Artur Staszczyk[1]

EUROPEAN PARLIAMENT'S POSITION ON EU CYBER SECURITY AND DEFENSE POLICY

Keywords: cyber security, cyber defense, European Parliament, European Union

ABSTRACT: Ensuring cyber security in scope of cyber defense is currently among the top priorities of the EU Common Security and Defense Policy (CSDP). Matters included in scope of cyber defense are a competence of the Member States and cooperation at EU level in this area is governed by decisions of the EU Council based on unanimity. This means that the European Parliament (EP) in the field of cyber defens acts only as an opinion-forming body expressing its position through the adoption of non-legislative resolutions. The aim of the article is to analyze the content of these resolutions and present the EP's opinion on the challenges facing the EU in the field of cyber defense. It should be stressed that the EP is the EU body that strongly emphasizes the need for a common EU approach to these issues. Given that the area of cyber defence is subject to intergovernmental cooperation mechanisms, the EP considers that the EU needs to develop not only cooperation and coordination mechanisms at the level of its institutions, but also to take action to enhance the EU's capability to counter cyber threats. These significant cyber defense capabilities should be essential elements of the CSDP and of the development of the European Defense Union, as it is becoming increasingly difficult to counter cyber attacks for the Member State level alone. The role of the CSDP should be to ensure that the EU, in cooperation with NATO, has an autonomous strategic capability to act in the field of cyber defense.

[1] Artur Staszczyk, PhD in Political Science, university lecturer at the Department of International Relations and European Studies of the Institute of Political Science and European Studies at Szczecin University. His research interests include such issues as: the EU's Foreign and Security Policy, European Neighborhood Policy, the role of European Parliament in the formation of the EU's external relations; ORCID: 0000-0001-9769-8991.

Cyber security is a term referring to the safeguards and actions that can be used to protect the cyber domain, both civil and military, from threats to its interdependent networks and information infrastructures that can damage them and their infrastructure. Ensuring cyber security is about preserving the availability and integrity of networks, infrastructure and the confidentiality of the information they contain (Chmielewski, 2016, pp. 107–108). For the European Union, cyber security policy took on a comprehensive strategic dimension only in 2013 with the adoption of the document entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". This document identifies five strategic EU priorities in the field of cyber security, such as: 1. Achieving resilience to cyber threats, 2. Radically reducing cybercrime, 3. Developing a defense policy and cyber security capabilities in conjunction with the Common Security and Defense Policy (CSDP), 4. Developing industrial and technological resources for cyber security, 5. Establishing a coherent international cyberspace policy for the European Union and promoting EU core values (Wspólny, 2013, p. 5). The development of the strategy was influenced by the events of 2007, when Estonia's IT infrastructure fell victim to cyber attacks commonly attributed to Russia. Similar situation took place during the Georgia – Russia conflict in 2008. At that time, these actions were an integral part of the Russian military operation against Georgia, giving the term cyber war a practical dimension. Although the Russian cyber attacks have not caused any physical damage, they have significantly weakened Georgia's defense potential, affecting the ability of the Georgian authorities to communicate with their own citizens and international public opinion. The Russian aggression against Ukraine in 2014 and the hybrid actions carried out at that time, with cyber attacks on critical infrastructure as an important element, were an important step towards EU involvement in cyber security (Szczygieł, 2018, pp. 167–169). Following these developments at EU level, it has become clear that the effective implementation of CSDP is increasingly dependent on the availability of protected cyberspace. It should be stressed that in cyberspace states have started to see another domain where conflicts can be conducted. This process is accompanied by the development of the potential of "digital weapons" to carry out offensive actions against the enemy. This

means that hostile actions from cyberspace are currently not limited to critical infrastructure, but are being taken by armed forces using digital tools in their fight (Świątkowska, 2017, pp. 173–174). The prioritization of cyber security aspects related to cyber defense is reflected in the adoption by the EU Council in November 2014 of the 'EU Cyber Defense Policy Framework'. It has priority areas for cyber defense in the field of CFSP, including: 1. Supporting the development of Member States' CSDP-related defense capabilities, 2. Improving the security of CSDP-related communication networks used by EU entities, 3. Promoting civil-military cooperation and synergies with broader EU cyber policies, relevant EU institutions and agencies, as well as with the private sector, 4. Improving training, education and exercise opportunities 5. Strengthening cooperation with relevant international partners (*Ramy polityki UE w zakresie cyberobrony*, pp. 4–13). The desire to make cyber security issues central to EU policy has also been articulated in the EU Global Strategy for Foreign and Security Policy adopted by the European Council in June 2016, which includes as one of its priorities the security of the Union itself. The lines of action under this priority include, i.a., cyber security. This document states, that in order to protect against cyber threats, it is necessary to integrate cyber issues into all EU policies, including CSDP missions and operations (*Globalna strategia UE na rzecz polityki zagranicznej i bezpieczeństwa*, pp. 16–19). The EU Council conclusions of November 2017 recognize the growing links between cyber security and defense. The document calls for a deepening of cooperation in the field of cyber defense by strengthening the interaction between civilian and military incident response services and for a strengthening of cybersecurity in CSDP operations. It also stresses that a serious cyber incident or crisis may constitute a basis for a Member State to invoke the EU solidarity or mutual assistance clause (Konkluzje Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. *Odporność. Prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE*, pp. 11–12). In December 2017, a permanent structural cooperation (PESCO) was initiated within the framework of which two projects related to cyber defense are being implemented: "Cyber incident Rapid Response and Mutual Assistance Teams in the field of cyber security" and "Platform for exchange

of information on cyber threats and cyber incident response" (*Declaration on PESCO Project*, pp. 1–2). A summary document of the EU's activities to date in the field of cyber defense is an update of November 2018 "The EU Cyber Defense Policy Framework". It modifies the priority areas of cyber defense, which include: 1. Supporting the development of Member States' cyber defense capabilities, 2. Improving the security of CSDP-related communication and information systems used by EU entities, 3. Promoting civil-military cooperation, 4. Research and technology, 5. Improving education, training and exercise capacities, 6. Strengthening cooperation with relevant international partners (*Ramy polityki UE w zakresie cyberobrony (aktualizacja 2018 r.),* pp. 9–24).

Although cyber defense issues belong to the competence of the Member States and are agreed at EU level through intergovernmental cooperation mechanisms, they are also of great interest to the EP which expresses its views on them through the adoption of non-legislative resolutions. Analyzing the EP's position on cyber security with a particular focus on the cyber defense dimension, it should be underlined that in today's globalized world, the EU and its Member States have become heavily dependent on a secure cyberspace, secure use of information and digital technologies, and resilient and reliable information services and related infrastructure. The EP considers that information and communication technologies are becoming the most effective means of communicating democratic ideas and organizing people who seek to fulfill their aspirations for freedom. However, they are also used by undemocratic and authoritarian governments as instruments of repression against society. This is why it is so important for cyberspace to remain open to the free flow of ideas, information and expression. Along with the development of cyberspace, the EP stressed the need for a global and coordinated approach to these challenges at EU level through the development of a comprehensive EU cyber security strategy, which was finally adopted in 2013. The EP insists in its resolutions that in the event of a cyber attack against any Member State, the Treaty's solidarity and mutual defence clauses may be applied. Furthermore, it called on the Commission and the Coun-

cil to explicitly recognise digital freedoms as fundamental rights and as indispensable conditions for the enjoyment of universal human rights. In the adopted in November 2012 EP resolution, the EP stressed that Member States should aim to ensure that the rights and freedoms of their citizens are never endangered when developing responses to cyber threats and attacks, and called for the prudent use of all restrictions on the use of communication and information tools by citizens.

The EP also called on the Commission and the Member States to propose programmes to promote and raise awareness among private and corporate users of the generally safe use of the Internet, information systems and communication technologies (*Rezolucja Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony*, 2012a). For the EP, it is also important to secure digital freedom in the EU outer surrounding. Any restrictions of the freedom should determine relations of the EU with third-party states, especially with those benefiting from the EU aid and support within aid programmes. The Union must act not only to guarantee freedom of expression and access to information on the Internet, but also to strengthen the position of human rights defenders, civil society activists and journalists in third-party states who use modern information technologies in their activities. In the opinion of the EP, accession negotiations and negotiations of framework agreements with third-party states, human rights dialogues, trade negotiations and all forms of human rights contact should include clauses providing for the guarantee and respect of unrestricted access to the Internet, digital freedom and human rights on the Internet. According to the EP, provision of political and diplomatic support to the digital freedom should become a priority of the EU's foreign policy (*Rezolucja Parlamentu Europejskiego z dnia 13 czerwca 2018 r. w sprawie cyberobrony*, 2012b). It needs to be stressed that in the adopted resolutions the EP takes the position that cyber and hybrid challenges, threats and attack constitute a severe threat to safety, defense, stability, competitiveness of the EU, its Member States and citizens. It considers that the EU and the Member States

face unprecedented threat of cyber attacks sponsored by state entities. In this regard, it is underlined that although cyber defense is one of the core competences of the Member States, the EU should play a key role in providing a platform for cooperation in this field, as cyber defense capabilities should be an indispensable element of the Common Security and Defense Policy and the development of the European Defense Union. Therefore, the EP calls on the European External Action Service and the Council of the EU to step up their efforts to increase cyber security under the CSDP, e.g. by taking action at EU and Member State level to mitigate CSDP threats, through training, exercises and dissemination of cyber defense education. The EP also supports the establishment of an EU Cyber Defense Unit within the framework of permanent structured cooperation and supports an increase in defence spending on research and development to at least 2%, with a special focus on cyber security and defense (*Rezolucja Parlamentu Europejskiego z dnia 13 grudnia 2017 r. w sprawie sprawozdania rocznego w sprawie realizacji wspólnej polityki bezpieczeństwa i obrony*, 2017). Welcoming the steps taken by the EU to enhance its cyber resilience by establishing a common cyber security certification framework and strengthening the EU cyber security agency, the EP recognizes the new challenges facing Europe in this area. An important threat today is interference in elections in other countries through cyber operations that undermine or violate the right of a nation to participate in the exercise of power in its own country, directly or through freely elected representatives. Such interference by other states, although not involving the use of armed force and not threatening territorial integrity and independence, is, in the EP's view, a violation of international law (*Rezolucja Parlamentu Europejskiego z dnia 12 grudnia 2018 r. w sprawie sprawozdania rocznego w sprawie realizacji wspólnej polityki bezpieczeństwa i obrony*, 2018a). Thus the EP is in favor of increasing cyber-security capabilities in all institutions, EU bodies, in the Member States and overcoming political, legislative and organizational obstacles to cyber-defense cooperation. It believes that a regular and in-depth exchange of information and cooperation between relevant public sector entities in the field of cyber defence at EU and national level is crucial. The EP strongly underlines that, as part of the emerging Euro-

pean Union of Defense, from the beginning the cyber defense capabilities of the Member States with a view to ensuring maximum effectiveness must be put in the foreground and integrated as much as possible. The EP recognizes that many Member States consider own cyber defense capabilities a basis of their national security strategy and is an essential element of state sovereignty. However it is underlined that due to the cross-border nature of cyberspace, the scale of actions and knowledge required to provide genuinely comprehensive and effective armed forces guaranteeing the strategic autonomy of the EU in cyberspace is beyond the reach of any single Member State. Thus the situation demands determined and coordinated reaction on part of all Member States at the EU level. It is underlined that as part of CSDP missions and operations, cyber defense should be considered as an operational task, which is included in all planning processes related to CSDP. The EP takes the view that any planning of CSDP missions and operations must be accompanied by a detailed assessment of the cyber crime landscape. It is believed that an improved set of EU education and training activities in the field of cyber defense would make it possible to significantly mitigate risks and calls on the EU and the Member States to strengthen cooperation in education, training and exercises. The EP appeals to introduce a platform for training and coordination of exercises in scope of cyber defense. It encourages more frequent exchange of information in the field of situational awareness through simulation exercises in the field of cyber security and coordination of efforts to develop appropriate capabilities in order to achieve greater interoperability and to better prevent and respond to future attacks. It calls for such projects to be carried out in cooperation with NATO allies, the armed forces of EU Member States and other partners with extensive experience in counteracting cyber attacks, in order to develop operational readiness, common procedures and standards to enable a comprehensive response to different cyber threats. The EP calls for the identification of new initiatives for further cooperation between the EU and NATO, including the possibility of cooperation within the NATO Cooperative Cyber Defense Center of Excellence (CCD COE) and the NATO Academy of Communications and Information (NCI), aimed at enhancing cyber defense training capabilities with regard

to information technology and cyber systems The both organizations are called to strengthen operational cooperation and coordination and joint capacity-building activities, in particular through joint exercises and training for civilian and military personnel involved in cyber defense, and through the participation of Member States in NATO projects in the field of smart defense. According to the EP it is of the utmost importance to increase information exchange between the EU and NATO in order to impose restrictive sanctions on the entities responsible of cyber attacks. The organ underlines that there is considerable scope for developing a more ambitious and detailed cyber defense cooperation programme, going beyond conceptual cooperation. It welcomes the establishment in 2014 of the NATO's Cybernetic Partnership with the Industry Sector (NICP) and calls for EU involvement in NICP cooperation. It calls for the inclusion of cyber defense capabilities in the CFSP and in the external actions of the EU and its Member States as a cross-cutting task. The EP also appeals to improve the coordination of cyber defense by Member States, the EU institutions, NATO, UN, the United States and other strategic partners, especially in relation to rules, standards and means of execution in cyberspace. It confirms full engagement in open, free, stable and safe cyberspace, characterized by observance of basic values of democracy, human rights and law and order, where international disputes are settled peacefully based on the Charter of the United Nations and international law regulations. The EP calls on the Member States to support the further implementation of a common and comprehensive EU approach to digital diplomacy and existing cyber-security standards and the development, in cooperation with NATO, of criteria and definitions for a cyber attack at EU level in order to enhance the EU's ability to rapidly reach a common position in response to violations of international law in the form of a cyber attack. It recognizes that most technology infrastructure is owned or operated by the private sector and that close cooperation, consultation and involvement of the private sector and civil society groups through multilateral dialogue is therefore essential to ensure open, free, stable and secure cyberspace. The EP contentedly notes that the Council have adopted the frameworks for Union's mutual diplomatic response to harmful cyber actions – the so-called Union set

of tools for cyber diplomacy. It supports the possibility for the EU to take restrictive measures against opponents attacking its Member States in cyberspace, including the possibility to impose sanctions. It also calls for the strengthening of cyber diplomacy as a task within the framework of EU foreign policy. It also observes that building third countries' cyber resistance contributes to international peace and security, which ultimately provides greater security for European citizens. The EP underlines the importance of elaborating standards considering privacy and security, coding, language of hatred, disinformation and terrorist threats. It recommends that each Member State should accept the obligation to assist any other Member State that is a victim of a cyber attack and to ensure national responsibility for cyber security issues in close cooperation with NATO. It points out that the protection of critical assets related to public and other civilian infrastructure, particularly IT systems and data, is becoming a key task for the Member States in the field of defence and, in particular, for the authorities responsible for the security of IT systems. The EP calls on all Member States to focus their national cyber security strategies on the protection of information systems and related data and to make the protection of these critical infrastructures one of their priorities. It recognizes that a stronger and more structured cooperation with police services may be recommended, particularly in some critical areas, e.g. in tracking threats such as cyber jihadism, cyber terrorism, radicalization on the Internet and financing extremist or radical organizations, given the changing environment of cyber threats. The EP urges the Commission to develop an action plan for a coordinated approach to European cyber defense, including an update of the EU cyber defense policy framework to ensure that it continues to be a suitable policy instrument for achieving EU cyber defense objectives, in line with its intended objective. It calls for international cooperation and multilateral initiatives to develop a rigorous framework for cyber defense and cyber security in order to prevent state capture through corruption, fraud, money laundering and terrorist financing (*Rezolucja Parlamentu Europejskiego z dnia 12 grudnia 2018 r. w sprawie sprawozdania rocznego w sprawie realizacji wspólnej polityki bezpieczeństwa i obrony*, 2018b).

Summarizing the EP's position on the issues of cyber security and defense, it should be noted that from a formal and treaty point of view, this body is not a fully-fledged co-decisive entity in the shape of these issues. This is because many Member States consider that having their own cyber defense capabilities is an essential element of their sovereignty. Therefore, as a supranational institution, the EP does not have decision-making powers with regard to the CSDP, which is dominated by intergovernmental cooperation mechanisms and of which cyber defense is one of the priorities. It is the EU Member States, when taking decisions on the basis of unanimity, that conduct cyber defense projects within the framework of permanent structured cooperation (PESCO), which is a mechanism for deeper integration in the area of CSDP. This means that, with regard to the cyber defense policy, the EP's role comes down to being, first and foremost, a consultative institution. Non-legislative resolutions adopted within the EP are the main instrument for expressing opinions. However, although not legally binding, they are of considerable political importance. They contain EP views which, because it is the only EU institution with democratic legitimacy that represents the people of Europe, must be more or less taken into account by other EU bodies as well as by the Member States. The EP can invoke the will of the European public to express its views on the most important issues of cyber security and defense. This allows it to play the role of political influence institution in relation to the EU Council which is the most important decision-making body in the area of cyber security and defense. Whereas cyber defense is a core competence of the Member States, the EP considers that the EU needs to develop not only cooperation and coordination mechanisms at European level, but also to take action to enhance the EU's capability to counter cyber threats. These significant cyber defense capabilities should be an essential element of the CSDP and of the development of the European Defense Union, as according to the EP it is becoming increasingly difficult to counter cyber attacks at the Member State level. The role of the CSDP should be to ensure that the EU, in cooperation with NATO, has an autonomous strategic capability to act also in the field of cyber defense. However, at the current level of development of the EU defense policy, it is not possible to establish transnational cooperation mechanisms within

the framework of the EU that would allow it to "communities" and give the EP the status of a fully fledged entity shaping cyber security and defense policy. The EP will therefore remain primarily a consultative and consultative body in this area of integration.

BIBLIOGRAPHY:

Chmielewski, Z. (2016). Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich. *Studia z Polityki Publicznej,* 2, pp. 103–128.

Declaration on PESCO Project. (2017). Downloaded from: www.consilium..europa.eu/doceo/media//32020/draft-pesco-declaratioclean-10122017.pdf.

Globalna strategia UE na rzecz polityki zagranicznej i bezpieczeństwa. (2016). Downloaded from: https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_pl_version.pdf.

Konkluzje Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność. Prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE" (2017). Downloaded from: data.consilium.europa.eu/doccument/14435-2017-INIT/pl/pdf.

Ramy polityki UE w zakresie cyberobrony (2014). Downloaded from: data.consilium..europa.eu/doc/doccument/ST-15585–2014-INIT/pl/pdf.

Ramy polityki UE w zakresie cyberobrony (update from 2018) (2018). Downloaded from: .consilium..europa.eu/doc/doccument/ST-14413–2018-INIT/pl/pdf.

Rezolucja Parlamentu Europejskiego z dnia 13 czerwca 2018 r. w sprawie cyberobrony (2018b). Downloaded from: www.europarl.europa.eu/doceo/document/TA-8–2018–0258_PL.html?redirect.

Rezolucja Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony (2012a). Downloaded from: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012–0457+0+DOC+XML+V0//PL.

Rezolucja Parlamentu Europejskiego z dnia 11 grudnia 2012 r. w sprawie strategii wolności cyfrowej w polityce zagranicznej UE (2012b). Downloaded from: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0470+0+DOC+XML+V0//PL.

Rezolucja Parlamentu Europejskiego z dnia 13 grudnia 2017 r. w sprawie sprawozdania rocznego w sprawie realizacji wspólnej polityki bezpieczeństwa i obrony (2017). Downloaded from: www.europarl.europa.eu/doceo/document/TA-8-2017-0492_PL.html.

Rezolucja Parlamentu Europejskiego z dnia 12 grudnia 2018 r. w sprawie sprawozdania rocznego w sprawie realizacji wspólnej polityki bezpieczeństwa i obrony (2018a). Downloaded from: www.europarl.europa.eu/doceo/document/TA-8-2018-0514_PL.html.

Świątkowska, J. (2017). Walka z cyberzagrożeniami jako wyzwanie stojące przed globalnym bezpieczeństwem. *Przegląd Geopolityczny,* 20, pp. 162–177.

Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (2013). Downloaded from: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.