contradiction between securitization and non-securitization of energy issues; Jinling examines the transformation of the EU's energy and climate strategy, arguing that economic competitiveness and energy security supply have become strategic priorities. This strategic adjustment reflects that the EU not only needs to rebuild the balance between the triple objectives of climate change, competitiveness and energy security, but also needs to seek a balance between government intervention and market mechanisms. In the long run, the EU's process of promoting low-carbon economic transformation is irreversible; Cui Hongwei analyses the characteristics of the EU's New Deal on Climate measures and proposes that the EU's New Deal on Climate will help promote the development of European integration. The New Climate Deal is motivated by the need to solve socio-economic problems such as economic growth, employment and energy supply, and aims to construct a "European identity", promote the in-depth development of European integration, and improve the EU's international competitiveness and international political influence; In addition, Shi Xiaodong and Tian Ye believe that the construction of cultural identity is also one of the hidden sources of power for European integration, regional democratism and national nationalism have a profound impact on the in-depth development of integration .

For the construction of EU technological sovereignty, domestic scholars have mainly conducted research from the perspectives of technological sovereignty transformation strategy, construction content, new trends, and digital governance. Transformation strategy research and content, Cai Cuihong et al. studied in the technology sovereignty discourse support, the European Union launched a number of columns of digital transformation related policies and strategies, and stressed that the transformation strategy to protect people as a grip, with internal and external dual-pointing goal, pay attention to industrial policy to promote the development of digital technology, strengthen the role of digital governance; on the trend of constructing technological sovereignty, Ma Chunguo analyses the new trend of digital sovereignty currently focusing on the antitrust of Internet platforms, increasing investment in scientific and technological innovation, advancing the integration of the EU's internal digital market, and attaching importance to international coordination in the digital field, and at the same time pays attention to the impact of the EU's construction of data sovereignty, enhances the EU's international discourse in the field of digital rules, and leads the rest of the world to adjust the digital rules and to shape the digital field. international pattern. And it is predicted that future digital regulation and technological innovation are the key to the EU's construction of digital sovereignty, linked to the process of global digital governance; on digital governance, Gong Muyun et al. studied the EU's global competition for the right to enact legislation and institutions related to digital governance, such as the

agenda-setting power game against the digital service tax, and the global competition for the governance of cloud space around the Gaia-X cloud programme .

In recent years, the concept of technological sovereignty has been a prominent topic of discussion within the European Union (EU). The idea revolves around achieving independence and control over technology, especially in terms of digital sovereignty. Foreign scholars explore how the discourse and practice of digital sovereignty can redefine European security integration. The central argument is that digital sovereignty has direct and indirect implications for European security as the EU seeks to develop and control digital infrastructures as well as use digital tools for European security governance i.e. sovereignty through digital (Bellanova, R; Carrapico, H; Duez, D). Subsequently, cloud sovereignty is proposed in the field of digital ecology, where cloud computing is a key technology for EU competitiveness in the digital economy. Two case studies are presented: the Gaia-X and the European Alliance for Industrial Data, Edge, and Cloud. Linking data sovereignty to the uncompetitive European cloud ecosystem reveals the strategic dimensions of cloud computing in a way that treats them separately (Blancato, FG). In the case of phenomena such as European defence autonomy to technological sovereignty, some studies have found that this type of shift is a means for the EU to construct its own hegemonic identity. By integrating the security imaginary into the broader process of technological governance, the EU transposes the high political logic inherent in "strategic autonomy" and "sovereignty" to increase the strategic prioritisation of technological and digital policy initiatives and instruments in the low political sphere. The eventual expansion of the concept of security has resulted in a more unified security imaginary (Raluca Csernatoni) .

As can be seen, there has been an abundance of research related to the traditional European integration dynamics, but there has been less discussion of the emerging integration dynamics. While academics have noted the development of European integration in the digital domain, the reasons behind it have not been analysed. This study attempts to fill this research gap by analysing the underlying logic of the EU's move towards deeper integration through the construction of technological sovereignty, using entanglement security as a research framework.

3. Entanglement Security and Technological Sovereignty

With the advancement of science and technology, human security relations have gradually become alienated to the "object" relationship of technology, and the "object" relationship in international relations has become the basic logic of action affecting international actors. As a result, more and more actors have begun to incorporate technology into the scope of securitisation, and the securitisation of technology has become an important factor influencing interactions between actors.

3.1 Conceptual Definition: Entanglement Security and Technological Sovereignty

3.1.1 Entanglement Security

Developments in science and technology have made security relations between States more complex. Entangled security refers to the fact that the security threats faced by actors are shifting from the clearly delineated border defence security and economic security of the past to a mixed content of security. This is manifested by the fact that, on the one hand, the topics of actors in the security field have become more complex, encompassing not only the traditional topics of security in physical space, such as military security, the economy, and the environment, but also virtual security areas, such as the field of digital space, science and technology, and so on. On the other hand, the actors involved in international relations have become more diversified, with countries not only pursuing absolute security unilaterally, but also realising that they need to cooperate with other countries in the pursuit of common security in order to make their security more secure, and thus the emergence of security subjects that go beyond the state.

Therefore, this paper proposes a new concept of "entangled security", which is a new type of security that deviates from the traditional security in three dimensions: security relations, security boundaries and security space. Usually, what we call security is characterised by a clear single security subject, military security and other physical security as the core content, and clear and single security boundaries between actors. Under the perspective of entanglement security, firstly, the security relationship has been alienated into the relationship between things, technology has become the main content of international competition, and the actors involved in international competition have also appeared a diversified trend, including states, supranational actors, international organisations and other types of actors active in the international community. While national security is emphasised, attention is also paid to the status of supranational actors as security subjects; secondly, security boundaries are characterised by the coexistence of clear and fuzzy features in different fields, and are developing in the direction of mutual dependence on the real and the imaginary. Containing both military security, economic security, political security, environmental security and other physical space security areas, while also focusing on virtual security, a new security space spawned by technological development; and finally, security borders are increasingly blurred, with the emergence of fuzzy security borders between countries, such as the refugee crisis, climate warming, and the need for countries to jointly govern, the The blurring of security beyond the borders of supranational actors and borders, such as the impact of the European debt crisis on global economic security, as well as the emergence of new areas such as digital space, which is itself characterised by blurred borders.

3.1.2 Technological Sovereignty

The construction of the concept of "sovereignty" at the EU level focuses on specific areas in order to achieve control and mastery over the relevant issues. The starting point of the EU's construction of "technological sovereignty" is to ensure the integrity and resilience of data infrastructures, networks and

communications, in the hope of empowering itself through the concept of "sovereignty" and enhancing the effectiveness of EU digital governance.

In 2017, French President Emmanuel Macron first proposed the construction of EU technological sovereignty in his speech at the Sorbonne University under the title of "A New European Initiative ". In 2018, European Commission President Jean-Claude Juncker argued that the EU should become a more sovereign actor in international relations actor. In 2020, the new President of the European Commission, Ursula von der Leyen, has successively launched a programme of the concepts of "technological sovereignty", "economic and financial sovereignty", and "digital sovereignty". At the same time, the European Commission released three important digital strategy documents, including Shaping Europe's Digital Future, the White Paper on Artificial Intelligence and the European Data Strategy, which centred on the notion that the EU must reclaim its 'technological sovereignty'. Overall, EU leaders' speeches and policy documents have repeatedly mentioned the concept of "technological sovereignty", and are committed to enhancing the EU's international status and competitiveness in the field of science and technology through the construction of "technological sovereignty".

At present, the concepts of "technological sovereignty", "digital sovereignty" and "data sovereignty" often appear in the EU discourse, which are applicable to different scenarios and fields due to their different focuses and core concerns. and domains. As mastery of digital strategy is not only a matter of digital technology, but also limited by technology, without mastery of technology, there is no autonomy of digital strategy. This is why this paper discusses "technological sovereignty" rather than "digital sovereignty". "Technological sovereignty" refers to the ability to develop, deploy, apply, acquire and guarantee the integrity of key technologies that, in this era of geopolitical competition in which we live, have become instruments of power acquisition, it is more responsive to the EU's political need to use technology as a means of macro-control for EU security shaping, to enhance the EU as a whole, and to deal with the entangled security that comes with the complexity of security issues.

3.2 Entangling Security Issues Facing the EU

As defined above, entangled security is characterised by ambiguity and entanglement in the three dimensions of relations, borders and space, where security issues in various spatial and temporal domains converge and influence each other. At the level of the European Union in particular, entangled security presents more complex phenomena and issues.

3.2.1 Relational Entanglement

Interaction Alienation of Security Relations The alienation of science and technology has reshaped the way in which countries interact with each other. The development of science and technology, with its unique value, has created a brand-new mode of human interaction, reshaped the new space of human social interaction, and brought about new changes in interpersonal communication. It is mainly reflected in the emergence of new technologies, which makes the alienation of the way of human interaction, which is manifested in the alienation of the interaction mapping relationship. That is, as the medium or

object of interaction, technology in turn controls and dominates the relationship of interaction between people. The tool of interaction as a product of labour should have been the intermediary for realizing the need of interaction between the subject and the subject, as Marx said, "Your product is the instrumental means to possess my product and thus satisfy your needs." But the strong potential power brought by the development of technology will make people go beyond the boundary of the tool and unconsciously regard it as another subject or even a "partner". For example, both the virtual world and the real world in cyberspace have an important impact on human social existence, and even though the real world takes precedence, it is difficult to detach from the impact of the scene created by virtual technology in cyberspace on human beings, which ultimately makes the technology not only have the nature of potential power that can be realised, but also have the characteristics of initiative as a competitive subject.

Ultimately, science and technology have led to a shift in human interaction from a reliance on physical objects such as commodities, goods, and capital to a reliance on information, data, and intelligence, and even to some technologies that can interact directly with people. The development of technology has led to the gradual alienation of human security relations into a technological "object" relationship, and the "object" relationship in international relations has become the basic logic of action affecting international actors, leading to new changes in interactions between States. In the past, technological means were regarded as the soft power of a country's comprehensive strength, but there is a possibility that they may evolve into hard power, the importance of which is reflected in their impact on industrial production capacity and expected returns, while the alienation of science and technology has transformed its original role as an object of interaction into the main factor of competition between countries. As a result, more and more countries have begun to incorporate technology into the category of securitisation, and the securitisation of technology has become an important influencing factor in inter-state interactions.

Overall, technological development has alienated the interaction between people and people, and between countries and countries, making the issue of technology show a trend of securitisation, and to a certain extent, reshaping the EU's perception of security threats in the field of technology. Technological sovereignty has risen to become an important political security issue, and has become a core element of the EU's international competition, reinforcing its political authority in technological governance through the construction of an "external threat", and giving legitimacy to the EU's internal and international technological policies, thereby rationalising non-conventional administrative interventions.

3.2.2 Spatial Entanglement: The Imaginary and the Real in Security Space

The security space for actors has both physical and virtual dimensions. On the one hand, the physical security space with clear boundaries, such as territory, military, economy and diplomacy, is the main content of actors' security; on the other hand, the virtual security space, which is the result of

the wave of scientific and technological development, such as the digital and cybersecurity space and the various kinds of practical activities hosted by online platforms as trading venues, is an even more important threat to be dealt with by actors in the wake of the information technology revolution. With the development of non-traditional security issues and digital technology, the EU's security content is also expanding from physical space areas such as security and defence, economy and trade to multi-dimensional areas, forming a security space from the physical to virtual and physical hybrid situation.

In terms of security in physical space, the main threats facing the EU today are global challenges such as economic globalisation, great power competition, climate change and natural resource scarcity, regional challenges such as regional instability and inter-state tensions, and EU-specific security threats such as terrorism and anti-integration camps. Physical space security is most clearly characterised by country-specificity and duality, with well-defined security boundaries, and when faced with this type of security threat, the EU level has the capacity to develop coherent and holistic policies to counteract it, and is rarely subject to external pressure on foreign policy from other actors.

The post-Cold War process of technological development and globalisation has led to a broadening of the range of threats faced by the EU, where the threat of a national military offensive is no longer imminent, the concept of security has expanded to include the digital, cyber and social domains, and threats have been described as hybrid and spatial in nature. In this context, the European Union (EU), which once attached importance to the public domain attribute of digital space, has revived the concept of "sovereignty" in global digital governance, and new concepts such as "digital sovereignty" and "data sovereignty" have returned to the EU's political discourse in the form of "digital sovereignty" and "data sovereignty". The concept of "digital sovereignty", "data sovereignty" and other new concepts have returned to the EU's political discourse. This type of virtual security space has brought new governance space to the EU, for example, cyberspace as a newly emerged geopolitical contestation site, due to its imperfect system, lack of country-specificity and regulatory boundaries, resulting in cybersecurity, such as virtual space security dimensions tend to become a state actor or non-state actor security loophole.

Therefore, the ambiguity of security in space makes "how to further translate the achievements and advantages of the EU's internal countries in the field of science and technology into the EU's discourse and global leadership" one of the key agendas of the EU's diplomacy. The EU hopes to enhance its scientific and technological strength and global influence by shaping a unified internal scientific and technological standard, strengthening research and development in the field of science and technology, and providing financial support to jointly promote scientific and technological innovation.

3.2.3 Borderline Entanglements: The Security Border Problem Facing the EU

Currently, the blurring of military and civilian boundaries within the EU, the blurring of security within and beyond a country's borders brought about by non-traditional security issues, and the blurring of security boundaries such as digital space as a new space of competition with its own unclear regulatory governance are all factors that have an important impact on the EU's concept of security.

Firstly, there is a trend towards increasing blurring of the military-civilian border. In international relations, when it comes to core areas of national security or state monopolies such as military aerospace technology, military positioning systems, lasers, etc., there is usually a clear demarcation between the military and civilian domains. Many of the "civilian" technologies we use today are derived from military technologies. Some military communications, satellite navigation and flight technologies were originally developed for the military. However, they have since found widespread use in civilian applications, such as satellite navigation systems and civil aviation. Similarly, cybersecurity technologies are used not only in the military domain to defend against cyberattacks, but also in the civilian domain to secure corporate and personal information. As a result, the line between military and civilian applications is becoming increasingly blurred, with technology consistently shifting between the two.

Secondly, there is a trend towards increasing blurring of boundaries within the EU and outside the EU. Within the EU, security is a sovereign matter for the member states due to its high political nature, and each member state formulates its own national security strategy, at which time the security boundaries between countries within the EU are relatively clear. With the deepening development of integration, the common security threats faced by member states have increased, and the need for coordination of security and defence policies has arisen. Therefore, the EU has begun to formulate a class of "national security strategy" documents to cultivate a common strategic culture, integrate the resources of member states, and form a stronger security capability. Since then, the EU's security borders have become increasingly blurred.

On the one hand, on the issue of the EU's internal security borders, there is the question of how much national sovereignty is to be ceded to the EU level, of which the empty chair crisis was a protest by France fearing too much power at the EC level. Since then, there have been many attempts within the EU to cede more power to the EU level to enhance the overall international competitiveness of the EU. 1986, the Single European Act for the first time in the legal documents to include the topic of security, the Maastricht Treaty of 1993 to establish the EU, the member states will be the implementation of the Common Foreign and Security Policy (CFSP), and towards the formation of a common defence policy or even the direction of the Common Defence. 2009, the Treaty of Lisbon from the mechanism of the EU to the EU level, the EU has been the first time that the EU has been a member of the European Union. The Lisbon Treaty of 2009 enriched and improved the EU's Common Security and Defence Policy in terms of mechanisms, decision-making modes, etc., and elevated the status and importance of this political issue in European affairs.

On the other hand, in terms of the EU's internal and external security borders, the boundaries between the EU and other actors have become increasingly blurred due to the emergence of non-traditional security issues, and the EU has become increasingly involved in each other's affairs and more and more affected by affairs beyond its borders. An example of this is the international financial crisis that erupted in 2008, which then quickly spread to the European financial markets and dealt a severe

blow to the real economy. This crisis triggered the European sovereign debt crisis, which led to a series of serious social problems and political consequences, such as weak economic growth, high unemployment, sluggish domestic demand and inflationary contraction. As a result, the European debt crisis has made the economic security border between EU countries and the outside increasingly blurred. Secondly, the influx of large numbers of Middle Eastern and North African natives into Europe since 2014 has affected the social order in Europe and become a hotbed of social conflicts and criminal activities. Finally, the Ukraine crisis has made the EU face unprecedented geopolitical challenges and security problems since World War II, and Russian-European relations have plunged into the lowest ebb since the Cold War, bringing huge economic losses to the EU, triggering huge internal disputes and disagreements, and at the same time increasing geopolitical risks.

Finally, the digital space itself is characterised by ambiguity at the boundaries also exacerbates the EU's blurring of security boundaries. The current perception of the attributes of cyberspace has the ambiguity of "global commons" and "national sovereignty". In order to realise its goal of global hegemony, the US regards cyberspace as a "commons" attribute, considering it a virtual space created by all mankind and incorporating it into its global commons strategy. On the other hand, the United States holds that cyberspace belongs to the information infrastructure of a country, and has the attributes of country-specificity and sovereignty; therefore, cyberspace should be managed by a sovereign country to maintain the stability of cyberspace, protect the security of cyberspace, and combat cybercrime, etc., and therefore, cyberspace belongs to an important part of national sovereignty.

In conclusion, the development of science and technology has led to the alienation of security relations between actors, and technology has become the new subject of competition between countries; the abundance of security issues has made the European Union (EU) face the security threat of real and imaginary; the blurring of security boundaries has made the EU face the governance dilemma of unclear jurisdictional competence, and the entanglement of security issues has become a major challenge in the integration process of the EU, and also an issue to be solved urgently to promote the development of the new round of integration. It is also a problem that needs to be solved in order to promote a new round of integration development.

4. The Power Shift of European Integration in the Context of Entangled Security

The current situation of entanglement security has prompted the European Union to seek a new direction of integration, "technological sovereignty" is proposed in this context and has become a new source of impetus to promote European integration, and the construction of "technological sovereignty" is a better response to the challenges posed by entanglement security to Europe. The construction of "technological sovereignty" is a better response to the challenges posed to Europe by entangled security.

4.1 Construction of Security Relations: Strengthening Identity

As mentioned above, the alienation of security relations brought about by technological progress has made the relationship between "things" an important factor influencing the security of actors, and

within the European Union, the existence of different technological standards, competences and resource advantages between countries will result in internal technological barriers and unhealthy technological competition, which is not conducive to the shaping of the overall strength of the European Union. Therefore, the construction of "technological sovereignty" is emphasised to strengthen the identity of the EU, satisfy the interests of member states, and build a unified discourse system, so as to achieve the goal of building a single digital market.

Firstly, the construction of "technological sovereignty" of the EU can satisfy the interests of member states, closely link the security of the EU and the security of member states, and give deeper impetus to integration. The international community prioritises the self-interest of member states, and the main reason for the deepening of European integration is the interests of member states in the political struggle for power in an anarchic state. The development of common science and technology can externally improve the competitiveness of the EU community in the international community and markets, internally support economic growth and job creation, reduce the uneven distribution of strategic resources in the European region, and bridge the technological gap between advanced and more backward countries in the EU.In 2020, the European Commission published its Data Strategy for Europe, which envisages investing in an EU data space and cloud infrastructure integration-related In 2020, the European Commission released the European Data Strategy, which plans to invest in a project related to the integration of the EU's data space and cloud infrastructure, focusing on areas such as edge computing, high-performance computing, cybersecurity, and 6G networks, which are crucial for the future development of the data infrastructure, so that the EU will have the appropriate infrastructure, computing power, encryption capacity, and cybersecurity tools to process data.

Secondly, the EU's construction of "technological sovereignty" can build a unified discourse system and promote the concept of European governance. On the one hand, as a more flexible and pragmatic discourse system, "technological sovereignty" can internally build consensus and promote the integration of the internal digital space, for example, the EU's White Paper on Artificial Intelligence of September 2020 pointed out that the EU's AI should be based on the EU's values and fundamental rights, and play a role in achieving sustainable development, supporting the democratic process and safeguarding social rights. and safeguarding social rights; and the EU Cybersecurity Strategy, presented in 2020, states that geopolitical tensions have exacerbated the threat landscape, thereby threatening the EU's core values. Therefore, the EU needs to promote a model of cyberspace governance based on the rule of law, human rights, fundamental freedoms and democratic values. On the other hand, the construction of "technological sovereignty" externally supports the EU's ideology of digital space governance and the promotion of EU values, complementing the two initiatives at the institutional and technological levels, which together serve the goal of achieving the EU's dominant capacity and returning to leadership. For example, the EU is supporting Africa's digital transformation in the name of "technological sovereignty", helping Africa to establish a single African digital marketplace, and

discussing the establishment of a "trusted data alliance" with partner countries that share European values and high standards;

Finally, the EU's construction of "technological sovereignty" could create a single digital market within the EU. The EU has a large base of Internet users, but the digital market is fragmented, as reflected in the high number of cross-border barriers that prevent the free flow of data, and the fragmentation of research and development that hinders the development of cross-border SMEs and cross-border business in the digital field, and is not conducive to attracting investment in the development of core technologies. To address the problem, the EU has tried to establish a digital single market. in 2010, the Digital Agenda for Europe put forward the goal of establishing a single digital market. in 2015, the Single Digital Market Strategy integrated the internal market through a series of standards and regulations, paving the way for the creation of a favourable environment for development. Also in 2020, the Long-Term Action Plan for a Better Implementation and Enforcement of the Single Market Rules was adopted, with the main objective of addressing barriers to EU legal rules. In the same year, the European Data Strategy set out plans to create a European public data space to enable cross-industry flows of data within the EU, further contributing to the development of a single European digital market. By the end of 2021, the construction of public data spaces in various fields had taken shape, such as a common European financial data space.

4.2 Construction of Security Borders: Expanding Geospatial Contestation

In the case of entanglement security, the shift in security content from physical security to the intertwining of virtual and physical security has made the European Union realise that geo-strategic thinking is reshaping the future of the digital space, and that the game of digital geo-strategy between the major powers has begun, and that the changes in the international landscape in the field of digital technology are compressing the space for the European Union's strategic autonomy. The EU urgently needs to build up a security border through the construction of "technological sovereignty", and seize the first opportunity in the international competition from both virtual and physical directions, so as to enhance the EU's international discourse power, promote industrial progress, and expand the geo-strategic competitiveness in the international arena.

Firstly, the construction of "technological sovereignty" by the EU can enhance the EU's international discourse and influence. Overall the EU's digital technology in the world belongs to a leading position, mastering the application of artificial intelligence manufacturing, 5G network technology, information technology giants, etc., but there is a clear internal "digital divide". In this regard, in early January 2021, the European Union started to implement the ninth phase of the R&D framework programme "Horizon Europe" (2021-2024), which is considered to be the world's largest R&D programme. Considered to be one of the largest publicly funded science and technology programmes in the world, the mission of the programme is to enhance science and technology, address societal issues and promote economic development. Specifically, the "Global Challenges and European

Industrial Competitiveness" pillar focuses on supporting applied research to address societal challenges and to improve the technological competitiveness and industrial level of the EU, forming a "6+1" structure of research clusters in areas such as health, culture, social security, digital industry, etc.; the "6+1" pillar focuses on supporting research in the fields of health, culture, social security, digital industry, etc. The "Innovative Europe" pillar focuses on supporting industrialisation, aiming to turn the EU's research strengths into innovation (industrial) strengths. This pillar is dedicated to supporting SMEs and start-ups in their activities such as breakthrough innovations in order to stimulate market dynamics. At the same time, it promotes the integration of education, research and innovation, and facilitates coordination with Horizon Europe and other funding programmes. In terms of locally specific projects, the pillar promotes deeper cooperation between innovation actors in each region.

Secondly, the construction of "technological sovereignty" in the EU can speed up the construction of infrastructure and promote the progress of the technology industry. The EU is accelerating the deployment of new infrastructure construction to shape the competitive advantage, and vigorously promote the deployment of secure 5G networks, launching the European cloud programme Gaia-x. 2020 introduced the "5G Network Security Tools Guidance Document" put forward for the supply chain, the main threat actors, end-users, and other risks to formulate the corresponding mitigation measures, including member states in the access privileges, security operations, monitoring rules, specific function outsourcing and other aspects, to improve the security of the member states in the access privileges, security operations, and monitoring rules, specific function outsourcing, etc.; in addition, member states are required to conduct risk assessments of suppliers and restrict high-risk suppliers involved in core network construction, while maintaining supply chain diversity and sustainability to avoid over-reliance on a single supplier. In 2019, Germany and France jointly proposed an initiative to build an EU "Gaia-x" programme for cloud services, which aims to establish a secure data infrastructure framework that connects cloud service providers in the EU and reduces reliance on foreign cloud service providers such as Amazon, Microsoft, Google, etc., so as to improve data security and safeguard data sovereignty, and seeks to build a secure decentralised cross-enterprise IoT data space on the basis of this model.

Finally, the EU's construction of "technological sovereignty" could expand the contestation of cyberspace and territorial space. The process of this construction is twofold: on the one hand, the promotion of research and development and the establishment of standards for emerging technologies expands competition in cyberspace; on the other hand, the perception of the network as a medium of communication in physical space expands competition in areas such as geopolitics and economic trade. As a result, the EU has made significant adjustments to its cyber strategy. By way of example, member states and businesses are encouraged to undergo digital transformation and invest in key technology areas such as artificial intelligence, big data, the Internet of Things and blockchain; build advanced cyberinfrastructure, including high-speed broadband networks, 5G networks, and satellite communication systems to enhance communication and connectivity in cyber and territorial space; and implement cybersecurity regulations to strengthen cyber surveillance and defence capabilities to

respond to cyberspace threats and attacks and ensure the security of cyber and territorial space; and co-operate with other countries and regions to jointly develop technical standards and norms. Through collaboration with international organisations and partners, the EU can play a leading role in cyberspace and shape the global landscape of technological development.

4.3 Construction of Safe Spaces: Shaping New Jurisdictions

The blurring of security borders makes the EU's jurisdictional competences unclear, and security within and between the EU's borders is often challenged. For example, the digital sphere, cloud space and other emerging areas of competition among great powers are themselves characterised by unclear borders, coupled with the lack of large Internet companies in the EU and the fact that information security is in the hands of technology giants in extra-territorial powers, which has made the EU's claim to power in the digital sphere even more urgent. In this case, the EU tries to build a security space to ensure the collective security of the EU by constructing "technological sovereignty" and shaping its jurisdiction over emerging spatial domains such as cyberspace.

For a long time, the division of jurisdiction between the EU and its member states has been one of the important issues in the European planning process. Under the federalist conception, the EU's jurisdiction lies in the policy of increasing efficiency and protecting the market with the aim of removing obstacles to the free movement of people, services, goods, and capital within the Union's borders, with the drawback that it is not possible to decide concretely which jurisdictions should be configured to the EU, and which jurisdictions should be retained at the national level of the member states. Functionalism in the 1950s proposed that member states delegate tasks such as regulation and enforcement to a supranational supreme directorate-general (known as the European Commission), and that member states focus more on the diffusion of automatic processes of spillovers into other areas, expanding from areas such as nuclear energy, tariffs, and trade, to incomes, social security systems, monetary credit tax system, and investment planning, among other areas.

This extension of competence did not grow linearly, and the rules it set were no longer implemented or complied with by the governments of the Member States as they should have been, and there was a "spillover effect", which has since been repeated in the mainstream of the extension of the Community's competence and in the mainstream of protectionism. At this time, Community jurisdiction was determined by the social demand for Community regulations in cross-border transactions, and increasingly, common market jurisdiction was centralised, mainly in the telecommunications and civil aviation industries. Neoliberal institutionalism, with its emphasis on the dynamic impact of the system, highlighted the role of the European Court of Justice (ECJ), which, through its expansive interpretation of treaty provisions and the creation of legal precedents, had already greatly influenced jurisdiction in terms of jurisdiction and interpretation of EC law. At this point, jurisdiction is not limited to purely economic matters or matters such as deregulation, but also extends to areas such as labour health and safety, social welfare, mutual recognition of educational and professional qualifications, and the right

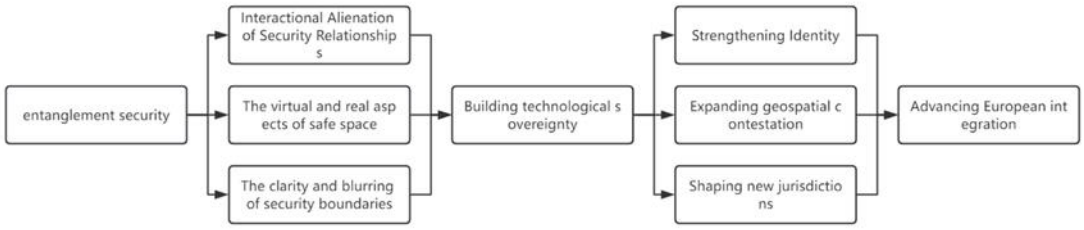
to political participation. In today's US-China technological competition, the global science and technology landscape and global governance structures, including the digital domain, are being reshaped. EU scholars have pointed out that core powers use technological dependence as a means of advancing their own interests in the digital economy, and that technology has thus become a weapon for these core powers to exert political pressure and economic influence on other asymmetrically dependent countries and firms.

It can be seen that the EU's core strategy in the digital sphere has gradually shifted from the past pursuit of technological advancement and mastery of advanced technologies to the right to formulate and speak on the rules of the global digital sphere, and then to the fight for jurisdiction over digital space, cyberspace, etc., reflecting the EU's exploration of how to use its strengths in the formulation of regulatory rules and laws, redefining the ideology of the digital space, and integrating the EU's discourse into the rule-making in the global digital space, and then promote the EU path globally, and ultimately establish its global leadership ground .

The shift in the demand for the right to technological governance has prompted the EU to hope to reduce its dependence on extraterritorial digital dependence through the construction of "technological sovereignty", and to enhance the overall digital technology to safeguard the security of the supply chain. In recent years, with the prevalence of U.S. unilateralism and the expansion of long-arm jurisdiction, the EU has faced a steep increase in security risks in terms of critical digital infrastructure and data information. For example, the US has used its strength and advantage in the supply chain chain chain to suppress and coerce Chinese technology companies and hinder their technological development. In a situation of renewed geopolitics, the EU also needs to consider the security of its own supply chain, especially to reduce its external dependence in the digital sphere. When exchanging data, it is important to ensure continuity of access control across the data value chain, and the EU Data Strategy sets out a framework for cross-industry governance of data access and use, according to which the first step is to empower the governance of the European public data space and improve the legislative framework. Secondly the Commission will work more on making more high-quality public sector data reusable, especially considering the potential of relatively small and medium-sized enterprises (SMEs).

In summary, the EU is characterised by the entanglement of security due to technological developments that have led to the alienation of security relations, the expansion of security space, the blurring of security boundaries and other such shifts in security content. Under such circumstances, it is necessary to seek new impetus to stimulate the vitality of the EU. Therefore, this paper seeks to strengthen the identity of the EU, expand the geospatial competition, and shape new jurisdictions through the construction of "technological sovereignty", so as to promote the further development of European integration.

Figure 1: Mapping Entangled Security and European Integration



5. Conclusion

In the era of globalisation, in the face of the emergence of non-traditional and entangled security, European integration has taken a new turn towards "technological sovereignty", but relevant studies have paid less attention to this change. This paper argues that the reason for the EU to promote the further development of European integration through the construction of "technological sovereignty" comes from the complexity of the current security environment, especially with the emergence of "entanglement security", the security environment and security structure of the European Union has undergone a major transformation. This paper first defines the concepts of entanglement security and technological sovereignty, and focuses on analysing entanglement security in terms of the three dimensions of relations, space and borders. At the EU level, entanglement security exhibits more complex phenomena and issues. In view of this, the EU has promoted a shift in integration towards "technological sovereignty", constructing security relations and strengthening identity through the construction of "technological sovereignty", while promoting the construction of security space and security borders as a means of expanding geospatial competition and shaping new jurisdictions, and promoting the continued and deeper development of European integration. promote the continued and deeper development of European integration.

The research in this paper provides a new perspective for analysing EU integration research, but the shortcomings of this paper are that it does not quantify technological sovereignty or develop the theory of entanglement security, which is, of course, the direction of this paper's future research. In the future, this study will also further analyse what kind of technological sovereignty has an impact on EU integration.

Acknowledgement

None.

Funding Statement

None.

Author Contributions

The author confirms sole responsibility for the following: study conception and designdata collection, analysis and interpretation of results, and manuscript preparation.

Availability of Data and Materials

The data for this study are derived from publicly available literature and news reports, which have been listed in the references.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1]. Gong Yunmu. (2022) The return of the concept of sovereignty in the digital age and the EU 's digital governance. European study (03), 18-48 + 165 + 6.

[2]. Feng Yiran: "Fusion of supranationalism and intergovernmentalism: EU's new defense construction initiatives and prospects", "International Security Studies", Issue 5, 2020.

[3]. Fang Lexian, Di Chongguang: "New progress in EU security and defense construction: permanent structural cooperation and its meaning", "Contemporary World and Socialism", Issue 3, 2018.

[4]. Li Xia, Shi Di: "Deepening of European Financial Integration", "China Finance", Issue 20, 2018.

[5]. Wang Jue: "From Technocrats to Political Bureaucrats: Research on the Politicization of the European Central Bank", "Foreign Social Sciences", Issue 3, 2020.

[6]. Zhong Yichen, Luo Yingjie: "Research on European Integration: New Public Management Reform in European Integration - Taking the Supranational Political Agency in the EU Judicial and Internal Affairs Fields as an Example", "European Studies", Issue 3, 2019.

[7]. Cai Cuihong, Zhang Ruoyang: "The EU Digital Transformation Strategy under the Discourse of "Technological Sovereignty" and "Digital Sovereignty", International Political Studies, No. 1, 2022.

[8]. Gong Yunmu: "The Return of the Concept of Sovereignty in the Digital Age and EU Digital Governance", European Studies, No. 3, 2022.

[9]. Bellanova, R, Carrapico, H and Duez, D, Digital/sovereignty and European security integration: an introduction, European Security, 2022, pp337-355.

[10]. Blancato, FG, The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem, Policy and Internet, 2023.

[11]. Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & technology, 33, 369-378.

[12]. Csernatoni, R, The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty, European Security, 2022, pp395-414.

[13]. Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8(1), 2053951720982012.

[14]. Pohle, J., & Thiel, T. (2020). Digital sovereignty. Pohle, J. & Thiel.

[15]. Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021). The road to European digital sovereignty with Gaia-X and IDSA. IEEE network, 35(2), 4-5.

[16]. Gong Yunmu: "The Return of the Concept of Sovereignty in the Digital Age and EU Digital Governance", published in "European Studies", Issue 3, 2022.

[17]. Ma Guochun: "New Trends in the EU's Construction of Digital Sovereignty and Its Impact", in "Modern International Relations", Issue 6, 2022.

[18]. Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. European journal of cultural studies, 21(5), 594-613.

[19]. Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital?. New media & society, 21(10), 2305-2322.

[20]. Lambach, D. (2020). The territorialization of cyberspace. International Studies Review, 22(3), 482-506.

[21]. Mueller, M. L.(2020). Against sovereignty in cyberspace. International studies review, 22(4), 779-801.

[22]. Emmanuel Macron, "President Macron Gives Speech on New Initiative for Europe," Élysée, 26 September 2017, https: / / www. elysee.fr / emmanuel-macron /2017 /09 /26 / president-macron-gives-speech-on -new-initiative-foreurope.en.

[23]. Jean-Claude Junker, "State of the Union 2018: The Hour of European Sovereignty," European Commission. 12 September 2018, https: / / ec.europa.eu / info / sites / default / files / soteu2018-speech_en_0. pdf.

[24]. Ursula von der Leyen, " A Union that Strives for More-My Agenda for Europe," European Commission, 14 July 2019, https: / / ec.europa.eu / info / sites / default / files political-guidelines-next-commission_en_0. pdf.

[25]. Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital?. New media & society, 21(10), 2305-2322.

[26]. Jennyfer Chrétien, Etienne Drouard, Guillaume Buffet, et al. Guillaume Buffet, et al, "European technological sovereignty", February 15, 2022.

[27]. Cheng Hongyan & Guo Xiaqing. (2020).Exploration of communication alienation caused by artificial intelligence. Research on Dialectics of Nature (09), 70-74.doi : 10.19484 / j.cnki.1000-8934.2020.09.013.

[28]. Zhang Jian. (2022). EU Security Strategy : Origin, Evolution and Policy Trends. Contemporaneous International Relations (05), 1-32.

[29]. Weingast, Br. (1995).The Economic-Role of Political insitutions: market-preserving federalism and economic development. Journal of Law, Economics, & Organisation, 1-31.

[30]. Zheng Chunrong & Jin Xin. (2022).The background, path and challenge of EU digital sovereignty construction. Contemporary World and Socialism (02), 151-159.doi : 10.16502 / j.cnki.11-3404 / d.2022.02.013.