ATHENÆUM
Polish Political Science Studies
Polskie Studia Politologiczne

vol. 76(4)/2022, pp. 127–148
DOI:10.15804/athena.2022.76.07
www.athenaeum.umk.pl
ISSN 1505-2192

DIGITAL TECHNOLOGIES AND THE PROSPECTS OF THE EUROPEAN UNION'S STRATEGIC AUTONOMY*

TECHNOLOGIE CYFROWE A PERSPEKTYWA AUTONOMII STRATEGICZNEJ UNII EUROPEJSKIEJ

*Tomasz Gajewski***

ABSTRACT

The aim of this study is to examine the impact of digital technologies on the creation and final shape of the EU's strategic autonomy. The author employed the network institutionalism as a theoretical basis and applied a critical analysis of the available material. The following hypothesis is positively verified: development of digital technologies is modifying strategic autonomy and extending it beyond the logic of freedom of political and military action. Digital resilience of core areas of EU's functioning should be at the heart of this concept. The author argues that this model of strategic autonomy (enhanced by the close alliance with the United States) will enable the EU to strengthen its global position in technologically driven world. Less politicization is also a key reason for such a solution. It is particularly important in the context of the crisis of European integration.

ABSTRAKT

Celem niniejszej analizy jest zbadanie wpływu technologii cyfrowych na budowę i ostateczny kształt autonomii strategicznej UE. Autor przyjął sieciowy instytucjonalizm jako podstawę teoretyczną wywodu i zastosował metodę krytycznej analizy dostępnego materiału. Pozytywnie zweryfikował postawioną hipotezę, zakładającą, że rozwój technologii cyfrowych modyfikuje autonomię strategiczną i rozszerza ją poza logikę swobody działań polityczno-wojskowych. W centrum tego konceptu znajduje się natomiast odporność kluczowych, zdefiniowanych przez technologie cyfrowe obszarów funkcjonowania UE. Autor dowodzi, że budowa tego rodzaju autonomii strategicznej (wraz ze ścisłym sojuszem technologicznym z USA) pozwoli UE wzmocnić pozycję globalną. Za podjęciem jej budowy przemawia także mniejsze upolitycznienie, co jest szczególnie istotne w warunkach kryzysu integracji europejskiej.

* Research forming the basis of this article, involving study visit to European Parliament Research Service in Brussels and structured interviews with Members of European Parliament, was financed from Jan Kochanowski University grant "Technological Dimension of the European Union's Strategic Autonomy" (SUPB.RN.21.072).

** Jan Kochanowski University in Kielce, Institute of International Relations and Public Policy.

Keywords: European Union; strategic autonomy; digital technology; resilience; security

Słowa kluczowe: Unia Europejska; autonomia strategiczna; technologie cyfrowe; odporność; bezpieczeństwo

INTRODUCTION

Dynamic changes in the architecture of the international system prompt state and non-state actors to take adaptation measures. The most important factor behind these changes is the US-Chinese competition for global primacy. Its impact is visible almost anywhere in the world. Alongside the Asia-Pacific region, which is the main theater of struggle, the European Union retains peculiar role in the ongoing rivalry.

As an integration project bringing together traditional US allies (also within NATO) and economically connected in many ways with China, the European Union is looking for its role in the world, while also dealing with the major internal crisis. However, the pace and direction of change on the global stage has led the Community institutions and the leaders of the most important Member States to discuss strategic autonomy. Its simplest definition assumes that it is a condition where an entity can formulate interests and objectives and freely take independent or cooperative actions in the international environment to implement them. This applies primarily to foreign and security policy. This concept has been circulating for years in the documents of the EU institutions (Conclusions – 19/20 December, 2013; *Shared Vision, Common Action…*, 2016).

The need to build it is particularly emphasized by France, which traditionally seeks ways to balance the position and influence of the United States in Europe. Continuing the political line initiated by President Charles de Gaulle, President Emmanuel Macron presented his vision of a "sovereign Europe" (*Sorbonne Speech of Emmanuel Macron*, 2017). This would constitute a European response to the then US President Donald Trump's policy and the UK's exit from the EU structures. French concepts place particular emphasis on autonomy in the field of security policy and military crisis response capabilities – particularly in areas where the strategic interests of France are located, primarily in North Africa and Sahel. However, new collective defense projects in Europe aimed, in the light of these concepts, at extending French nuclear deterrence to the EU as a whole and at engaging in strategic dialog with Russia, have been seen as an attempt to undermine NATO's role. The French concept is read as a sole instrument for

seeking independence from the United States. Admittedly, Macron has departed from the term 'sovereignty' in favor of the term 'strategic autonomy' (Gressani, Malik, & Bloj, 2020), but this has not fundamentally changed the perception of French concepts. In Germany in particular, the attachment to the transatlantic alliance with the United States as a guarantor of European security has proved especially strong (Rahman, 2021).

The weakness of the divided EU in global relations is striking. In the light of the deep problems of the European project, strategic autonomy is regarded as a "pipe dream". There is also no shortage of voices that France wants to make the strategic autonomy a "vehicle" to pursue its own interests. However, this does not mean that the debate on the need to develop a strategic autonomy exists only in the political projects of the individual Member States. Following the European Council meeting on February 26, 2021, the President of the European Council, Charles Michel, stated that the Community would increase its capacity to act independently, but in close cooperation and coordination with NATO and the United States. This was a response to the statements by the newly elected US President Joseph Biden announcing "return of America" (Bielecki, 2021).

This, necessarily limited, outline shows the framework of the debate on European strategic autonomy. It is delineated by the political weakness of the EU itself, the differences in interests and perceptions of threats in Member States; the parameters of the global situation; the influence of external actors – both allies (the United States) and potential and real adversaries (Russia, China).

The European discussion on strategic autonomy focuses mainly on the military dimension. Although more detailed analyzes refer to the industrial base, the resilience of critical infrastructure, cyber security, value chains and energy, the discussion on strategic autonomy is most intense when it comes to military capabilities or, more widely, the ability to actively define situation in the international environment. The impact of dynamic development of digital technologies such as 5G networks, artificial intelligence, nanotechnology and quantum computing is an important, but fundamental element in defining European strategic autonomy. However, these issues are dealt with as part of a separate concept – the "technological sovereignty". The observed pace of development and the impact of digital technologies on all functions of social and political systems require that they be assigned a different rank within strategic autonomy concepts. Digital technologies will redefine many aspects of states' and society's realities. Many instances of these transformations can be seen contemporarily. Consequently, the concept of strategic autonomy will also be modified. Strategic autonomy also

means that the entity is technologically "capable of" and "immune to". It also has, of course, a political dimension. "Sovereignty", on the other hand, is not attractive or even acceptable for the EU and its Member States.

As elaborated, the strategic autonomy of the European Union is not a new idea. In addition to the political debate at EU and Member State level, the interest in this concept is reflected in scientific research.

LITERATURE REVIEW

There are many publications in the international scientific input which take up a conceptual analysis of European strategic autonomy, focusing primarily on their political and military dimensions (e.g., Bellou, 2021; Bartels, Kellner, & Optenhögel, 2017; Chappell, Mawdsley, & Petrov, 2018; Fägersten, 2020; García Pérez, 2019; Grevi, 2021; Howorth, 2018; Knutsen, 2016; Meijer & Brooks, 2021; Noël, 2019; Pieper & Lak, 2019; Ryon, 2020; M.E. Smith, 2018; Zieliński, 2020). A European approach to strategic autonomy, defined on the basis of the freedom of offensive political action, supported by military force, is being examined in the works about development of the Common Foreign and Security Policy, Common Security and Defense Policy, Permanent Structured Cooperation and other similar EU initiatives (e.g., Allen, Hodges, & Lindley-French, 2021; Dijkstra, 2021; Egeland & Pelopidas, 2021; Fiott, 2019; Karampekios & Oikonomou, 2015; Timmers, 2018; Sweeney & Winn, 2020; Trybus, 2014; Violakis, 2020; Voskopoulos, 2021). The defence industry plays an important role in these publications, which emphasizes the role of technology in the structure of strategic autonomy in turn.

The issue of strategic autonomy is addressed directly or indirectly by the authors who analyze the European Union's foreign policy. They show all the problems the EU faces in areas of strategic importance for each Member State (e.g., Biscop & Whitman, 2013; Blockmans & Koutrakos, 2018; Howorth & Keeler, 2003; Morillas, 2019; Shepherd, 2021; Sjursen, 2007; M.E. Smith, 2017; Wessel & Larik, 2020; Westlake, 2020; Zyla, 2020). In addition to this, mention should also be made of publications dealing with foreign policies of the most important European actors (i.e., Ostermann, 2019; Joly & Haesebrouck, 2021).

A classically defined European strategic autonomy is linked to the nature of the transatlantic relationship and cooperation with NATO. Many authors (including: Hofmann, 2013; Howorth, 2017; Howorth, 2017a; S.J. Smith, Gebhard, & Graeger, 2020; Toje, 2008) analyze this complex issue.

The EU's strategic autonomy is also being examined in a global context, with particular regard to the transformation of the global balance of power (i.e., Biscop, 2016; Ginsberg & Penksa, 2012; Haar et al., 2021; Johansson-Nogués, Vlaskamp, & Barbé, 2020; Keukeleire & Delreux, 2014; Lütz et al., 2021; Tocci, 2017). Account should also be taken of the context of the capacity to undertake military interventions, which, according to certain political and expert circles in Europe, is at the heart of the EU's strategic autonomy (Bakardjieva Engelbrekt et al., 2020; Koenig, 2016; Nováky, 2018; Pohl, 2014).

A separate category of exploration of the theoretical and practical dimension of European strategic autonomy is constituted by analyses published by European and American think tanks (Besch & Scazzieri, 2020; Borrell, 2020; Cameron, 2021; Demertzis, 2021; Drent, 2018; Franke & Varma, 2019; Grevi, 2020; Helwig, 2020; Koenig, 2020; Lefebvre, 2021; Lippert, von Ondarza, & Perthes, 2019; Nissen & Larsen, 2021; Romanyshyn, 2021; Sabatino et al., 2020; Youngs, 2021; Terlikowski, 2021). The catalogue of sources is complemented by legal acts and publications of various kinds issued by the European Union institutions.

The study's literature outline, although non-exhaustive, allows to advance to presentation of methodological parameters.

METHODOLOGY AND CONCEPTUAL FRAMEWORK

The author adopted the network institutionalism as a theoretical basis. The importance of social and technological networks in society focuses the growing interest of social science representatives, including political science and its sub-discipline – international relations. Christopher Ansell (2006, pp. 75–76) lists four meta-principles of network institutionalism.

Firstly, the network institutionalism adopts a relative approach rather than an atributional approach in the analysis of the activities of social institutions. This means that the focus is on the links and interactions, not the attributes of the institution. In the context of the action of the EU institutions, not their formal powers are important, but the current state of relations with the various Community countries. This is a condition for their actions, also in terms of formulating strategies or making politically binding interpretations of reality.

Secondly, it assumes complexity because the above-mentioned links have complex structures. The network of interactions and linkages between the EU and its institutions is highly complex and composed. These links take place in

all areas of activity of European institutions and agencies, Member States and European societies, economic entities, NGOs, or virtual communities.

Thirdly, networks – in the context of action of social institutions – are both a resource and a limiting factor. The network approach to EU's structure and actions clearly shows that the EU is generating resources through Member States. On the other hand, however, it is limited by the interests and political will of the Member States and its goverments and societies.

Fourthly, the network institutionalism assumes that networks have the capacity to mobilize social resources and social capital in many different ways. The world of social networks is not only complex. It is also biased. In the ecosystem of EU institutions and Member States, this means differentiated access to information, resources and support, sometimes resulting in serious conflicts and inertia. The European Union, as a multi-level integration structure, with many political, social and economic forces, can be analysed through the prism of network.

The author employs scientific pragmatism as a strategy which sets out how to formulate the methodological basis. It creates the causal chain. It postulates full flexibility in the selection of methods and techniques. The most important criterion is the maximum utility (Creswell, 2013, pp. 36–37).

From the explored issue perspective, it is natural to choose qualitative research tools: analysis and critique of available sources and analysis of documents. The methodological body will be complemented by structured interviews with Members of the European Parliament. The choice of European legislators is dictated by their specific position in the network of EU institutions and by intensive work on technological issues.

The aim of the study is to identify the impact of digital technologies on the European Union's strategic autonomy *in statu nascendi*. The following research questions should therefore be answered: What are the EU's potentials in digital technologies and how do they determine its international position? How do digital technologies impact the EU's core functions?

Considering the research problem outlined above, the author puts the following hypothesis: multidimensional pressure of digital technologies requires the extension of the classic concept of EU's strategic autonomy and forces withdrawal from the logic of military force projection and freedom of political actions in crisis situations. EU's multi-level resilience should be at the heart of the strategic autonomy in a world defined by digital technologies.

The analysis of the research problem described above should begin with a reflection on the technological determinants of the EU's international position.

THE EU IN THE DIGITAL WORLD

According to Mark Rhinard and Gunnar Sjöstedt (2019, p. 5), the status of the EU as an actor on the international stage cannot be seen solely through the "actor capacity" dimension, but also through the "actor performance" concept that they have introduced. Researchers argue that the EU "has accumulated enough of the key traits of a generic foreign policy actor" (2019, p. 24). The EU, analyzed through the lens of network institutionalism, is a network structure capable of mobilizing various resources, generated by links between different institutions at different levels of the Community. It is capable of carrying out various activities in an international environment. In the field of technological development, the EU seeks to harmonize Member States' policies to underpin global competitiveness. The interests of the Member State are a limiting factor, an immanent element of the network institutionalism. This makes it difficult to generate strength in the international environment. The size of the market and the resources of the EU (along with political potential when it is mobilized), however, allow to classify the EU as a major actor.

The international position is increasingly defined by the level of development of digital technologies. The Fourth Industrial Revolution, like the previous ones, affects all areas of activity in societies, economies, and countries. However, in the case of this ongoing, the pace and extent of this impact are unprecedented. The Fourth Industrial Revolution is driven by rapid progress in Artificial Intelligence, superfast 5G telecommunications networks, Big Data analytics, automation and robotics, Internet of Things (Schwab, 2016, pp. 1–3). Those technologies give impulses to vast array of innovations, therefore complex technological ecosystem expand across all domains of human activity – from social, through economic, to political.

The establishment of regulations and standards is dominant in EU activities in the field of digital technologies. Primarily in the Artificial Intelligence and Big Data sectors. These technologies are perceived as crucial for economic and social development (data is treated as technological avatar of oil). Regulatory activities are beneficial and strengthen the position and competitiveness of the EU (Sikorski, 2021). The size and structure of the European digital market and the volumes of data produced can guarantee high levels of profit over a decade (Soulava, Cameron, & Ying, 2021, p. 8). The potential of the EU in this sector can be considered as high and solid. The most important obstacle to its use is, however, the lack of uniform, innovation-friendly rules for the commercial

use of data, which is the main resource serving the development of Artificial Intelligence. The first step in addressing these issues, foreseen in *A European Strategy for Data* (2020), was adopted in the 2021 in the form of *Data Governance Act*, which creates a new legal structure for data management in the EU. This legislation will apply to the creation of the European Common Data Spaces, which will initially cover the health, energy, and agriculture sectors (Bertuzzi, 2021). As Angelika Niebler, Member of the European Parliament (Committee on Industry, Research and Energy, D-US Delegation for relations with the United States), argues, data space should "grow organically" and the EU "can and should facilitate cooperation between Member States to break-up and connect national and sectoral data silos, share best practices and develop common data standards where it is reasonable" (Niebler, 2021). *The Data Act* is considered to be the next step. It is intended to regulate the methods and scope of the collection and commercial use of non-personal data (Headdon, 2021).

Methods, scope and management distrust for data sharing (Niebler, 2021) in the EU can hinder the development of Artificial Intelligence. Strategic relevance of this technology requires to treat it not only as a "matter of regulation" (Voss, 2021). The quality of data used in European Artificial Intelligence projects is not sufficient (Draft Report on Artificial Intelligence, 2021, p. 15). In addition to regulations (including General Data Protection Regulatory), there is also a low level of trust in this technology in EU countries. Community's actions in this field are also limited by the Member States themselves, as they see the question of AI differently (Bratberg, Csernatoni, & Rugova, 2020, p. 21).

The conclusions of the report prepared by the Center for Data Innovation (Castro & McLaughlin, 2021) show that the EU is developing slowly in the field of Artificial Intelligence. The analysis was based on 30 metrics across six categories: talent, research, development, hardware, adoption, and data. The United States leads in talent, research, development, and hardware; China – in adoption and data. Overall, the US amassed 44.2 out of 100 possible points. China was behind with the result of 32.3. The European Union earned 23.5 points. The study also takes the size of labor force into account. This has shown a slightly different picture of AI competition, with the US remaining at the leading position (58 points). However, the EU (24.2 points) has been better off than China (17.8). Nevertheless, the Middle Kingdom is consistently closing the gap (Castro & McLaughlin, 2021, p. 2).

The EU's position in the development of 5G superfast networks has relatively improved. Successful roll-out of 5G will stimulate the development of an entire

ecosystem of different innovations (notably the industrial Internet of Things) and will contribute to an even faster growth of data volumes. 5G development was the first significant manifestation of the fierce US-Chinese competition for global primacy. Initially, the EU had to choose between cooperating with the economically competitive Chinese companies or the traditional US alliance (at the time of Donald Trump's administration). The EU itself has, under the influence of this situation, attempted to strengthen screening procedures for telecommunications investments, particularly in the most sensitive parts of the network (Carcy, 2021, p. 17).

According to Gartner report (*Ericsson Named…*, 2021), Swedish Ericsson is the market leader in 5G. The EU therefore has a solid basis for developing and generating the advantages in this sector. The most important risks are China's offensive in international standardization bodies (like the EU in the area of AI and data, China wants to be a rule-setter rather than a rule-taker) and the continued support of Chinese authorities (including intelligence) for companies such as Huawei.

However, the missing component of the *modus operandi* of the EU in the field of digital technologies is geopolitical thinking. Competing for global primacy, the United States and China are rightly assuming that the global force pattern of the future will be defined by countries with strong potential in the fields of AI, robotics, autonomous devices, additive technologies (3D printing, 4D printing), nanotechnology, and quantum computing.

Globalization, which has defined production and trade models, is increasingly fragmented. Major international actors build the "tech-protectionism" and seek control over the value chains that are most important for digital technologies development. The United States and China have a dominant position over the EU in increasingly intense digital competition. They are world's "technological centers of gravity". According to 2019 data, the digital technology companies located in these countries "accounted for 90 per cent of the market capitalization of the 70 largest digital platforms (68 per cent and 22 per cent speed), 75 per cent of all patents related to blockchain technologies, 75 per cent of the cloud computing market, and 50 per cent of global funding on the internet of things" (Torreblanca, 2021, p. 41). The United States continues to be the leader in innovation, with the strategy to become a technological superpower with the market of appropriate size and financial resources to compete with China. However, the Middle Kingdom is consistently implementing its technological superiority strategies, utilizing vast state potentials to support economic enti-

ties (Mozur & Myers, 2021). Given the Chinese population control practices in Xinjiang Province and the actions against foreign (and domestic) Big-Tech companies, it can already be described as a 'techno-authoritarian state' (Kynge & Yu, 2021). This gives China an advantage over the EU and the United States, driven by traditional democratic values. This is a natural stimulus for deeper cooperation between them. After Joseph Biden took office as the President of the United States, an attempt was made to rebuild the transatlantic relations that were undermined during Donald Trump's term. This is reflected in the establishment of the EU-US Trade and Technology Council (TTC) at their summit in Brussels on June 15, 2021. It is intended to work as a mechanism for coordinating activities in the field of technological standards, climate and clean technology, information technology, data governance, misuse of technology, competitiveness, security, export controls (*EU-US Trade and Technology Council…*, 2021). The very creation of such an institution is undoubtedly beneficial for both sides, although its operations may encounter problems (e.g., the regulation of data flows). According to the assessment of Radosław Sikorski – the chairman of the European Parliament's Delegation for relations with the United States of America (D-US) – the basis for cooperation is solid even after a possible change in the US to a policy that is less favorable to strengthening transatlantic relations. The reason for this is a bipartisan understanding of the importance of technological rivalry with China (Sikorski, 2021).

The EU, despite its high potential in digital technologies, is not in a position to achieve a global advantage. This is despite the mobilization of resources and the synergy of the activities of the various EU institutions. The limiting factor is, of course, conflicting interests, the specific policies of the Member States and the perception of the importance of digital technologies (lack of trust, resulting in sharp regulations). The EU's activities are further complicated by the international context and the ongoing US-Chinese technological cold war. The result is an increasingly strong "tech-protectionism" and fragmented globalization. Objective factors such as narrow access to raw materials in the EU should not be overlooked either. Thus, it seems impossible to catch up with the US and China in many areas of digital technologies.

The EU, however, will not be a weak player, but it will also not be able to generate global advantages that are comparable to the US and China. Nevertheless, close cooperation with the US can compensate for this. Therefore, the strategic autonomy of the EU in digital age will have to rely on building resilience in key areas to be impacted by digital technologies. Such resilience is essential

to building EU strategic autonomy. This will define the optimal level of future political-military freedom of action (regarding the nature of the links between EU institutions and the constraints created by Member States).

STRATEGIC AUTONOMY THROUGH DIGITAL RESILIENCE

The European Political Strategy Centre enumerates three "*sin qua non* dimensions" of strategic autonomy: political (susceptibility to blackmailing, coercion; integrity of democratic procedures; ability to shape global norms, rules and standards), operational (exposure to cyber threats; integrity of critical information infrastructure), and industrial (import dependencies; supply chain disruptions; supply chain security; compromised equipment entering the EU; foreign control of critical infrastructure and essential service providers; ability to develop future capabilities). Industrial dimension covers the ability of the EU to meet current and future technological demands, including digital technologies. Operational dimension refers to the security of critical IT and communication networks. Political dimension is defined by undisrupted, efficient functioning of political processes and social stability (European Commission, 2019, p. 3). Digital technologies will define each dimension of strategic autonomy described above. The European ability to set goals and achieve them will therefore depend on its resilience. It can be defined as the state of architecture of various types of systems (technological or social), guaranteeing continuity of operations and readiness for various variants of situations of unexpected events – failures, disturbances, intentional destructive actions, etc. In an increasingly connected social and technological environment, the undisrupted functioning of digital infrastructure is the foundation of social, economic and political order. This is all the more important in the complex constellation of the EU institutions and the Member States.

According to the author, the most significant areas of strategic autonomy in the EU, as defined by digital technologies, are integrity of political processes, primarily the election cycles; integrity of critical information infrastructure; digital equipment entering the EU; control of critical infrastructure and essential service providers.

Integrity of the democratic procedures is a guarantee of the proper and stable functioning of political institutions – both at the Community and Member State level. Digital technologies already set the framework for the functioning

of political life in all its forms. They are the regulator of political processes, the main tool for communication and analytics. This is particularly important for the election cycles (Gajewski, 2021). They are especially vulnerable to computational propaganda, or "the ways in which the use of algorithms, automation (most often in the form of political bots), and human curation are used over social media to purposefully distribute misleading information" (Saurwein & Spencer-Smith, 2021, p. 225). This creates a serious threat, namely, the ability of an external entity to control political processes in the EU and to influence large social groups through the construction and deconstruction of views, inducement and regulation of emotions, generation of conflicts, etc. At a time of populist surge in Europe and increased Russian offensive operation in cyberspace, this has put the democratic institutions of the Member States and the EU itself at risk.

It is crucially important to control algorithms acting as "gatekeepers" or "intermediaries", between the producer of news or opinion content and the recipient. In many cases, they increase polarization, mainly promoting emotional content (Mems, 2020). This is the space for manipulation and aggressive actions that can shape social opinions in the way that an external entity planned to pursue its own political or economic objectives. The UK referendum campaign is an evocative example of this type of threat (Scientific Foresight Unit, 2019, pp. 19–20). Building resilience in this area is therefore crucial for the undisrupted operation of the EU as a whole, including external dimension. The key in this perspective is the creation of regulations that force the accountability of technology companies, especially the owners of social media. The EU should promote deep reforms of electoral laws to adapt them to the changing digital social reality. In addition to the regulatory actions in which the EU is a leader, the resilience of citizens and political actors is also needed. This is not just a question of the effective use of electronic media and algorithms in political campaigns. It is also a question of creating a body of skills for politicians at different levels to protect them from negative impacts and problems arising from the misuse of digital platforms.

The importance of integrity of critical information infrastructure for the functioning of the EU and the Member States can be compared to the importance of the nervous system in the human body. The resilience of digital critical infrastructure is a prerequisite for social stability. It is also a prerequisite for modern economies defined by data collection and flows. This realm falls within the broader category of cyber security in its technical dimension. The EU is taking a series of steps in this regard, creating an ecosystem of institutions

and mechanisms that *de facto* place cybersecurity issues at Community level. Within this scheme, the European Union Agency for Cybersecurity (ENISA) was established. It operates within four "communities": Cyber Resilience Community, Cyber Defense Community, Cyber Diplomacy and Policies Community, and Justice in Cyberspace and Cybercrime Community (Gajewski, 2020, p. 113). Key management systems for civil and special communications, energy networks and production processes, banking, transport, and other sectors in general need to be safeguarded. Joint action at EU level is all the more important as the threat of hostile action (states, terrorist and criminal organizations) using Artificial Intelligence engines will consistently increase. Defending against this type of automated attacks will be difficult, but not impossible. It will be crucial to build defensive capabilities based on AI, i.e., automated vulnerabilities detection systems in key networks (Schneier, 2021). However, the human factor (when dealing with complexity and size of the critical information infrastructure) makes it necessary to continuously invest in the digital competence of citizens and professional labor force. Advanced hacking attacks, such as the case of Ukraine's power networks hit with the Industroyer malware (Greenberg, 2017), are the glimpse of future hybrid warfare. The EU will undoubtedly be the target, given the size of the market and its geopolitical importance. Building resilience in this area also requires the necessary political action – building long-term compromises and a common European strategic awareness.

Equipment entering the EU is the hardware dimension of networked critical information infrastructure. The risk of foreign control of critical infrastructure and essential service providers is a complement to it. As it was mentioned, globalization and the removal of trade barriers, suffered many setbacks since the beginning of US-China technological cold war. This leads to the closing behind technological barriers – it is not currently a question of creating "cyberspace borders" (although China's attempts to create a new Internet protocol and Russian attempts to cut off from the global network prove that this direction has already been taken), but barriers to equipment and service providers. The United States first excluded the equipment of Chinese Huawei and ZTE companies, after concerns about possible penetration of critical networks. The exclusion of Chinese companies from building 5G infrastructure in the Member States (in whole or only from critical information infrastructure) is evidence of the magnitude of the problem in the EU. Strengthening investment screening – already adopted by the EU – is one of the most important tools for building resilience in this realm. Similarly, acquisitions and mergers that are changing the ownership

structure of European critical infrastructure operators must be controlled, also by the intelligence and counterintelligence services.

Many of existing backdoors in industry processes control software (SCADA) are already known. This vulnerability requires continuous close monitoring and aggressive posture (Hemsley & Fisher, 2018). Although these issues are closely linked to advanced digital technologies, the HUMINT intelligence capabilities remain relevant. This also applies to the oversight of critical infrastructure critical workers. The ENISA report highlights, among other things, a possible scenario of paralysis of SCADA systems by a person employed by a critical infrastructure operator (ENISA, 2016). Considering the network of multi-dimensional links that exist across the EU and the potential cascading effects of hostile activities, the security of the sector must be consistently increased.

CONCLUSIONS

The strategic autonomy of the EU in a rapidly changing world must take flexible, adaptive shape. Transformative features of digital technologies make them central to the concept of strategic autonomy.

This concept, in its classic form, is politically controversial. This is due to the structure of the EU itself and the dynamics of relations in the network of Community and national institutions. It is mainly associated with the freedom to set foreign policy objectives and to pursue European interests without having to consider the positions of other global actors. This involves building military crisis response capabilities and conducting expeditionary military operations. The dispute over foreign policy priorities between Member States is therefore a natural consequence. As a result, the EU's strategic autonomy is treated as a "hollow concept". The EU's internal crisis is also an important factor, which prevents the transfer of further competences in the field of foreign and security policy. Thus, the construction of a core of traditional strategic autonomy is virtually impossible.

However, it would be advisable to abandon the "maximum option", which is associated with the strong fear of EU Federation and the creation of a European superstate. The EU is *de facto* operating in a network model. Its operations are based on a number of power centers and a complicated network of links and flows. These links are more important in the functioning of these institutions than their specific attributes. Strategic autonomy in interconnected digital,

infrastructural, political, economic, and social networks should be based on resilience of these key elements of the EU and the Member States' functioning. These are, above all, democratic processes, the foundation of social stability. It is important to consistently raise the level of security of the broadly defined cyberspace, especially the critical information infrastructure, which is the EU's 'neural system'. Utilizing the potential of mobilizing resources of networked European institutions is far less politicized than building real EU military capabilities (and thus the competences of nation state).

In the context of complex global conditions for the EU, the technological and political alliance with the United States also becomes an element of strategic autonomy. Its foundations are already being created. If this project is successful, there will be an opportunity to improve the EU's global position in relative terms by securing value chains in key sectors (microchips, raw materials).

Taking action to build strategic autonomy, at the heart of which are digital technologies and the resilience of core EU functional areas and the consistent development of standards for the use of digital technologies, will build the foundation for future enlargement of its concept and practice. This will, of course, depend on the direction of the evolution of the European project. However, the creation of multi-level digital resilience will provide the EU with a solid basis for the possible creation of real political and military force if this proves to be a desired or necessary objective.

References:

A European Strategy for Data. (2020, February 19). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Retrieved December 2, 2021 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066.

Allen, J.R.L., Hodges, F.B., & Lindley-French, J. (2021). *Future War and the Defence of Europe*. Oxford: Oxfrod University Press.

Ansell, C. (2006). Network Institutionalism. In: S.A. Binder, R.A.W. Rhodes, & B.A. Rockman (Eds.). *The Oxfrod Handbook of Political Institutions* (pp. 75–90). Oxford: Oxford University Press.

Bakardjieva Engelbrekt, A., Bremberg, N., Michalski, A., & Oxelheim, L. (Eds.). (2020). *The European Union in a Changing World Order: Interdisciplinary European Studies*. New York: Palgrave Macmillan.

Bartels, H.P., Kellner, A.M., & Optenhögel, U. (Eds.). (2017). *Strategic Autonomy and the Defence of Europe: On the Road to European Army?* Bonn: Dietz Verlag.

Bellou, F. (2021). The Strategic Context of the European Security and Defence Policy. In: G. Voskopoulos (Ed.). *European Union Security and Defence: Policies, Operations and Transatlantic Challenges* (pp. 25–37). Cham: Springer.

Bertuzzi, L. (2021, December 1). *Data Governance: New EU Law for Data-Sharing Adopted*. Euractiv. Retrieved December 2, 2021 from: https://www.euractiv.com/section/digital/news/data-governance-new-eu-law-for-data-sharing-adopted/.

Besch, S., & Scazzieri, L. (2020, December). *European Strategic Autonomy and a New Transatlantic Bargain*. Berlin: Centre for European Reform – Konrad Adenauer Stiftung. Retrieved from: https://www.cer.eu/sites/default/files/pbrief_strategic_autonomy_11.12.20_4.pdf.

Bielecki, T. (2021, February 26). *Szczyt UE. Autonomia strategiczna, ale we współpracy z NATO*. Deutsche Welle. Retrieved October 28, 2021 from: https://www.dw.com/pl/szczyt-ue-autonomia-strategiczna-ale-we-współpracy-z-nato/a-56716866.

Biscop, S. (2016). All or Nothing? The EU Global Strategy and Defence Policy after the Brexit. *Contemporary Security Policy, 37*(3), 431–445, DOI: 10.1080/13523260.2016.1238120.

Biscop, S., & Whitman, R.G. (Eds.). (2013). *The Routledge Handbook of European Security*. Routledge: New York.

Blockmans, S., & Koutrakos, P. (Eds.). (2018). *Research Handbook on the EU's Common Foreign and Security Policy*. Cheltenham: Edward Elgar Publishing.

Borrell, J. (2020). *Pourquoi l'Europe doit-elle être stratégiquement autonome?* Paris: Institut français des relations internationales. Retrieved from: https://www.ifri.org/fr/publications/editoriaux-de-lifri/leurope-etre-strategiquement-autonome.

Cameron, F. (2021, February 3). *Money Talks: EU Strategic Autonomy Requires a Strong Euro*. European Policy Centre. Retrieved October 29, 2021 from: https://www.epc.eu/en/publications/Money-talks-EU-strategic-autonomy-requires-a-strong-euro%7E3b2a7c.

Carcy, L. (2021, March). *The New EU Screening Mechanism for Foreign Direct Investments When the EU Takes Back Control*. Bruges Political Research Papers, 84. Brugge: Colleger of Europe. Retrieved from: http://aei.pitt.edu/103426/1/wp84_carcy.pdf.

Chappell, L., Mawdsley, J., & Petrov, P. (Eds.). (2018). *The EU, Strategy and Security Policy: Regional and Strategic Challenges*. New York: Routledge.

Conclusions – 19/20 December. (2013, December 20). European Council. Retrieved October 28, 2021 from: https://www.consilium.europa.eu.

Creswell, J.W. (2013). *Projektowanie badań naukowych. Metody jakościowe, ilościowe i mieszane*. Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego.

Demertzis, M. (2021, Februrary 2). *Strategic Autonomy or Strategic Alliance?* Bruegel. Retrieved October 29, 2021 from: https://www.bruegel.org/2021/02/strategic-autonomy-or-strategic-alliance/.

Dijkstra, H. (2021). *Policy-Making in EU Security and Defense: An Institutional Perspective*. London: Palgrave Macmillan.

Drent, M. (2018, August). *European Strategic Autonomy: Going It Alone?* The Hague: Clingendael Institute. Retrieved from: https://www.clingendael.org/sites/default/files/2018-08/PB_European_Strategic_Autonomy.pdf.

Egeland, K., & Pelopidas, B. (2021). European Nuclear Weapons? Zombie Debates and Nuclear Realities. *European Security, 30*(2), 237–258. DOI: 10.1080/09662839.2020.1855147.

ENISA. (2016, December). *Communication Network Dependencies for ICS/SCADA Systems*. Athens: European Union Agency for Cybersecurity.

Ericsson Named a Leader in the 2021 Gartner Magic Quadrant for 5G Network Infrastructure for Communications Service Providers Report. (2021, February 23). Ericsson. Retrieved December 2, 2021 from: https://www.ericsson.com/en/press-releases/2021/2/ericsson-named-a-leader-in-the-2021-gartner-magic-quadrant-for-5g-network-infrastructure-for-communications-service-providers-report.

European Commission. (2019, July). *Rethinking Strategic Autonomy in the Digital Age*. EPSC Strategic Notes, 30. DOI: 10.2872/231231.

EU-US Trade and Technology Council: Commission Launches Consultation Platform for Stakeholder's Involvement to Shape Transatlantic Cooperation. (2021, October 18). European Commission. Retrieved December 6, 2021 from: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_5308.

Fiott, D. (2019). *Defence Industrial Cooperation in the European Union: The State, the Firm and Europe*. New York: Routledge.

Franke, U., & Varma, T. (2019, July). *Independence Play: Europe's Pursuit of Strategic Autonomy*. London: European Council on Foreign Relations. Retrieved from: https://ecfr.eu/wp-content/uploads/Independence-play-Europes-pursuit-of-strategic-autonomy.pdf.

Fägersten, B. (2020). European Autonomy in a Changing World Order. In: A. Bakardjieva Engelbrekt, N. Bremberg, A. Michalski, & L. Oxelheim (Eds.). *The European Union in a Changing World Order: Interdisciplinary European Studies* (pp. 23–46). New York: Palgrave Macmillan.

Gajewski, T. (2020). Towards Resilience: European Cybersecurity Strategic Framework. *Ante Portas. Security Studies*, 1, 103–122. DOI: 10.33674/3201911.

Gajewski, T. (2021). The Technology of Future Leadership. In: A. Kasińska-Metryka, & T. Gajewski (Eds.). *The Future of Political Leadership in the Digital Age: Neo-leadership, Image and Influence* (pp. 34–51). London–New York: Routledge.

García Pérez, R. (2019). Strategic Autonomy of the European Union: A Perspective. In: E. Conde, Z.V. Yaneva, M. Scopelliti (Eds.). *The Routledge Handbook of European Security Law and Policy* (pp. 81–95). London: Routledge.

Ginsberg, R.H., & Penksa, S.E. (2012). *The European Union in Global Security: The Politics of Impact*. New York: Palgrave Macmillan.

Greenberg, A. (2017, June 12). *'Crash Override': The Malware That Took Down a Power Grid*. Wired. Retrieved December 16, 2021 from: https://www.wired.com/story/crash-override-malware/.

Gressani, G., Malik, M., & Bloj, R. (2020, November 16). *La doctrine Macron: une conversation avec le Président français.* Le Grand Continent. Retrieved October 28, 2021 from: https://legrandcontinent.eu/fr/2020/11/16/macron/.

Grevi, G. (2020, December). *Fostering Europe's Strategic Autonomy: A Question of Purpose and Action*. Brussels: European Policy Centre – Konrad Adenauer Stiftung. Retrieved from: https://www.epc.eu/content/PDF/2020/Final_Paper_Purpose_and_Action_Layout_JF_II__1_.pdf.

Grevi, G. (2021). Europe's Strategic Autonomy and the Partnership Approach. In: P. Gieg, T. Lowinger, M. Pietzko, A. Zürn, U.S. Bava, & G. Müller-Brandeck-Bocquet (Eds.). *EU-India Relations: The Strategic Partnership in the Light of the European Union Global Strategy* (pp. 19–31). Cham: Springer International Publishing.

Haar, R., Christiansen, T., Lange, S., & Vanhoonacker, S. (Eds.). (2021). *The Making of European Security Policy: Between Institutional Dynamics and Global Challenges*. New York: Routledge.

Headdon, T. (2021, December 9). *Data Act: Summary Report on Public Consultation*. Lexology. Retrieved December 9, 2021 from: https://www.lexology.com/library/detail.aspx?g=88907ef5-edac-4ce2-a994-233aea64948e.

Helwig, N. (2020, October). *EU Strategic Autonomy: A Reality Check for Europe's Global Agenda*. FIIA Working Paper, 119. Helsinki: Finnish Institute of International Affairs. Retrieved from: https://www.fiia.fi/wp-content/uploads/2020/10/wp119_strategic_autonomy-2.pdf.

Hofmann, S.C. (2013). *European Security in NATO's Shadow: Party Ideologies and Institution Building*. Cambridge: Cambridge University Press.

Howorth, J. (2017). EU-NATO Cooperation: The Key to Europe's Security Future. *European Security, 26*(3), 454–459. DOI: 10.1080/09662839.2017.1352584.

Howorth, J. (2017a, May). *Strategic Autonomy and EU-NATO Cooperation: Squaring the Circle*. Security Policy Brief, 85. Brussels: Egmont Royal Institute for International Relations. Retrieved from: https://www.egmontinstitute.be/app/uploads/2017/05/SPB85.pdf?type=pdf.

Howorth, J. (2018). Strategic Autonomy and EU-NATO Cooperation: Threat or Opportunity for Transatlantic Defence Relations? *Journal of European Integration, 40*(5), 523–537. DOI: 10.1080/07036337.2018.1512268.

Howorth, J., & Keeler, J. (Eds.). (2003). *Defending Europe: The EU, NATO, and the Quest for European Autonomy*. New York: Palgrave Macmillan.

Johansson-Nogués, E., Vlaskamp, M.C., & Barbé, E. (Eds.). (2020). *European Union Contested: Foreign Policy in a New Global Context*. Cham: Springer International Publishing.

Joly, J.K., & Haesebrouck, T. (2021). *Foreign Policy Change in Europe since 1991*. New York: Palgrave Macmillan.

Karampekios, N., & Oikonomou, I. (Eds.). (2015). *The European Defence Agency: Arming Europe*. New York: Routledge.

Keukeleire, S., & Delreux, T. (2014). *The Foreign Policy of the European Union*. New York: Palgrave Macmillan.

Knutsen, B.O. (2016). European Defence Research in Crisis? The Way towards Strategic Autonomy. *Global Affairs*, *2*(3), 287–295. DOI: 10.1080/23340460.2016.1219152.

Koenig, N. (2016). *EU Security Policy and Crisis Management: A Quest for Coherence*. New York: Routledge.

Koenig, N. (2020, December 4). *Time to Go beyond the Meta-Debate on EU Strategic Autonomy in Defence*. Policy Brief. Belin: Jacques Delors Centre. Retrieved from: https://www.delorscentre.eu/fileadmin/2_Research/1_About_our_research/2_Research_centres/6_Jacques_Delors_Centre/Publications/20201203_defence_Koenig.pdf.

Kynge, J., & Yu, S. (2021, September 7). *China and Big Tech: Xi's Blueprint for a Digital Dictatorship*. Financial Times. Retrieved December 13, 2021 from: https://www.ft.com/content/9ef38be2-9b4d-49a4-a812-97ad6d70ea6f.

Lefebvre, M. (2021, Febrary 1). *Europe as a Power, European Sovereignty, Strategic Autonomy: A Debate That Is Moving towards an Assertive Europe*. Paris: Foundation Robert Schuman. Retrived from: https://www.robert-schuman.eu/en/european-issues/0582-europe-as-a-power-european-sovereignty-strategic-autonomy-a-debate-that-is-moving-towards-an.

Lippert, B., von Ondarza, N., & Perthes, V. (Eds.) (2019, March). *European Strategic Autonomy: Actors, Issues, Conflicts of Interests*. SWP Research Paper, 4. Berlin: Stiftung Wissenschaft und Politik. Retrieved from: https://www.swp-berlin.org/publications/products/research_papers/2019RP04_lpt_orz_prt_web.pdf.

Lütz, S., Leeg, T., Otto, D., & Dreher, V.W. (2021). *The European Union as a Global Actor Trade, Finance and Climate Policy*. Cham: Springer.

Meijer, H., & Brooks, S.G. (2021). Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back. *International Security, 45*(4), 7–43. DOI: 10.1162/isec_a_00405.

Mims, Ch. (2020, October 19). *Why Social Media Is So Good at Polarizing Us*. The Wall Street Journal. Retrieved December 16, 2021 from: https://www.wsj.com/articles/why-social-media-is-so-good-at-polarizing-us-11603105204.

Morillas, P. (2019). *Strategy-Making in the EU: From Foreign and Security Policy to External Action*. Cham: Springer International Publishing.

Mozur, P., & Myers, S.L. (2021, March 10). *Xi's Gambit: China Plans for a World Without American Technology*. New York Times. Retrieved December 13, 2021 from: https://www.nytimes.com/2021/03/10/business/china-us-tech-rivalry.html.

Niebler, A. [MEP]. (2021, December 23). *Technological Dimension of EU's Strategic Autonomy*. [An Interview by Tomasz Gajewski].

Nissen, C., & Larsen, J. (2021, February). *Strategic Autonomy: From Misconceived to Useful Concept: What Can We Learn from the Northern Outlook*. DIIS Policy Brief. Copenhagen: Danish Institute for International Affairs. Retrieved from: https://www.jstor.org/stable/resrep28784#metadata_info_tab_contents.

Nováky, N.I.M. (2018). *European Union Military Operations: A Collective Action Perspective*. New York: Routledge.

Noël, P. (2019). Nord Stream II and Europe's Strategic Autonomy. *Survival, 61*(6), 89–95. DOI: 10.1080/00396338.2019.1688569.

Ostermann, F. (2019). *Security, Defense Discourse and Identity in NATO and Europe: How France Changed Foreign Policy*. New York: Routledge.

Pieper, M., & Lak, M. (2019). The End of Transatlanticism? EU Security and Defence Policies and the 'Strategic Autonomy' Debate from a Historical and Contemporary Perspective. *Studia Europejskie*, *4*, 23–44. DOI: 10.33067/SE.4.2019.2.

Pohl, B. (2014). *EU Foreign Policy and Crisis Management Operations: Power, Purpose and Domestic Politics*. New York: Routledge.

Rahman, M. (2021, April 7). *European Sovereignty Has Lost Its Biggest Champion*. Politico. Retrieved October 28, 2021 from: https://www.politico.eu/article/european-sovereignty-has-lost-its-biggest-champion-emmanuel-macron/.

Rhinard, M., & Sjöstedt, G. (2019, May). *The EU as a Global Actor: A New Conceptualisation Four Decades after 'Actorness'*. Swedish Institute of International Affairs (UI) Papers, 6. Retrieved from: https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-paper-no.-6-2019.pdf.

Romanyshyn, I. (2021, March). *Breaking the Law of Opposite Effects: Europe's Strategic Autonomy and the Revived Transatlantic Partnership*. Security Policy Brief, 140. Brussels: Egmont Royal Institute for International Affairs. Retrieved from: https://www.egmontinstitute.be/app/uploads/2021/03/spb-140-Iulian-Romanyshyn-final.pdf?type=pdf.

Ryon, E. (2020). European Strategic Autonomy: Energy at the Heart of European Security? *European View, 19*(2), 238–244. DOI: 10.1177/1781685820968302.

Sabatino, E., Fiott, D., Zandee, D., Mölling, Ch., Major, C., Maulny, J.P., Keohane, D., & Moro, D. (2020, December). *The Quest for European Strategic Autonomy – A Collective Reflection*. Rome: Instituto Affari Internazionali. Retrieved from: https://www.iai.it/sites/default/files/iai2022.pdf.

Saurwein, F., & Spencer- Smith, C. (2021). Automated Trouble: The Role of Algorithmic Selection in Harms on Social Media Platforms. *Media and Communication, 9*(4), 222–233. DOI: 10.17645/mac.v9i4.4062.

Schneier, B. (2021, April). *The Coming AI Hackers*. Cambridge, MA: Harvard Kennedy School – Belfer Center for Science and International Affairs. Retrieved from: https://www.belfercenter.org/sites/default/files/2021-04/HackingAI.pdf.

Schwab, K. (2016). *The Fourth Industrial Revolution*. New York: Portfolio Penguin.

Scientific Foresight Unit. (2019, March). *Polarisation and the Use of Technology in Political Campaigns and Communication*. Brusells: European Parliamentary Research Service. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf.

Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. (2016, June). European External Action Service. Retrieved October 28, 2021 from: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

Shepherd, A.J.K. (2021). *The EU Security Continuum: Blurring Internal and External Security*. New York: Routledge.

Sikorski, R. [MEP]. (2021, December 17). *Technological Dimension of EU's Strategic Autonomy*. [An Interview by Tomasz Gajewski].

Sjursen, H. (Ed.). (2007). *Civilian or Military Power?: European Foreign Policy in Perspective*. New York: Routledge.

Smith, M.E. (2017). *Europe's Common Security and Defence Policy: Capacity-Building, Experiential Learning, and Institutional Change*. Cambridge: Cambridge University Press.

Smith, M.E. (2018). Transatlantic Security Relations since the European Security Strategy: What Role for the EU in Its Pursuit of Strategic Autonomy? *Journal of European Integration, 40*(5), 605–620. DOI: 10.1080/07036337.2018.1488840.

Smith, S.J., Gebhard, C., & Graeger, N. (Eds.). (2020). *EU-NATO Relations: Running on the Fumes of Informed Deconfliction*. New York: Routledge.

Sorbonne Speech of Emmanuel Macron. (2017, September 26). Ouest-France. Retrieved October 28, 2021 from: http://international.blogs.ouest-france.fr/archive/2017/09/29/macron-sorbonne-verbatim-europe-18583.html.

Soulava, B., Cameron, H., & Ying, V. (2021, November). *Data Rules for Machine Learning: How Europe Can Unlock the Potential While Mitigating the Risks*. Washington, D.C.: Atlantic Council. Retrieved from: https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Data-Rules-for-Machine-Learning-Report-2021.pdf.

Sweeney, S., & Winn, N. (2020). EU Security and Defence Cooperation in Times of Dissent: Analysing PESCO, the European Defence Fund and the European Intervention Initiative (EI2) in the Shadow of Brexit. *Defence Studies, 20*(3), 224–249. DOI: 10.1080/14702436.2020.1778472.

Terlikowski, M. (2021, January). *European Strategic Autonomy and Third Countries: The Defence Industrial Dimension*. Bratislava: GLOBSEC Policy Institute. Retrieved from: https://www.globsec.org/sites/default/files/2021-01/GLOBSEC-Policy-Paper_EUROPEAN-STRATEGIC-AUTONOMY-AND-THIRD-COUNTRIES-THE-DEFENCE-INDUSTRIAL-DIMENSION.pdf.

Timmers, P. (2018). The European Union's Cybersecurity Industrial Policy. *Journal of Cyber Policy, 3*(3), 363–384. DOI: 10.1080/23738871.2018.1562560.

Tocci, N. (2017). *Framing the EU Global Strategy: A Stronger Europe in a Fragile World*. Cham: Springer Nature.

Toje, A. (2008). *America, the EU and Strategic Culture: Renegotiating the Transatlantic Bargain*. New York: Routledge.

Torreblanca, J.I. (2021, December). Technology. In: M. Leonard (Ed.), *The Power Atlas: Seven Battlegrounds of a Networked World* (pp. 38–61). Berlin: European Council on Foreign Relations – Stiftung Mercator. Retrieved from: https://ecfr.eu/wp-content/uploads/power-atlas.pdf.

Trybus, M. (2014). *Buying Defence and Security in Europe: The EU Defence and Security Procurement Directive in Context*. Cambridge: Cambridge University Press.

Violakis, P. (2020). *Europeanisation and the Transformation of Eu Security Policy: Post-cold War Developments in the Common Security and Defence Policy*. New York: Routledge.

Voskopoulos, G. (Ed.). (2021). *European Union Security and Defence: Policies, Operations and Transatlantic Challenges*. Cham: Springer.

Voss, A. [MEP]. (2021, December 2). Technological Dimension of EU's Strategic Autonomy. [An Interview by Tomasz Gajewski].

Wessel, R.A., & Larik, J. (Eds.). (2020). *EU External Relations Law: Text, Cases and Materials*. New York: Hart Publishing.

Westlake, M. (Ed.). (2020). *The European Union's New Foreign Policy*. New York: Palgrave Macmillan.

Youngs, R. (2021, March 8). *The EU's Strategic Autonomy Trap*. Carnegie Europe. Retrieved October 30, 2021 from: https://carnegieeurope.eu/2021/03/08/eu-s-strategic-autonomy-trap-pub-83955.

Zieliński, T. (2020). Strategic Autonomy of the European Union in Security and Defence. *Lithuanian Annual Strategic Review*, *18*(1), 5–22. DOI: 10.47459/lasr.2020.18.1.

Zyla, B. (2020). *The End of European Security Institutions? The EU's Common Foreign and Security Policy and NATO after Brexit*. Cham: Springer International Publishing.