EURODEFENCE-PORTUGAL

CYBERSPACE SECURITY AND THE PROTECTION OF CRITICAL INFRASTRUCTURES: THE EUROPEAN DIGITAL AGENDA AND NATIONAL RESILIENCE

Colonel Paulo Viegas Nunes
Deputy Director of Education of the Military Academy
Director of the CAIH Implementation Group
Head of the CIIWA Board
EURODEFENCE Portugal Associate

Eng.º Paulo Moniz
Director IT Cybersecurity and Risk - EDP Group
Member of CIIWA Board
Adviser to EURODEFENCE Portugal Board

Abstract

In a digital and connected world, hybrid threats exploit the dependence of individuals, organizations and States on the internet and cyberspace. Critical infrastructures, also operating in a networked environment are, today, appealing targets for cyber-attacks of a high disruptive and destructive power. New threats, exploiting the vulnerabilities of an information age society, raise new social risks and require a concerted response, both at national and international levels.

Portugal has been investing, essentially over the last decade, in its national cybersecurity and digital infrastructure's structural and functional resilience but it is also crucial to ensure critical infrastructures' protection to manage social risks and defend national sovereignty.

This article covers the national critical infrastructures protection in the scope of the European Digital Agenda. In this work we will characterize the fundamentals associated with the formulation of a cybersecurity and cyber defence policy and strategy, a framework for digital resilience and a succinct analysis of the protection of critical infrastructures and the safeguarding of essential services in the scope of both, national and European contexts.

Key-words: Cyberspace, Cybersecurity, Critical Infrastructures Protection, Risk Management, Digital Resilience.

1. INTRODUCTION

The Internet is now an aggregating and connective element of society, overcoming geographical barriers, creating virtual communities and fostering the development and prosperity of states. Over the past few years, digital transformation has accelerated greatly, fostering technological innovation and making a decisive contribution to the building up of national resilience during the recent COVID-19 pandemic.

The structuring and development of a network society has generated interdependencies and led to the interconnection of infrastructures and systems, facilitating the provision of services, essential to its operation. International cooperation and market liberalisation, leading to the creation of economic communities, has also promoted the interconnection and extension of the perimeter of these infrastructures across national borders, generating interdependencies and increasing social risks at both national and international level. The occurrence of blackouts, or the prolonged interruption of the operation of these" systems of systems", could have a domino effect with catastrophic consequences, due to the multiple existing interdependencies.

In the information age, emerging threats in cyberspace have evolved rapidly, becoming increasingly sophisticated, disruptive and destructive. These do not respect the sovereign borders of states and can arise, without warning, from anywhere in the world. Critical infrastructure networks, being a centre of gravity of modern societies, are potential profitable strategic objectives and targets that, when hit by a cyberattack, can affect national security and defence.

The threat spectrum, hybrid in nature and exploiting multiple vectors, can range from cyber attacks launched by criminal groups, to hackers linked to activist groups and even advanced and persistent threats supported by state actors, involving careful planning and the use of sophisticated techniques that invariably discover new vulnerabilities in order to achieve their goals. On the other hand, the proliferation of software tools and new attack techniques, facilitating access to hacking services, has made it easier to carry out malicious attacks, with attackers exploiting legal loopholes and anonymity to achieve their objectives.

At a time when the exercise of citizenship is more and more shaped by a digital matrix, a large-scale cyber attack launched on national critical infrastructures would have an increased disruptive effect, not only at national level but also at the global level, creating social chaos, jeopardising governance and the exercise of digital sovereignty.

Over the past few years, both at national and cooperative level, European Union (EU) Member States have been investing heavily in enhancing the security of their digital

infrastructures, making it imperative to ensure not only their protection but also their defence, in order to ensure the resilience of all networked essential services infrastructure.

2. CYBER SECURITY AND CYBER DEFENSE: NATIONAL FRAMEWORK

Reflecting the evolution of national public policies, both in the field of cybersecurity and cyber defence, over the past decade Portugal has consolidated a number of structuring initiatives aimed at ensuring a safer use of cyberspace. To this end, in 2012, following the adoption of a comprehensive strategic plan for the rationalisation of costs for Information and Communication Technologies (ICT) in Public Administration[1], Resolution of the Council of Ministers No 12/2012, of 7 February, under the coordination of the National Security Office (GNS) and in collaboration with all relevant bodies in this field, provided for the establishment of a National Information Security Strategy (ENSI), which included the establishment, installation and operation of a National Cybersecurity Centre (CNCS). To this end, directly reporting to the prime minister, a CNCS' Installation Commission was established by the Council of Ministers Resolution 42/2012 of 5 April.

In the field of cyber defence, given the emerging challenges of cyberspace security, the Strategic National Defence Concept (NSSC, 2013) has set out a number of strategic priorities, recognising the information and security of cyberspace as one of its strategic pillars. In the same year, within the framework of the "Defence 2020" reform, the Minister of National Defence (MDN) established a Cyber Defence Centre (CDC) within the Military General Staff (EMGFA) and defined its political guidance for cyber defence, Order 13692/2013 of 28 June.

Following the indications of the European Union (EU), which recommended the operationalisation of this type of structures in all Member States (MS) by December 2012, the CNCS was integrated into the GNS in 2014. Following this step, a National Cyberspace Security Strategy (ENSC, 2015) was also approved. Following the technological developments and the cyber threats dynamics, this strategy was recently revised and updated for the period 2019-2023 (ENSC, 2019), highlighting the need to strengthen the building of a national cyber-defence capacity (EMGFA, 2018). This process was conducted in close coordination with the cooperative efforts already launched by other countries and international organisations of which Portugal is an integral part, inter alia, with the North Atlantic Treaty Organization (NATO) and the EU.

[1] This plan, organised into five lines of action, included 25 ICT rationalisation measures, transversal and impacting on every part of public administration. Measure 4, which is one of these lines of action, focused on the definition of a national strategy for the security of ICT and communication networks.

Following the approval of ENSC (2015), the National Council for Cyberspace Security (CSSC, 2017) was also established, which assumed responsibility for political and strategic coordination of national cybersecurity. These responsibilities were consolidated by Article 5 of Law No. 46/2018 of 13 August, establishing the legal regime for cyberspace security.

With a view to developing a political vision for cyber defence and the consequent creation of a National Cyber Defence Strategy (ENCD), several studies and working documents have been developed, both at the level of the MDN (2019a) and EMGFA (2019b) and at the National Defence Institute (Freire, Nunes & Acosta, 2013; Nunes, 2018). In this context, it should also be noted that in the latest revision of the Military Strategic Concept (CEM, 2014, p.19), several scenarios have already been identified for the use of the Armed Forces, notably in terms of the protection of systems considered essential/critical for the country, both in the field of cyber defence and in the area of national cybersecurity. More recently, through its Order No 15/2020 of 6 February, the MDN established a Cyber Defence Monitoring Committee (CMCD) which mission is to monitor all issues related to national cyber defence, thus ensuring the necessary coherence and integration of efforts.

Although before and during the COVID-19 pandemic no major disruptive and/or destructive cyber attacks were reported, the large volume of small/medium-sized attacks has demonstrated the need to strengthen the country's cybersecurity and cyber defence capabilities (European Council, 2020). Like in several other European countries, this set of events demonstrated that national resilience could be jeopardised by more severe cyber attacks, in particular because it is becoming increasingly difficult to ensure the following requirements/conditions:

- the availability of communication systems, as well as the security of telecommunications and information networks, which are essential to ensure the operation of essential services and infrastructures as well as their proper functioning under crisis conditions;
- e-governance and its critical services, conditioning or even compromising the political decision-making process in a crisis situation;
- the comprehensive protection of all critical infrastructures, in particular to minimise the impact of a targeted cyber attack which, due to its disruptive nature, could also lead to the occasional unavailability of energy supply systems, jeopardising access to backup/reserve networks, both domestically and internationally, if the cyber attack affects several countries simultaneously.

As for the protection of critical infrastructures, it should be noted that the national context is also governed by European and international guidelines. Reflecting the growing security concerns with critical infrastructure resilience, such as the generation, transmission and distribution of energy, water supply, banking and financial services, this issue has been on the international agenda for a long time. Following the adoption of Resolution 58/199 by the United Nations (UN) in 2003, on the creation of a global cybersecurity culture and the need to protect critical information infrastructures, calling for a more effective international cooperation in this area, it was specifically recognised that it is up to each State to identify its critical infrastructures.

In line with this concern, on 18 December 2008, the European Union created Directive 2008/114/EC, establishing a procedure for the identification and designation of European Critical Infrastructures (ECI) with the aim of promoting a common approach to their protection. This Directive was translated and transposed into domestic law by means of Decree-Law No 62/2011 of 09 May, which established procedures for the identification and protection of critical infrastructures related to the energy and transport sectors. As an example of the adoption of this new legal framework by the energy sector, infrastructures for the production and transmission of electricity and infrastructures for the production, refining, processing, storage and transportation of oil by pipelines, as well as the storage and transportation of gas, were identified and listed as critical infrastructures.

Building on this concern for critical infrastructure protection, in 2016 the EU recognised the growing dependence of the European society on cyberspace and adopted Directive 2016/1148 of 6 July (the NIS Directive), which includes a comprehensive set of measures to ensure a high common level of network and information security throughout the EU. This directive introduced the concept of "essential service operators" and "digital service providers", the need to define common minimum security requirements, as well as the need to implement a risk management culture and shared responsibility between public and private entities.

The NIS Directive was transposed into the Portuguese law by Law No 46/2018 of 13 August, which established the legal regime for cyberspace security, identifying a number of entities, such as the “energy distribution grid operator”, assigning them obligations to report incidents and establishing a system of penalties for non-compliance with the legislation in force. Recently, the draft decree-law regulating the legal regime for cyberspace security was submitted to public consultation, as it is a clarification of Law 46/2018, identifying in more detail such activities as the identification and reporting of vulnerabilities and the obligation to adopt risk management frameworks within the organisation.

Following a similar approach, it can be seen that the national regulatory framework for critical infrastructures is evolving in line with European directives, allowing the construction of a legal framework and imposing a practice that, due to its scope, already includes some key-sector organisations, with a tendency to expand and include more entities in the medium term. The organisations currently covered by Law 46/2018 and Decree-Law No 62/2011 have already developed contingency plans and capabilities for the protection of their infrastructure which, by law, should be constantly updated and tested to address the dynamic nature of new threats.

Given the framework of international alliances and organisations of which Portugal is an integral part, it is now important to characterise the international context, the cooperative efforts and to analyse how these factors contribute to the national strategic alignment.

3. CYBER RESILIENCE: A STRATEGIC CHALLENGE FOR EUROPE

In view of the national political and strategic alignment described above, a differentiated but still articulated evolutionary framework encompassing the defence and security of cyberspace is assumed as a relevant strategic driver. While the area of cyber defence has been influenced by the steps taken by NATO and the way that organisation approaches the development of military capabilities and the evolution of its cooperative cyber defence policy, the cybersecurity area is strongly influenced, sometimes even regulated/directed, by the EU with a position to strengthening the security and resilience of the digital ecosystem.

Aware of the strategic impact of cyber threats, in 2009, the EU also developed an European Union Cyber Defence Policy (EU, 2009), which was further expanded and approved in 2012 (EU, 2012). The first strategic cyber defence framework was adopted by the Council in 2014 (EU, 2014), contributing to the strengthening of European cooperation in this field.

Reinforcing this initiative, the EU Council also promoted the updating of the cyber defence strategic framework (EU, 2018), identifying priority areas for action and clarifying the roles to be played by all actors involved. To enhance its capacity to deal with cyber attacks, the EU announced a set of measures to encourage Member States to strengthen their cyber defence capabilities, offering the possibility for them to submit cooperative projects under the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF), including the launch of an education and training platform to enhance their training opportunities. Involving the industrial and technological sectors and

universities, national participation in European projects in the field of cyber defence is emphasised, in particular by assuming the co-leadership, together with France, of the EU Military Training Group Cyber Defence Discipline and by leading the Cyber Academy and Innovation Hub (CAIH), a PESCO Project coordinated by the Directorate-General of National Defence Resources.

In May 2019, the regulatory framework for the imposition of sanctions set out in the Cyber Diplomacy Toolbox (CDT) was approved and adopted by the EU Council as an instrument of the Common Foreign and Security Policy (EU, 2019). Reflecting the adoption of a more pragmatic approach, the recently-published new European Security Strategy (EU, 2020b) provides for the establishment of a cyberspace centre of expertise and a Joint Cyber Unit (EU, 2020b, p. 9), strengthening ongoing efforts in order to establish a common set of rules in the area of cybersecurity across all EU institutions. This could contribute to an increased situational awareness and to enhance cooperation between the various EU agencies and organisations, such as the European Union Agency for Cybersecurity (ENISA), Europol's European Cybercrime Centre (EC3) and the European Computer Security Incident Response Teams (CSIRT) network.

On 16 December 2020, the Commission presented the new EU Cybersecurity Strategy (2020c), which will play a key role in the construction of a digital future for Europe (EU, 2020d), in its economic recovery plan (EU, 2020e) and in affirming the European Security Strategy. The primary purpose of this strategy is to ensure the collective resilience of the EU against cyber-attacks. It aims to ensure that all citizens and businesses can fully benefit from trusted and reliable digital tools and services. Simultaneously, the Commission has also developed a set of initiatives aimed at increasing the physical and cyber resilience of the networks and systems operated by essential service providers, as well as to enhance the protection of critical infrastructures by presenting a proposal to revise the NIS Directive (EU, 2020f), geared towards the adoption of a set of measures to enhance the level of cybersecurity within the EU. At the same time, the EU has also ensured the adoption of a consistent approach with the proposed revision of the critical infrastructure resilience legislation, in particular by proposing a new directive on the resilience of critical entities (EU 2020g).

In this area, the EU has also strengthened its strategic partnership with NATO. Recognising that 22 of the 30 NATO nations are part of the EU, these organisations signed a joint declaration at the NATO summit in Warsaw (EU-NATO, 2016). Cybersecurity and cyber defence were taken up as priority areas for cooperation and concrete options were identified, with immediate effect.

Favouring the development of a convergent political vision and a common cooperative strategy, it should be noted that there is a wide range of other international initiatives already under way or to be launched within NATO, the EU, the UN and the Organisation for Economic Cooperation and Development (OECD). Stressing their strategic, operational and economic/industrial importance, Portugal assumed cybersecurity and cyber defence as priority areas for the development of cooperative capabilities, adopting for this purpose an "aggregating and sharing" perspective, in particular by exploring the concept of "smart defence" and "pooling & sharing", respectively within the framework of NATO and the EU.

4. DEFENCE POLICIES IN CYBERSPACE: DEVELOPMENT PROSPECTS

Anticipating the international security environment dynamic change, taking into consideration the European information and cyberspace security (EU, 2020b), the development of Member States' security and defence policies is expected to follow a set of guiding principles in order to:

- ensure that the policies adopted in this field reflect the dynamic spectrum of the threat, in particular with regard to organised crime, cross-border terrorism, social radicalisation activities and actions conducted by other actors (State and non-State) that affect the achievement of national interests and the safeguarding of national sovereignty;
- involve all governmental institutions, public administration, the private sector and all citizens, following an inclusive whole-of-society approach;
- integrate, in a coherent framework, the various policy areas with a direct impact on cyberspace security and defence, enhancing the security of the digital ecosystem;
- contribute to the construction of a long-term sustainable national resilience.

Bearing in mind that the defence of national cyberspace depends on the synergetic and "networked" action of the entire society, in line with the EU's vision, with a supplementary and complementary character, it is also considered necessary to promote the following political priorities:

- improve digital literacy and individual and collective awareness of the risks and threats posed by the Internet to the Portuguese society, by investing in cybersecurity awareness and education, thus reducing the knowledge gaps associated with cybersecurity and cyber defence;

- increase international cooperation and strengthen national synergies in these areas to facilitate the fight against cybercrime and reduce (existing) barriers to cooperation in the field of cybersecurity and cyber defence. This will make it possible to improve transversal knowledge and the adoption of best practices by addressing the risks associated with a social context of rapid technological innovation;
- strengthen Research, Development and Innovation (R&I) to seize the opportunities and overcome the challenges associated with cybersecurity raised by emerging technologies by accelerating the adoption of solutions capable of addressing their future impact on the international security environment;
- promote the adoption of scalable, dual-use (civil-military) and use-dually (multi-domain) cybersecurity solutions that can accelerate the adoption of best practices and increase national cyber resilience.

The implementation of this strategic vision, which is structured, operational and genetic, will greatly depend on the national capacity to join forces and generate concerted action by the various entities that contribute to the State's cybersecurity and cyber defence.

5. CONCLUSIONS

Today Portugal faces the challenge of deepening its digitisation effort and embracing the challenges of digital transformation by integrating and aligning the technological choices of an information society with cyberspace security. Assuming this challenge poses serious risks to the protection of interests and the defence of national sovereignty, it cannot be separated from the need to continuously adjust public policies to the strategic environment and to enhance the development of new processes and capabilities.

Cybersecurity and the protection of critical public and private national infrastructures are a primary responsibility of the State, in particular to ensure national resilience to cyber attacks. As an area of collective responsibility, the reduction of the attack surface and the multiple vulnerabilities of the networks, responsible for the provision of essential services, depends on the adoption of a preventive action of the public and private sectors which, to this end, need to mobilise the necessary knowledge and resources. However, while some private companies and institutions are relatively pretty aware of the risks associated with their sector, it should be highlighted that the vast majority are still mainly focused on their business areas and have no economic or commercial incentive to reduce existing vulnerabilities. In many cases, the costs involved far outweigh the benefits associated with

reducing the social risks associated with cyber attacks or even the risks arising from natural disasters.

To counteract the fragmented actions taken by the various entities responsible for the operation of essential/critical services, it is necessary to ensure a national approach consistent with the growing disruptive power of cyber threats and the increased attack surface, which pose important challenges to the security of modern societies. Efforts should be undertaken to review and adjust domestic legislation, in particular by proposing measures to strengthen the resilience of critical entities, services and networks.

The national digital ecosystem, which is permanently connected to cyberspace, also plays an important role, impacting the EU cybersecurity, the NATO cyber defence and even the global cybersecurity. This linkage and interdependence imposes a requirement on Portugal to honour its political commitments within the international organisations of which it is a member, ensuring the strategic alignment necessary to ensure cooperative security and collective defence in cyberspace, asserting itself as an important partner in the joint effort to ensure the stability of the international security environment. This requires the definition of consistent policies and strategies that are coherent with this reality and based on credible capacity building.

REFERENCES

European Council. (2020, 30 April). Declaration by the High Representative Josep Borrell, on the European Union, on malicious cyber activities exploiting the coronavirus pandemic. Available at: https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/.

Conselho Superior de Defesa Nacional (2014). *Conceito Estratégico Militar.* Available at: https://www.fd.unl.pt/docentes_docs/ma/FPG_MA_27255.pdf.

Curso de Promoção a Oficial General (CPOG) 2019-2020 (2020). Desafios Estratégicos para Portugal no Pós-Covid-19. Cadernos do IUM, 43. Lisbon: Instituto Universitário Militar.

Decree-Law No 69/2014 of 9 May (2014). *Cria o Centro Nacional de Cibersegurança (CNCS)*. Diário da República, 1.ª Série, 89, 2712-2719. Lisbon: Presidência do Conselho de Ministros.

Estado-Maior-General das Forças Armadas. (2018). *Diretiva Estratégica do EMGFA 2018-2021*, 18 April 2018. Lisbon: Chefe do Estado-Maior-General das Forças Armadas.

Freire, F., Nunes, P. & Acosta, O. (2013). Estratégia da Informação e Segurança do Ciberespaço, trabalho de investigação conjunta (IDN-CESEDEN), IDN Nº12, Imprensa Nacional – Casa da Moeda.

Organic Law No 02/2019 of 17 June (2019). *Aprova a Lei de Programação Militar* (LPM) e revoga a Lei Orgânica n.º 7/2015. Diário da República, 1.ª Série, 114, 2982-2985. Lisbon: Assembleia da República.

Organic Law No 46/2018 of 13 August (2018). *Aprova o Regime Jurídico da Segurança do Ciberespaço*. Diário da República, 1.ª Série-A, 155, 4031-4037. Lisbon: Assembleia da República.

Ministério da Defesa Nacional. (2013). *Orientação para a Política de Ciberdefesa* (Despatch No 13692/MDN of 11 October). Lisbon: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2018). *Diretiva Ministerial de Orientação Política para o Investimento na Defesa* (Despatch No 4103/MDN of 12 April). Lisbon: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2019a). *Proposta de Estratégia Nacional de Ciberdefesa* Lisbon: Direção-Geral de Recursos da Defesa Nacional.

Ministério da Defesa Nacional. (2019b). *Linhas Orientadoras para a Estratégia Nacional de Ciberdefesa-Horizonte 2019-23* (Despatch No 52/MDN of 23 October). Lisbon: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2020a). *Diretiva Ministerial de Planeamento de Defesa Militar* (Despatch No 2536/MDN of 24 February). Lisbon: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2020b). *Criação do Comité de Monitorização da Ciberdefesa* (Despatch No 15/2020 of 6 February). Lisbon: Ministro da Defesa Nacional.

North Atlantic Treaty Organization. (2010). NATO Strategic Concept 2010. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf. Accessed on 14 May 2020.

North Atlantic Treaty Organization. (2014a). *Wales Summit Declaration: Issued by the Heads of State and Government partipating in the meeting of the North Atlantic Council in Wales*. Press Release (2014) 120, 5 September 2014. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

North Atlantic Treaty Organization. (2014b). *Enhanced NATO Policy on Cyber Defence* (Decision PO/2014/0358). Brussels: Emergency Security Challenge Division.

North Atlantic Treaty Organization. (2016a). *Cyber Defence Pledge*. NATO Warsaw Summit Press Release (Communiqué 124). Brussels: NATO Allied Council.

North Atlantic Treaty Organization. (2018). *Military Vision and Strategy on Cyberspace as a Domain of Operations* (Decision of 12 June). Brussels: Military Committee.

North Atlantic Treaty Organization. (2019a). *London Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London, 3-4 December 2019*. Press Release (2019) 115, 4 December 2019. Available at: https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

Nunes, P.F.V. (Ed.). (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa.* IDN Cadernos, 28. Lisbon: Instituto da Defesa Nacional.

Nunes, P.F.V. (2020). *A Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Definição de uma Estratégia Militar para o Ciberespaço.* Coleção "ARES", 36. Lisbon: Instituto Universitário Militar.

Resolution of the Assembly of the Republic No 15/2005 of 7 April. (2005). *Aprova a VII Revisão Constitucional da Constituição aprovada pela Assembleia Constituinte, 02 de abril de 1976*. Diário da República, 1.ª Série, 74, 2979-2979. Lisbon: Assembleia da República.

Resolution of the Council of Ministers No 115/2017 of 13 July 2017. (2017). *Cria o grupo de projeto denominado "Conselho Superior de Segurança do Ciberespaço"*. Diário da República, 1.ª Série, 163/2017, 5035 – 5037. Lisbon: Presidência do Conselho de Ministros.

Resolution of the Council of Ministers No 19/2013 of 21 March. (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1.ª Série, 67, 1981–1995. Lisbon: Presidência do Conselho de Ministros.

Resolution of the Council of Ministers No 26/2013 of 11 April. (2013). Aprova a reforma "Defesa 2020". Diário da República, 1.ª Série, 77, 2285–2289. Lisbon: Presidência do Conselho de Ministros.

Resolution of the Council of Ministers No 92/2019 of 5 June. (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1ª Série, 108, 2888–2895. Lisbon: Presidência do Conselho de Ministros.

European Union-North Atlantic Treaty Organization. (2016). *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*. Available at: https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

European Union. (2009). *EU Concept for Computer Network Operations in EU-led Military Operations* (EEAS Decision 13537/09). Brussels: European Union Military Staff.

European Union. (2012). *EU Concept for Cyber Defence for EU-led Military Operations* (Decision EEAS01729/12). Brussels: European Council.

European Union. (2017). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* Available at: http://data.consilium.europa.eu/doc/document/ST-7923-2017-REV-2/en/pdf.

European Union. (2019). *Council Decision (CFSP) ST/7299/2019/INIT concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. Available at https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32019D0797.

European Union. (2020a). Council Implementing Regulation (EU) 2020/1124 of 30 July 2020 implementing Regulation (EU) 2016/1686 imposing additional restrictive measures directed against ISIL (Da'esh) and Al-Qaeda and natural and legal persons, entities or

bodies associated with them, *Official Journal of the European Union L 246*, Vol. 63, pp. 1-4. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2020:246:FULL&from=EN

European Union. (2020b). European Security Union. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en.

European Union. (2020c). The Cybersecurity Strategy. Available at: https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy.

European Union. (2020d). *Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273.

European Union. (2020e). *Recovery plan for Europe*. Available at: https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

European Union. (2020f). *Shaping Europe's digital future: NIS Directive*. Available at: https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive.

European Union. (2020g). *Migration and Home Affairs: Protection*. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/protection_en.