https://www.doi.org/10.12797/9788381383899.01

Andrzej Jacuch
Military University of Technology, Poland

European Union response to hybrid threats

Abstract: We live in an era of hybrid threats. Hence, the EU and its member nations are redefining their security policy and implementing new strategies. The objective of this paper is to identify, analyze, and assess the EU responses to hybrid threats targeting European, and particularly Central and Eastern Europe countries' security. The main hypothesis stipulates that 'resilience' with civil preparedness as its central pillar forms a base of the EU strategy and that cybersecurity and strategic communication are EU's priorities.

Is resilient cyberspace critical for our daily life, economy, and national security? Should we enhance strategic communications? How to prepare our civil sectors to continue providing essential services to population and supporting military operations in a crisis?

Europe is facing the greatest security challenges since the end of the Cold War. Crimea seizure, the destabilization of eastern Ukraine, disinformation campaigns, cyber-attacks, terrorism, crisis in the Middle East, poverty, global financial volatility, and current COVID-19 pandemic create new challenges. The security environment has become more demanding because of globalization. How to prepare for a crisis?

Keywords: European Union, resilience, civil preparedness, cybersecurity, disinformation

Introduction

Hybrid threats are our main security challenges. Russia's intervention in Crimea, eastern Ukraine and Black Sea, as well as Middle East, terrorism, illegal migration, complex political crises, natural disasters, cyber-attacks, fake news, and propaganda, etc. have involved the Western world in a new type of Cold War. Our world is increasingly insecure.

With globalization and a new level of interconnectedness, thanks to the Internet and social media, security is at risk. Moreover, outsourcing of non-combatant military tasks has become the norm and, as a result, dependence of the armed forces on the availability of civilian resources has increased. Particularly, the use of hybrid tactics and means to seize Crimea and destabilize Ukraine have changed our perception of world's security. Russia, taking advantage of geographical proximity and of former and existing social and economic relations, is targeting security of European countries.

Effective and efficient countering hybrid threats requires in-depth analysis and places great constraints on policy makers. The question should be asked how to respond to these threats, what capabilities should be developed, where to invest, what and how infrastructure and services should be protected. This requires answers to questions such as: What strategy did Russia use to seize Crimea and destabilize Ukraine? What are EU responses to hybrid threats? What is resilience in security context? What are the EU resilience priorities? The aim of the study is to substantiate the thesis that strengthening resilience, the combination of civil preparedness and military capacity, is crucial for national and international security. This paper focuses on civil preparedness.

The EU has taken steps to counter hybrid threats by building societal resilience. The EU and NATO have discussed security environment and decided on the strengthening of civil preparedness by building resilience in areas critical for national and regional security and defense. They cooperate on countering hybrid threats, building resilience, increasing military mobility, improving critical infrastructure protection, strengthening cyber security and strategic communication.[1]

The article considers hybrid threats, brings an assessment of the hybrid warfare employed by Russia in Ukraine, determines which elements were most critical for Russia's success and presents the EU measures and structures to counter hybrid threats. Europe must be prepared for a crisis, including natural and man-made disasters,[2] and

[1] Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, 10 Jul. 2018.

[2] A. Jacuch, 'Disaster response mechanisms in EU and NATO,' *Przegląd Europejski*, 2019/3, p. 73.

able to respond to and recuperate after hybrid attacks. Closing remarks reiterate that strengthening resilience is EU's strategic response to hybrid threats. In the research process qualitative methods were used, including analyses based on interviews of civil and military experts in the research field, public records, policy documents, legislative acts, media statements as well as professional experience of the author.

Hybrid threats

In his treaty *On War*, Carl von Clausewitz wrote that war is not merely a political act, but a real political instrument, a continuation of the political process by other means. Sometimes, these means are conventional, legal in accordance with international humanitarian law, however, this is rarely the case. Hybrid threats are variable and may take different forms, including fake news and propaganda, malicious cyber activities, sabotage, economic means, etc. Particularly challenging are information operations and cyberspace warfare.

The EU defines: "Hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives. Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion to hinder swift and effective decision-making."[3]

The Polish Bureau of National Security (Biuro Bezpieczeństwa Narodowego, BBN) defines hybrid war and introduces the term of 'subthreshold aggression.' Hybrid war combines various possible simultaneous means and methods of violence, including regular and irregular armed actions, cyberspace operations and economic or psychological information campaigns.[4] Hybrid war combines symmetrical and asymmetrical (classic and non-classical) methods of action and uses both military and non-military means. Hybrid concepts and strategies target vulnerabilities – from disinformation and propaganda, cyber-attacks on critical information systems, through the disruption of critical services and infrastructures, such as energy supplies or financial services, to

[3] EU Website, *A Europe that Protects: Countering Hybrid Threats* (retrieved on 24.04.19).

[4] *Słownik BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa – wojna hybrydowa, agresja podprogowa*, https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (retrieved on: 10.04.2019).

undermining public trust in government institutions or social cohesion. The diversity of hybrid tactics masks the thoroughly planned order behind the spectrum of tools used and the effects being achieved.[5]

In 2013, the Chief of General Staff of the Russian Armed Forces General Valery Vasilyevich Gerasimov wrote: "The role of non-military means of achieving political and strategic objectives has increased and in many cases, exceeded military capabilities in its effectiveness." Russia sees 'non-linear' actions consisting of military and non-military elements combined in an integrated, comprehensive strategy as the future of warfare.[6] According to Gerasimov's doctrine, non-military methods of conducting conflict – including information warfare – are more effective than conventional weapons. The concept of hybridity has been attributed to the Russian-Ukrainian conflict.

Hybrid warfare in Ukraine

The Russia-Ukraine conflict is a classical hybrid conflict. "It has involved a combination of activities, including disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure, and military actions."[7] Polish scholars Mirosław Banasik and Ryszard Parafianowicz distinguish four stages of the hybrid war in Ukraine: political diversion, building the social and political position of separatists, armed intervention, and deterrence.[8] In 2014, it was difficult to determine who the opponent was. Non-military actions and military instruments were used. The main stress was on non-military activities, such as propaganda and disinformation, cyber-attacks, provoking unrests on political grounds, destabilizing economy, applying financial pressure, intensifying corruption and crime, conflicting ethnic groups, illegal border crossing and disinformation about its purpose, attacks on electricity networks

[5] R. D. Thiele, 'Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective,' *ISPSW Strategy Series: Focus on Defence and International Security*, 449, 2016.

[6] V. V. Gerasimov, *'Tsennost' nauki v predvidenii'. Voyenno-promyshlennyy kur'yer*, 8(476), 27 Feb. 2013, http://www.vpk-news.ru/articles/14632.

[7] *The Conversation, Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?*, the UK, 17.06.2019, https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841 (retrieved on 19.06.2020).

[8] M. Banasik, R. Parafianowicz, 'Teoria i praktyka działań hybrydowych,' *Zeszyty Naukowe Akademii Obrony Narodowej*, 2(99), 2015, p. 11.

and power plants, etc. The course of the conflict also shows that the Russians' aim was not to occupy Ukraine, but to destabilize its eastern part.[9]

Propaganda and disinformation, cyber-attacks, subsequent low morale of Ukrainian forces and lack of military mobility were main reasons for handing over Crimea to Russia without any fight. Consistent informational warfare in many different environments led to the outbreak and continuation of the conflict. Cyberspace has also become one of the major battle fields. In addition to the armed struggle in the east of Ukraine, the Russian Federation has been conducting a cyber warfare against the Ukrainian state. The activity of the Russian Federation, supported by various groups and organizations, is conducted in several dimensions simultaneously (these include cyber-attacks, cyber-spying, and mass-propaganda on the internet). The common goal of these activities is to destabilize Ukraine by breaking the ties between the state and society.[10]

The Russia-Ukraine conflict drew attention to the challenges closer to the territory of the Alliance and the EU. To counter new security threats posed by this conflict, NATO decided on the most significant strengthening of common defense capabilities as well as civil preparedness and decided to increase resilience in areas that are critical for NATO's collective defense. In response to Russian hybrid warfare, NATO adopted the Readiness Action Plan (RAP).[11] The Alliance has been responding to challenges growing from various strategic directions.[12]

In April 2016, the EU adopted its 'Joint framework on countering hybrid threats – a European Union response.'[13] It outlined actions at the EU and national levels, which included raising awareness and building resilience in cybersecurity, critical infrastructures, protection of the financial system, protection of public health, and supporting efforts to counter violent extremism and radicalization. NATO and the EU cooperate in areas such as countering hybrid threats, building resilience, increasing military mobility, improving infrastructure, cyber security and defense, and strategic communication.[14]

[9] A. Jacuch, *Civil Preparedness – Military Mobility*, chapter 12 of *Security and Russian Threats*, M. Banasik, P. Gawliczek, A. Rogozińska (editors), Piotrków Trybunalski 2019, p. 236.

[10] F. Bryjka, *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej.* In *Bezpieczeństwo personalne a bezpieczeństwo strukturalne III. Czynniki antropologiczne i społeczne bezpieczeństwa personalnego*, T. Grabińska, Z. Kuźniar (editors), Wrocław 2015, pp. 128-129.

[11] 2014 Summit Declaration, para 5.

[12] 2019 London Declaration, para 3.

[13] Joint communication to the European Parliament and the Council: 'Joint Framework on countering hybrid threats - a European Union response,' JOIN(2016) 18 final.

[14] *EU-NATO cooperation – Factsheet*, 2018 (retrieved on 24.04.19).

Resilience as the EU response to hybrid threats

There are many definitions of resilience, but neither is perfect for all contexts. A comprehensive discussion on resilience in security context has been presented by the Centre for Transatlantic Relations, Johns Hopkins University. It describes the key operational characteristic, the physiology, morphology of resilience and recipes for resilience. There are three core abilities: to survive a sudden shock; to return to its original state after the shock; and to adjust itself to new conditions if they do not permit a return to the original state, but without losing its essence and vitality. The essence or core function of a resilient system would survive a shock, where supporting elements, important under normal circumstances, may be sacrificed in a crisis. Under extreme stress, the active functioning of the essence may be shut down retaining the minimum necessary to restart functioning when conditions allow.[15]

The EU defines resilience as: "… the ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks."[16] It highlights two resilience dimensions: the strength of an entity to resist pressure and shock and the capacity to recuperate rapidly from the impact. Increasing resilience and reducing vulnerability requires enhancing the entity's strength and/or reducing the impact.

Building resilience has become a strategic priority for the EU and its member states. To respond to hybrid warfare in today's global interconnected world, with new technologies, Internet, social media and artificial intelligence, it is necessary to develop comprehensive security. This would require involving all relevant actors – civil and military, administration and private (national companies and international corporations), and academia – in this process. Working together requires building trust between all participants of this process. In response to hybrid threats, the EU develops its capabilities, continues building readiness and resilience by improving civil preparedness in areas that are critical for EU's security and defense.

[15] T. Ries, Chapter 1, *Forward Resilience in Context*. In *Forward Resilience: Protecting Society in an Interconnected World*, D. S. Hamilton (editor), Centre for Transatlantic Relations, Johns Hopkins University, 2016.

[16] Communication from the Commission to the European Parliament and the Council, The EU Approach to Resilience: Learning from Food Security Crises, COM(2012) 586 final, p. 5.

In 2013-2014, the EU set up a new Civil Protection Mechanism (CPM).[17,18] The Mechanism can be activated for any serious natural or man-made disaster.[19] In 2016, the EU adopted a Joint Framework to counter hybrid threats and foster resilience.[20] It outlined actions, like raising awareness and building resilience in cybersecurity, critical infrastructures, protection of the financial system, protection of public health, and supporting efforts to counter violent extremism and radicalization. Further actions have been put forward to reinforce these efforts, such as hybrid risk surveys to identify key vulnerabilities and develop capacities for proactive strategic communication. It defined effective procedures for preventing, responding to and recovering from crisis and examined applicability and practical implications of the Solidarity Clause[21] and the mutual Defense Clause,[22] in case of a serious hybrid attack. The EU identified areas for enhanced cooperation and coordination with NATO as well as other partner organizations on countering hybrid threats.

In June 2016, the EU provided strategy for resilience,[23] which was translated into priorities and actions in 2017.[24] The approach to resilience aims at strengthening: the adaptability; the capacity of a state to build, maintain or restore its core functions; the capacity of societies, communities and individuals to manage opportunities, and to build, maintain or restore livelihoods in the face of major pressures. The EU has been strengthening cybersecurity, including EU structures and response capabilities, safer internet, and efforts to counter violent extremism and radicalization. These measures are part of wider EU's response to hybrid threats.[25] The EU has been developing measures and structures particularly in two areas – cybersecurity and strategic communications – to monitor, prevent and counter aggressive operations in cyber and information spaces, such as cyber-attacks, fake news, and propaganda.

[17] Decision No. 1313/2013/EU (2013), On a Union Civil Protection Mechanism.

[18] Commission implementing Decision laying down rules for the implementation of Decision No. 1313/2013/EU and of the Council on a Union Civil Protection Mechanism and repealing Commission Decisions 2004/277/EC, C(2014)7489/F1 (2014).

[19] A. Jacuch, *Disaster response…*, p. 72.

[20] Joint communication to the European Parliament and the Council: 'Joint Framework on countering hybrid threats - a European Union response,' JOIN(2016) 18 final.

[21] The Solidarity clause introduced by Article 222 of the Treaty on the Functioning of the European Union (TFEU).

[22] Article 42 (7) TEU states: If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter.

[23] The European Union Global Strategy for the Foreign and Security policy, EUGS 2016.

[24] Joint Communication to The European Parliament and The Council, Brussels, A Strategic Approach to Resilience in the EU's external action, JOIN(2017)21 final (2017).

[25] EU Website, A Europe that Protects: Countering Hybrid Threats (retrieved on 24.04.19).

Cybersecurity measures

The 2013 EU cybersecurity strategy clarifies roles and responsibilities and proposes specific activities, such as achieving cyber resilience; reducing cybercrime; developing an EU Cyber Defense Policy and capabilities in the framework of the Common Security and Defense Policy; developing the industrial and technological resources for the Digital Single Market; establishing international cyberspace policy for the EU and building capacity.[26] Since then, the EU has adopted legislative proposals, secured investment for research and innovation in cybersecurity, and fostered cooperation within the EU and with partners, particularly NATO. In 2016, the Commission adopted a set of measures for cooperation in case of a large-scale cyber incident.[27] The adoption of the Directive on security of network and information systems (NIS) by the European Parliament in July 2016 is the first EU-wide legislation on cybersecurity across the Union.[28] It defines organization of the national cybersecurity system and the tasks and responsibilities of the entities comprising that system. The national cybersecurity system aims at ensuring cybersecurity, including the uninterrupted provision of key and digital services. The national cybersecurity system includes: 1) key service providers; 2) digital service providers; 3) three Computer Security Incident Response Teams, sectoral cyber security teams; and public finance sector entities. Another body established by the new law is the Critical Incident Panel.

In September 2017, The EU published a cybersecurity package including existing instruments and new initiatives to improve cyber security in three areas: resilience to cyber-attacks and cybersecurity capacity; an effective criminal law; and global stability through international cooperation.[29] In 2018, the Commission proposed the creation of a Network of Cybersecurity Competence Centers and a new European Cybersecurity Industrial, Technology and Research Competence Center to invest in cybersecurity capacity in the EU. It has also recommended measures to ensure cybersecurity of

[26] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/01 final.

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final.

[28] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, L 194/1.

[29] Joint Communication to the European Parliament and the Council Brussels on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13.9.2017, JOIN(2017) 450 final.

5G networks in the EU and the measures which can be used to strengthen the EU's response to activities that harm its interests.

The 2019 Cybersecurity Act[30] has provided a consolidated cybersecurity certification framework. It has reformed the ENISA and created a certification framework, which provides support to Member States, EU institutions and businesses, including the implementation of the NIS Directive. The European Cyber Security Organization and Digital Europe Organization provide the NIS Implementation Tracker, which presents current status of the implementation of the NIS Directive in all member countries. In March 2019, several countries did not have a fully implemented Directive in place. However, given that all countries already have their own 'laws and regulations,' there are issues like: the lack of European critical infrastructure; entities that do not have their seat in the EU's area; and a clear reference to EU citizens (e.g. social networks).

In July 2019, a dedicated Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats has been set up. It deals with questions relevant for the capacities to counter and respond to hybrid threats and supporting measures to strengthen societal resilience. The objective is to facilitate coordination within the Council and with other EU institutions, services, and agencies.

Countering disinformation

The EU defines 'disinformation' as verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public; it distorts public debate, undermines citizens' trust in institutions and media, and even destabilizes democratic processes such as elections.[31]

Since 2015, the EU has been implementing measures to address disinformation, protect its democratic systems and public debates. To address Russia's disinformation campaigns, the EU set up the East StratCom Task Force in March 2015.[32] It develops communication products and campaigns focused on explaining EU. It also

[30] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), L 151/15.

[31] EEAS homepage, Countering disinformation, 11/03/2019, https://eeas.europa.eu/topics/countering-disinformation/59411/countering-disinformation_en (retrieved on 24.04.19).

[32] EEAS homepage, Questions and Answers about the East StratCom Task Force, 05/12/2018, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en (retrieved on 10.01.2020).

reports on and analyses disinformation trends, explains and corrects disinformation narratives, and raises awareness of disinformation. To this last end, it produces the weekly *Disinformation Review*.[33]

In June 2018, the Joint Communication: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats focused on strategic communications and situational awareness, resilience and cybersecurity, and counterintelligence.[34] In September 2018, the Commission issued a package of measures to support free and fair European elections, including protection against cybersecurity incidents and fighting disinformation campaigns. In December 2018, the EU announced its action plan against disinformation. Its key priority was to address potential threats to the elections and to strengthen the resilience of the EU's democratic systems.[35] In 2019, a Rapid Alert System on Disinformation was set up, the EU, member states and the ENISA carried out a live test of their preparedness, and the EU published its report on the progress achieved in the combat against disinformation and the main lessons identified from the European elections.[36]

The EU and NATO countering hybrid threats

In December 2015, NATO adopted its strategy on how to fight hybrid threats[37] and four months later, the EU adopted its 'Joint framework on countering hybrid threats – a European Union response.' Both NATO and the EU work closely on countering hybrid threats and enhancing resilience with a special focus on countering cyber-attacks and disinformation.

In 2016 and 2017, the EU and NATO decided on 74 actions within the seven areas on countering shared threats among Member States and the increasing need to protect infrastructure or cross-border networks. It called for working with a variety of actors in order to improve resiliency, security, and continuity of governance in the

[33] EUvsDisinformation, https://euvsdisinfo.eu/ (retrieved on 10.01.2020).

[34] Joint Communication to the European Parliament, the European Council and the Council Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final.

[35] Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions on Action Plan against Disinformation, JOIN(2018) 36 final.

[36] Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Region, Report on the implementation of the Action Plan Against Disinformation, JOIN(2019) 12 final.

[37] Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, 2 December 2015.

face of hybrid threats. It also put in place cooperative working mechanisms at staff and senior levels.[38] Four progress reports highlighted main achievements and added value of EU-NATO cooperation, including in countering hybrid threats.[39]

In July 2018, the EU and NATO signed a second Joint Declaration in Brussels calling for swift and demonstrable progress in implementation. In September 2018, NATO's North Atlantic Council and the E.U.'s Peace and Security Committee held a discussion on hybrid threats with a subsequent scenario-based exercises.[40]

In late 2018, NATO established Counter Hybrid Support Teams and other military advisory bodies (in the areas of cyber, electronic warfare, and chemical, biological, radiological and nuclear capabilities) to assist allies in the event of a hybrid crisis. In late 2019, the first Counter Hybrid Support team was deployed to Montenegro.[41] In April 2017, the EU established its Centre of Excellence for Countering Hybrid Threats in Helsinki. It works both with the EU and NATO and serves as a hub of expertise, working on improving civil-military capabilities, resilience and preparedness to counter hybrid threats.[42] NATO established the Strategic Communications Centre of Excellence in Riga, Latvia; the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia; and the Energy Security Centre of Excellence in Vilnius, Lithuania.[43]

Conclusions

A shift from the classic military confrontation to information and cyber warfare can be noticed. The information era, globalization, and internet have brought new capabilities as well as new vulnerabilities. Countering hybrid threats requires a comprehensive approach, involving all relevant actors, to raise awareness, increase resilience, and active measures to prepare and protect the functions and structures that are most likely to

[38] Council of the EU Press release, EU-NATO cooperation: Council adopt conclusions to implement Joint Declaration. Brussels, 6 December 2016.

[39] Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017, 2019.

[40] The Foreign Service Journal AFSA, Working with NATO to Address Hybrid Threats, Washington DC, 2019.

[41] NATO Website, *NATO: Ready For the Future - Adapting the Alliance (2018-2019)*, 2019, pp. 8, 9, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf (retrieved on 08.12.2019).

[42] The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/what-is-hybridcoe/ (retrieved on 08.12.2019).

[43] NATO Website, Centres of Excellence, 2019, https://www.nato.int/cps/en/natohq/topics_68372.htm (retrieved on 08.12.2019).

be targeted by hybrid attacks.[44] A way to respond to the hybrid threats is resilience. Strengthening resilience serves avoiding escalation of crises both within and outside of the EU and NATO.[45]

Lessons identified from the conflict in Ukraine show that if territorial integrity is under any form of hybrid aggression, than in order to resist this type of aggression, adequate civil preparedness, political and military means have to be employed at national and regional levels, including such crisis response measures as counter-aggression in information and cyber spaces. The previous sections showed that in reaction to hybrid threats, the EU have further adapted its strategy, structures, regulations and other measures to counter them. NATO continues building readiness and resilience. In particular, along with military reinforcement, NATO has been improving civil preparedness in the areas that are critical for NATO's collective defense.

Each country is responsible for strengthening resilience of its infrastructures and services, governance, and defense. However, there are cross-border infrastructures and services and trans-border and transnational systems and interest which are vital at national, regional and global levels. For NATO, seven areas that must be resilient in order to support deterrence and collective defense have been defined. Civil preparedness serves defense by enabling military operations, primarily enabling military mobility, which is a force multiplier.

Awareness, resilience, and response are crucial for countering hybrid threats. The EU has been improving its capacity to detect and understand malicious activities at an early stage; enhancing the resilience of critical infrastructure, societies and institutions. The EU directives and regulations have guided the planning by members, including the commercial sector. The EU focuses on responses to cyber threats and on countering disinformation and propaganda.

Civil preparedness, and particularly adaptive resilience, including vulnerability reduction in critical areas allowing to resist and recover from any kind of attack, kinetic and/or hybrid, is of key importance. In a crisis, civil sectors must be prepared and ready to resist any shock, recover quickly, continue to provide essential services to population and government and to support military operations. In today's globally interconnected world, information operations and cyber-attacks are the most common means used by aggressive and malicious state and non-state actors. What goes unnoticed is they often target young population, who are social media and internet 'citizens.' Being prepared,

[44] A. Hagelstam, K. Narinen, 'Cooperating to counter hybrid threats,' *NATO Review Magazine*, 2018.

[45] A. Wieslander, *How NATO and the EU can Cooperate to Increase Partner Resilience*, Chapter 12 in *Forward Resilience: Protecting Society in an Interconnected World*, Washington, DC, 2016.

protected, and ready to respond to a crisis, requires cooperation and involvement of all relevant actors, including partner bodies and international bodies, as well as key private industry players and academics. Comprehensive approach to resilience is necessary, however, working together requires trust among all involved parties.

Today, the pandemic COVID-19 can have far-reaching consequences for national and regional security. Countries will have to adapt their military and civil emergency planning capabilities to traditional security threats, to hybrid threats as well as to new challenges resulting from, among others, technological developments, climate change, pandemics, and mass migration. The advancement of civil preparedness in critical sectors is necessary to ensure that countries are prepared to prevent and respond to future threats.

References

Documents

2014 Wales Summit Declaration.

2019 London Summit Declaration.

Commission implementing Decision laying down rules for the implementation of Decision No. 1313/2013/EU and of the Council on a Union Civil Protection Mechanism and repealing Commission Decisions 2004/277/EC, C(2014)7489/F1 (2014).

Communication from the Commission to the European Parliament and the Council, The EU Approach to Resilience: Learning From Food Security Crises, COM(2012) 586 final, p. 5.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final.

Decision No. 1313/2013/EU (2013), On a Union Civil Protection Mechanism.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, L 194/1.

Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/01 final.

Joint communication to the European Parliament and the Council: 'Joint Framework on countering hybrid threats - a European Union response,' JOIN(2016) 18 final.

Joint Communication to The European Parliament and The Council, Brussels, A Strategic Approach to Resilience in the EU's external action, JOIN(2017)21 final (2017).

Joint Communication to the European Parliament, the European Council and the Council Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final.

Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions on Action Plan against Disinformation, JOIN(2018) 36 final.

Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Region, Report on the implementation of the Action Plan Against Disinformation, JOIN(2019) 12 final.

Joint Communication to the European Parliament and the Council Brussels on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13.9.2017, JOIN(2017) 450 final.

Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 10 Jul. 2018, https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), L 151/15.

The European Union Global Strategy for the Foreign and Security policy, EUGS 2016.

Chapters in joint publication:

Bryjka F., *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej*. In T. Grabińska, Z. Kuźniar (editors), *Bezpieczeństwo personalne a bezpieczeństwo strukturalne III. Czynniki antropologiczne i społeczne bezpieczeństwa personalnego*, Wrocław 2015.

Jacuch A., Chapter 12 *Civil Preparedness – Military Mobility*. In M. Banasik, P. Gawliczek, A. Rogozińska (editors), *Security and Russian Threats*, Piotrków Trybunalski 2019.

Ries T., Chapter 1 *Forward Resilience in Context*. In Daniel S. Hamilton (editor) *Forward Resilience, Protecting Society in an Interconnected World*, Center for Transatlantic Relations, Washington, DC, 2016.

Wieslander A., Chapter 12 *How NATO and the EU can Cooperate to Increase Partner Resilience*. In Daniel S. Hamilton (editor), *Forward Resilience: Protecting Society in an Interconnected World*, Working Paper Series, Center for Transatlantic Relations, Washington, DC, 2016.

Journal Articles:

Banasik M., Parafinowicz R., 'Teoria i praktyka działań hybrydowych,' *Zeszyty Naukowe Akademii Obrony Narodowej*, 2(99)/2015, p. 11.

Gerasimov V. V., *'Tsennost' nauki v predvidenii'. Voyenno-promyshlennyy kur'yer*, 8(476)/, 27 Feb 2013, http://www.vpk-news.ru/articles/14632.

Hagelstam A., Narinen K., 'Cooperating to counter hybrid threats,' *NATO Review Magazine*, Brussels, 2018.

Jacuch A., 'Disaster response mechanisms in EU and NATO,' *Przegląd Europejski* 3/2019, Warsaw, 2019, https://doi.org/10.5604/01.3001.0013.5842.

Thiele R. D., 'Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective,' *The Institute for strategic, political, security and economic* *consultancy (ISPSW) Strategy Series: Focus on Defence and International Security*, 449/2016, Berlin.

'Working with NATO to Address Hybrid Threats,', The Foreign Service Journal AFSA, Washington DC, 2019.

Press statements:

Council of the EU Press release, EU-NATO cooperation: Council adopt conclusions to implement Joint Declaration. Brussels, 6 December 2016.

Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, Brussels, 2 December 2015.

Internet sources:

EEAS homepage, Countering disinformation, 11/03/2019, https://eeas.europa.eu/topics/countering-disinformation/59411/countering-disinformation_en.

EEAS homepage, Questions and Answers about the East StratCom Task Force, 05/12/2018, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and--answers-about-the-east-stratcom-task-force_en.

EUvsDisinformation, https://euvsdisinfo.eu/.

NATO Website, Centres of Excellence, 2019, https://www.nato.int/cps/en/natohq/topics_68372.htm.

NATO Website, NATO: Ready for the Future - Adapting the Alliance (2018-2019), 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129--adaptation_2018_2019_en.pdf.

Słownik BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa – wojna hybrydowa, agresja podprogowa, https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html.

The Conversation, Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?, the UK, 17.06.2019, https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841.

The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/what-is-hybridcoe/.