The Copernicus Journal of Political Studies 2020
No. 1/2020, pp. 5–26
ISSN 2299-4335
DOI: http://dx.doi.org/10.12775/CJPS.2020.001
www.apcz.umk.pl/czasopisma/index.php/CJPS

# Articles

**Andrzej Jacuch**[1]
Military University of Technology, Poland

# COUNTERING HYBRID THREATS: RESILIENCE IN THE EU AND NATO'S STRATEGIES

## ABSTRACT

The objective of this paper is to identify, analyze and assess NATO's and the EU's responses to hybrid threats targeting Europe, in particular the Baltics[2], the Visegrád Group[3] and the Balkan[4] countries. It considers measures, regulations, structures and capabilities of both organizations. The main hypothesis stipulates that strengthening resilience through civil preparedness is the basis of both NATO and EU strategies to counter hybrid threats, and that cybersecurity, strategic communication and military mobility are key areas the two organizations are working on.

[1] This article reflects the personal opinions of the author and does not represent the views of any institution or organisation.

[2] Estonia, Latvia, and Lithuania.

[3] The Czech Republic, Hungary, Poland, and Slovakia.

[4] Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Kosovo, Montenegro, North Macedonia, Romania, Serbia, and Slovenia.

Is resilient cyberspace critical for our daily life, economy, and national security? Should we enhance strategic communications to prevent disinformation? How to prepare our civil sectors so that they 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. The seizure of Crimea, destabilization of Eastern Ukraine, disinformation campaigns, cyber-attacks, terrorism, crisis in the Middle East, poverty, and global financial volatility create new challenges and involve Western countries in a hybrid war, fought predominantly on cyber and information fronts with the extensive use of social media. Meanwhile, globalization has made the security environment more demanding, raising an urgent question: How to prepare for a crisis?

**Key words**

NATO, EU, hybrid threats, resilience, civil preparedness

> *"We do not merely destroy our enemies, we change them.*
> *We change their thoughts."*
>
> *George Orwell*, 1984

## Introduction

During the Cold War, the blocs on both sides of the Iron Curtain continued to build their military capacity and prepared their civil sectors "in order to ensure that the Home fronts will stand the strain of war" (Ismay, 1957). Civil sectors were prepared to support the military and protect civil population in case of war. Civil preparedness, also called civil emergency planning, was an important pillar of defense strategies. At that time NATO established mechanisms for control and use of civil assets and infrastructure during a crisis or war, which included the NATO Civil Wartime Agencies (Jacuch, 2018).

Today we are facing new threats where the main security challenges are of a hybrid kind. Russia's intervention in Crimea, Eastern Ukraine and in the Black Sea; incidents involving Soviet planes and warships on the Baltic Sea; conflicts in Iran and Syria; terrorism, illegal migration, complex political crises, natural disasters, cyber-attacks, fake news and propaganda, threat of financial crisis, etc. – all this makes our world an increasingly insecure place. Globalization and a new level of interconnectedness, the Internet and social media – all this poses a security risk. Outsourcing of non-combatant military tasks has become the norm, leading to increased dependence of the armed forces on the availability of civilian resources (Jacuch, 2019a). What has particularly changed our perception of the global security was the use of hybrid tactics and means to seize Crimea and destabilize Ukraine. By taking advantage of geographical proximity as well as past and present socio-economic relations, Russia is targeting the security of European countries.

If hybrid threats are to be countered effectively and efficiently, the applied tactics and means need to be analyzed first. Not every critical service or infrastructure can be protected; redundancy cannot be built everywhere, and many threats are impossible to anticipate. Hence, the conundrum of limited resources versus anticipated and unknown threats places great constraints on policymakers. The question is how to prepare, how to stay alert and ready to respond to those threats, which capabilities should be developed, where to invest, and how to ensure that areas critical for national and regional security become resilient.

This requires answering such questions as: What are the current security and defense challenges? What strategy did Russia use to seize Crimea and destabilize Ukraine? What is resilience in security context? What are NATO and EU responses to hybrid threats? What are their resilience priorities? The aim of the study is to substantiate the thesis that bolstering resilience is crucial for national and international security. The recent NATO summits discussed security environment and took a decision to strengthen common defense capabilities as well as civil preparedness, and to build resilience in areas critical for collective defense. Each country is responsible for strengthening resilience of its infrastructures and services, governance and defense. However, there are also cross-border infrastructures and services as well as transborder and transnational systems and interests which are vital at national, regional and global levels. In NATO, civil preparedness serves defense by facilitating military operations, primarily by enabling military mobility, which is a force multiplier (Jacuch, 2019a). Seven areas have been defined where resilience is necessary to support deterrence and collective defense. In turn, the EU has taken an approach to countering hybrid threats which involves building societal resilience, including strengthening cyber security and strategic communication. Both organizations cooperate in countering hybrid threats, building resilience, increasing military mobility, improving critical infrastructure protection, strengthening cyber security and strategic communication (Joint Declaration on EU-NATO Cooperation, 2018).

The article consists of six sections. The first one considers hybrid threats in general. The next section brings an assessment of current security environment, particularly focusing on the hybrid war in Ukraine. The third explores resilience in security context. The fourth examines NATO measures. The fifth explores EU decisions and structures related to countering hybrid threats. The sixth briefly presents NATO-EU cooperation. To be prepared for a crisis, including natural and man-made disasters (Jacuch, 2019 b), and to be able to respond to and recuperate after hybrid attacks, both organizations focus on civil preparedness and particularly on resilience requirements. The concluding remarks reiterate that "resilience" is NATO's and the EU's strategic response to hybrid threats.

The research process uses qualitative research methods as well as work experience, synthesis, abstracting, comparison, generalization and implication. The article analyzes the treaties, directives and regulations of the EU and NATO – the documents that form the basis for actions responding to hybrid threats, particularly societal resilience. Other sources are monographs, articles referring to an aspect of the investigated problem, and internet sources. Among them, the study carried out at the Center for Transatlantic Relations, Johns Hopkins University, *Forward Resilience: Protecting Society in an Interconnected World* (Hamilton, 2017) provides a comprehensive discussion on resilience, including concepts and definitions as well as an assessment of resilience efforts and future needs.

## 1. Hybrid threats

Carl von Clausewitz states in his treaty *On War*: "We see, therefore, that War is not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means. All beyond this which is strictly peculiar to War relates merely to the peculiar nature of the means which it uses" (2018). Sometimes these means are conventional, i.e. legal in the light of international humanitarian law such as the Geneva Conventions, and sometimes they are not. Hybrid war is quite variable in nature and may take more subtle forms, including information war, malicious cyber activities, sabotage, influencing enemy's economy, etc. Threats considered as particularly challenging are information operations and warfare in cyberspace. Hybrid concepts and strategies target vulnerabilities. The diversity of hybrid tactics masks the thoroughly planned order behind the spectrum of tools used and the effects being achieved (Thiele, 2016).

NATO describes hybrid threats as those which combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations ("NATO's response to hybrid threats", 2019).

The EU defines hybrid threats as those which 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. Hybrid threats can range from cyberattacks on critical information systems, through disruption of critical services such as energy supplies or financial services, to undermining public trust in government institutions or widening social divides ("A Europe that Protects", 2018; EU2019FI, 2019).

The Polish Bureau of National Security (*Biuro Bezpieczeństwa Narodowego*, BBN) defines hybrid war and introduces the term "subthreshold aggression". Hybrid war combines various possible means and methods of violence used concurrently, including regular and irregular armed actions, cyberspace operations and economic or psychological information campaigns. Subthreshold aggression is a method of warfare whose impetus and scale are deliberately limited and kept by the aggressor at a level below the recognizable threshold of regular, open war. The aim of subthreshold aggression is to achieve the goals set, while at the same time hindering international security organizations from obtaining decision-making consensus (Słownik BBN, n.d.).

The Warsaw University defines hybrid war as conducting warfare without an official declaration of war, combining elements of conventional war, cyberwarfare, terrorism, irregular actions (e.g. diversion) and other destructive actions (e.g. economic pressure), with the simultaneous use of propaganda actions ("New words", 2015).

## 2. Security environment

In 2014 the conflict in Eastern Ukraine, which is still ongoing (D'Anieri & Kuzio, 2019), drew attention to the challenges closer to the territory of the Alliance and the EU, and predominantly to the danger of hybrid threats. To counter new security threats which emerged from that conflict, NATO decided to strengthen significantly common defense capabilities as well as civil preparedness, concentrating in particular on increasing resilience in areas critical for NATO's collective defense.

The hybrid war in Ukraine has not been an unknown type of conflict, but in many respects different from previous ones (Bowen, 2019). Firstly, it was difficult to determine the opponent. Secondly, non-military as well as military instruments were used to a great extent (Piekarski, 2019). Moreover, the key role was played by propaganda and disinformation aimed at influencing both the attacked country and the international opinion. It is worth noting that Russian special forces took over the Crimean Peninsula without a fight mainly due to prior long-term information operations. Propaganda and disinformation, cyber attacks, the resulting low morale of Ukrainian forces and lack of military mobility were extensive and thus were the main reasons why Crimea was handed over to Russia without even a token resistance (Jacuch, 2019a). The UK-based defense contractor BAE Systems reported that in 2014, Ukraine computers were targeted by an aggressive "Snake" virus (Phys.org, 2014). Four malware groups believed to be linked to the Ukrainian conflict were identified. The cyber and information activities included Russian dominance of the Crimean news and information sources, erosion of Ukrainian government's credibility among the nation, and the resulting loss of trust in the authorities. There were economic effects such as loss of revenue and the costs of replacing infrastructure and equipment following cyberattacks on the Ukrainian power grid (Baezner, 2018).

Unlike a conventional war, the conflict in Ukraine mostly revolved around non-military activities such as propaganda and disinformation, cyber-attacks, provoking unrests on political grounds, destabilizing economy, applying financial pressure, spreading corruption and crime, sowing discord between ethnic groups, illegal border crossing and disinformation about the purpose of such actions, attacks on power grid 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 (Jacuch, 2019a).

In response to Russian hybrid warfare, in 2014 NATO adopted the Readiness Action Plan (RAP) as a means of responding rapidly to new threats as they present themselves along the eastern and southern flanks (NATO Wales Summit Declaration, 2014, para 5). The NATO Summits in Warsaw in 2016, Brussels in 2018 and London in 2019 continued to deal with challenges arising from various strategic directions, conventional and hybrid threats, terrorism, mass migration and proliferation of weapons of mass destruction, Russia's aggressive actions; state and non-state actors undermining the international order; instability triggering migration; and last but not least, cyber and hybrid threats (NATO London Declaration, 2019, para 3).

In response to the threats, NATO and the EU continue to increase social resilience (Bajarūnas, 2020). NATO priorities include critical infrastructure protection; energy security; communications (including 5G networks); and tools to respond to cyber attacks (NATO London Declaration, 2019, para 6). The Alliance keeps strengthening its ability to prepare for, deter and defend against hybrid tactics. In April 2016 the EU adopted its "Joint framework on countering hybrid threats – a European Union response" (JOIN(2016) 18 final). It outlined actions at 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 support for 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 (EU-NATO cooperation – Factsheet, 2019).

## 3. Resilience: responses to hybrid threats

Strengthening resilience has become a strategic task for the EU, NATO and their member states. To respond to hybrid threats in today's interconnected world with all the new technologies, the Internet, social media and artificial intelligence, we have to develop comprehensive security not only by increasing military capacity but first and foremost by enhancing civil preparedness in critical areas so as to enable monitoring, mitigation, recovering from, and countering potential hybrid attacks. This would require all the relevant actors – civil and military, public and private (including national and international companies), as well as academia – to be involved in this process, and this requires building trust between all participants.

NATO defines resilience as a society's ability to resist and recover quickly and easily from a major shock such as a natural disaster, failure of critical infrastructure, or hybrid or armed attacks; it requires both civil preparedness and military capacity. Robust resilience through civil preparedness in Allied countries are essential to NATO's collective security and defense ("Resilience and Article 3", 2020).

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 (COM(2012) 586 final, 2012). It stresses two resilience dimensions: the strength of an entity to resist stress and shock and the capacity to recover rapidly from the impact. Increasing resilience (and reducing vulnerability) can be achieved by enhancing the entity's strength, by reducing the intensity of the impact, or by a combination of both.

Numerous scholars, by applying different contexts (e.g. economy, psychology, ecology, etc.) provide various definitions of resilience and its systems. In the context of security, the Centre for Transatlantic Relations, Johns Hopkins University presented a comprehensive discussion on resilience and described its key operational features, i.e. physiology, morphology, and recipes. There are three core abilities a resilient system must have: 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 essence and vitality. The essence or core function of a resilient system would survive a shock, while supporting elements, though 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 the conditions allow it (Ries, 2016). There are four identified "focus areas" with potential to enhance resilience: identifying key vulnerabilities and associated risks; synchronizing cross-governmental decision making; building military sustainability and civil preparedness; and balancing the allocation of available (yet limited) resources (Thiele, 2016).

Countering hybrid threats requires 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 be targeted by hybrid attacks (Hagelstam & Narinen, 2018). Thus, strengthening resilience is a means of responding to hybrid threat as it helps avoid escalation of crises both within and outside of the EU and NATO (Wieslander, 2018). Another aspect of hybrid warfare is instrumentalization of international law, which has been extensively used by Russia during Crimea seizure and conflict in Donbas, and can be "countered by adopting a legal resilience perspective and by fostering an operational mindset" (Sari, 2020).

## 4. NATO: strengthening resilience

Resilience is not a new task for the Alliance. Article 3 of the North Atlantic Treaty says that "in order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack". Resilience was always understood to go beyond military capabilities. As early as the 1950s, NATO had in place policies and planning for civil preparedness, also called civil emergency planning (CEP).

During the Cold War, most critical civil assets, services and infrastructures were in government's hands. In a situation of crisis or war, there were mechanisms in place to allow NATO allies to control and use these assets. These mechanisms included NATO Civil Wartime Agencies, which were to deal with shipping management, land transport coordination, aviation, central supply, energy, and refugee organizations. By the late 1980s, the Alliance maintained plans for eight NATO Civil Wartime Agencies to be activated in times of crisis or war to coordinate and direct efforts ranging from allocation of industrial resources and oil supplies to food production, civil transportation, and management of refugee flows (Jacuch, 2017). These Agencies were put in dormant status and finally disbanded in the early 2000s; in general, civil preparedness planning, structures and capabilities had been reduced starting from the 1990s, both at national level and within NATO.

In 2000, the North Atlantic Council defined the five roles of NATO Civil Emergency Planning: (1) civil support for Alliance military operations under Article 5; (2) support for non-Article 5 crisis response operations; (3) support for national authorities in civil emergencies; (4) support for national authorities in the protection of the population against the effects of weapons of mass destruction; and (5) cooperation with partner nations (NATO Backgrounder, 2016). Today, these five roles still apply; however, considering the decisions taken at recent NATO summits, NATO's focus has shifted toward enhanced civil preparedness.

The CEP structures responsible for civil preparedness include Civil Emergency Planning Committee (CEPC), and Planning Groups covering 8 functional areas: transport with ocean shipping, inland surface transport and civil aviation; health; agriculture and food; industrial resources; communications services; and civil protection. Members of the Planning Groups are representatives of the relevant national ministries often reinforced by military representatives and civil experts.

The Planning Groups have formed and maintain their pools of international experts from different industries, academia and in some cases also from administration. They advise NATO and countries on civil preparedness-related issues. CEP experts play advisory and operational role at any stage of crisis management. They advise on the civilian aspects of crises and the effective use of civilian capabilities, support civil-military planning and the development of programs and concepts. The NATO experts contribute to development of resilience requirements, evaluation criteria, guidelines, measurements and assessments (Jacuch, 2017).

Another CEP mechanism is the Euro-Atlantic Disaster Response Coordination Centre, which is NATO's principal response mechanism in case of natural or man-made disasters or any CBRN (chemical, biological, radiological or nuclear) incident. It is active all year round, operational on a 24/7 basis, and involves NATO's Allies and all partner countries. The Centre functions as a clearing-house system for coordinating both requests from and offers of assistance for a stricken country (Jacuch, 2019b).

As from 2014, unpredictable security environment on the eastern and southern flanks has led to a renewed focus on civil preparedness. In times of crisis, population and civilian resources are exposed to external attack and internal disruption. Hybrid threats, including cyber threats, are also blurring the dividing lines of war and peace. Civilian preparedness means that in times of crisis or disaster the government can continue its core functions, and that basic services to the population as well as civilian support for military operations are ensured. It means civil sectors are prepared to support NATO military operations.

In response to the current threats, the Alliance has developed its capabilities, adapted its structures, and continues to build its readiness and resilience. It has increased its military presence on the eastern flank. Importantly, along with military reinforcement, NATO has been improving civil preparedness and building resilience in areas crucial for NATO's defense.

At the Warsaw Summit, NATO called not only for strengthening the military but also for improving civil preparedness, in particular by building resilience in areas of key importance for NATO's defense. The final declaration stated that "[c]ivil preparedness is a central pillar of Allies' resilience and a critical enabler for Alliance collective defence" (NATO Wales Summit, 2014, para 73). NATO has been improving civil preparedness in strategic sectors such as continuity of government, energy, essential services, security of critical civilian infrastructure, and support to military forces. The Alliance agreed on seven baseline requirements for national resilience:

> (1) assured continuity of government and critical government services: for instance the ability to make decisions, communicate them and enforce them in a crisis; (2) resilient energy supplies: back-up plans and power grids, internally and across borders; (3) ability to deal effectively with uncontrolled movement of people, and to de-conflict these movements from NATO's military deployments; (4) resilient food and water resources: ensuring these supplies are safe from disruption or sabotage; (5) ability to deal with mass

casualties: ensuring that civilian health systems can cope and that enough medical supplies are stocked and secure; (6) resilient civil communications systems: ensuring that telecommunications and cyber networks function even under crisis conditions, with enough back-up capacity; and (7) resilient transport systems: ensuring that NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis ("Resilience and Article 3", 2020).

To improve civil preparedness is national responsibility. The aim of these seven baseline requirements is to support countries in achieving the required resilience and to provide benchmarks, guidelines, methodology and measurements against which the state of civilian preparedness can be assessed. These resilience requirements apply to the entire crisis spectrum, from an evolving hybrid threat up to the most demanding scenarios. NATO has set up capabilities, such as resilience expert teams, that can support Allies in assessing their civil preparedness and (upon request) provide advice on enhancing it ("Resilience and Article 3", 2020). Civil preparedness/resilience-related questions have been included in the NATO Defence Planning Process.

NATO adopted a strategy of "prepare, deter and defend" to counter both conventional and hybrid threats based on the 360-degree principle. To improve situational awareness, NATO established its Joint Intelligence and Security Division, a capability to monitor and analyze hybrid threats ("NATO's response to hybrid threats", 2019).

New challenges require a full range of civil capabilities and active cooperation between public and private partners, government, private sector and academia. They also necessitate cooperation with partners and international bodies, particularly with the EU ("Resilience and Article 3", 2020). NATO and the EU have been cooperating on countering hybrid threats, with a special focus on enhancing resilience, improving military mobility, and countering cyber attacks and disinformation.

## 5. EU response to hybrid threats

The EU set up a new Civil Protection Mechanism (Decision No. 1313/2013/EU, 2013; C(2014)7489/F1, 2014). The Mechanism can be activated for any serious natural or man-made disaster (Jacuch, 2019b). In 2016 the EU adopted a joint framework to counter hybrid threats and foster resilience (JOIN(2016) 18 final), which outlined such actions as raising awareness of and building resilience in cybersecurity, critical infrastructures, protection of the financial system and of public health, as well as supporting efforts to counter violent extremism and radicalization. Further actions have been put forward to reinforce these efforts, including surveys of hybrid risks to identify key vulnerabilities and develop capacities for proactive strategic communication. It defined effective procedures for crisis prevention, response and recovery, and examined the applicability and practical implications of the Solidarity Clause[5] and the mutual Defence Clause[6] 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 Strategy provided for resilience (EUGS, 2016), which was translated into priorities and actions (JOIN(2017)21 final, 2017). The approach to resilience is aimed at strengthening the following: adaptability; the capacity of a state to build, maintain or restore its core functions; and 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 a part of the EU's wider response to hybrid threats (A Europe that Protects, 2018).

## 5.1. Cybersecurity

The 2013 EU cybersecurity strategy clarified roles and responsibilities and proposed specific activities including achieving cyber resilience; reducing cybercrime; developing the EU Cyber Defence Policy and capabilities in the framework of the Common Security and Defence Policy; developing the industrial and technological resources for the Digital Single Market; establishing an international cyberspace policy for the EU; and building capacity (JOIN/2013/01 final, 2013). The EU has updated its priorities for network and information security policy with the aim to develop capacity to cope with security challenges within the European Union Agency for Network and Information Security (ENISA) (Regulation (EU) 526/2013).

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

[6] 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.

Since then, the EU has adopted legislative proposals, secured investments 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 (COM(2016) 410 final, 2016). 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 EU (Directive (EU) 2016/1148, 2016). It defined 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. It 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 (JOIN(2017) 450 final, 2017). In 2018, a Network of Cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence Centre were proposed, having built on the expertise that has already existed in more than 660 cybersecurity expertise centers from all Member States. The Centres are also to ensure cybersecurity of 5G networks and develop measures which can be used to strengthen the EU's response to activities that harm its interests (Proposal for a European Cybersecurity, 2018).

The 2019 Cybersecurity Act (Regulation (EU) 2019/881, 2019) 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 Organisation and Digital Europe Organisation maintain the NIS Implementation Tracker, which presents the 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 ("NIS Implementation Tracker", 2019).

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

### 5.2. 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 ("Countering disinformation", 2019).

Since 2015, the EU has been implementing measures to address disinformation and to protect its democratic systems and public debates. To address Russia's disinformation campaigns, in March 2015 the EU set up the East StratCom Task Force ("Questions and Answers", 2018). It develops communication products and campaigns focused on explaining EU policies. It also reports on and analyses disinformation trends, explains and corrects disinformation narratives, and raises awareness of disinformation. To that aim, it produces the weekly Disinformation Review (EUvsDisinformation, n.d.).

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 (JOIN(2018) 16 final). 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 (JOIN(2018) 36 final, 2018). The plan includes a Rapid Alert System on Disinformation (RAS), which was set up among the EU institutions and Member States to facilitate sharing of insights related to disinformation campaigns and coordinate responses. The RAS is based on open-source information and will also draw upon insights from academia, fact-checkers, online platforms and international partners. In 2019 the EU Member States and the ENISA carried out a live test of their preparedness; a progress report on the fight against disinformation was published (JOIN(2019) 12 final, 2019).

## 6. The EU and NATO – cooperating to counter hybrid threats

In December 2015, NATO adopted its strategy on how to fight hybrid threats (Press statements, 2015) 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 (Yaniz, 2020). 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 resilience, security, and continuity of governance in the face of hybrid threats (EU-NATO cooperation, 2019). It also put in place cooperative working mechanisms at staff and senior levels (Council of the EU Press release, 2016). Until now, four progress reports highlighted the main achievements and added value of EU-NATO cooperation, including those related to countering hybrid threats (Fourth progress report, 2019). In 2018, NATO's North Atlantic Council and the EU's Peace and Security Committee held the discussion on hybrid threats with subsequent scenario-based exercises (Courtney, 2019).

Both NATO and the EU continue to build their shared capabilities to respond to hybrid threats. In 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 (Hybrid CoE, n.d.). In late 2018 NATO established Counter Hybrid Support Teams and other military advisory bodies (in the areas of cyber warfare, electronic warfare, and CBRN capabilities) to assist allies in the event of a hybrid crisis. In late 2019 the first Counter Hybrid Support team was deployed to Montenegro (NATO: Ready for the Future, 2019). NATO also established the Strategic Communications Centre of Excellence in Riga, Latvia; the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia; and the Energy Security Centre of Excellence in Vilnius, Lithuania ("Centres of Excellence", 2019).

## Concluding remarks

In his 2015 speech, NATO Secretary General Jens Stoltenberg, reiterated: “actually, I think the first hybrid warfare we know of might be the Trojan Horse, so we have seen it before, but the new thing is that it’s larger scale, it’s taking place close to our border, so we have to focus more on the concept of hybrid warfare. And that’s exactly what we are doing” (Zero-Sum, 2015).

Lessons learned from the conflict in Ukraine show that if territorial integrity is under hybrid aggression in any form, then in order to resist it, adequate civil preparedness is necessary, and political and military means have to be used at national and regional levels, including such crisis response measures as counter-aggression in information and cyber spaces. There has been a noticeable shift from the classic military confrontation to information and cyber warfare. In actuality, today’s societies are more connected – not only technologically but in practically all spheres of life. The information era, globalization and the Internet have brought new capabilities as well as new vulnerabilities.

NATO continues building readiness and resilience. It has increased its military presence in the eastern flank. Along with military reinforcement, the Alliance has been improving civil preparedness in areas that are critical for collective defense, particularly military mobility. Reducing dependency on commercial support by developing further arrangements to manage efficiently civil capabilities critical for deterrence and collective defense may improve support to military operations, enabling agile military mobility in time of crisis and/or war.

There are common threats as well as those faced by individual countries; thus, each country is responsible for strengthening resilience of its infrastructures and services, governance and defense. Resources are not unlimited, so not every entity can be sufficiently resilient. Hence, countries should assess vulnerabilities and exercise threat scenarios (known and unknown threats) and decide on priorities critical for national security and defense; the decision-makers may also consider which elements of the national system will have to be sacrificed as unaffordable if specific threats materialize and/or extend their impact. However, there are cross-border infrastructures and services as well as transborder and transnational systems and interests which are vital at national, NATO, EU, and global levels.

The previous sections discussed that the EU and NATO have further adapted their strategies, structures, regulations and other measures to counter hybrid threats. In NATO, civil preparedness enables functioning of national critical services and infrastructures, and facilitates military operations during a crisis or war. The EU focuses on responses to cyber threats and on countering disinformation and propaganda.

The Baltics, the Visegrád Group and the Balkan countries are particularly vulnerable to hybrid threats due to such factors as Russia's political objectives, geographical proximity and economic influence; Russian speaking minorities and/or economic migrants; and (possibly) cultural codes affected by Soviet dominance over these regions during the Cold War (Górnikiewicz, 2018). Hence – in addition to members' cooperation at NATO and/or EU – a regional, bilateral and/or multilateral cooperation between countries facing similar threats would allow synergizing their efforts to counter those threats.

As adaptive resilience makes it possible to resist and recover through civil preparedness from any kind of attack, kinetic and/or hybrid, it is a crucial security element. In a crisis, civil sectors must be prepared and ready to resist any shock, to recover quickly, to continue providing essential services to the population and government, and to support military operations. In today's globally interconnected world, information operations and cyber attacks are regularly used by aggressive and malicious state and non-state actors. What goes mostly unnoticed, such attacks often target the young population, who are digital citizens in social media and on the Internet.

To be prepared, protected and ready to respond to a crisis requires cooperation and involvement of all relevant actors, including partners and international bodies, key private industry players and representatives of academia. Awareness, resilience and response are indispensable for countering hybrid threats. Both NATO and the EU have been improving its capacity to detect and understand malicious activities at an early stage; enhancing the resilience of critical infrastructure, societies and institutions. Mechanisms are in place which allow NATO and the EU to work together, particularly at the staff level. Nevertheless, there is a room for enhancement of the cooperation of both organizations and for building synergy further in countering hybrid threats. Comprehensive approach to resilience is necessary; however, working together requires trust among all involved parties.

## REFERENCES

A Europe that Protects: Countering Hybrid Threats. (2018, 13 Jun). EEAS. Brussels. Retrieved from https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en

Baezner, M. (2018). Cyber and Information warfare in the Ukrainian conflict. Centre for Security Studies (CSS), ETH Zürich.

Bajarūnas, E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*, *19*(1), 62–70. DOI: https://doi.org/10.1177/1781685820912041

Bowen, A. S. (2019). Coercive diplomacy and the Donbas: Explaining Russian strategy in Eastern Ukraine. *Journal of Strategic Studies*, *42*(3–4), 312–343. DOI: https://doi.org/10.1080/01402390.2017.1413550

C(2014)7489/F1. (2014). 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.

Centres of Excellence. (2019, Jan 24). NATO website. Retrieved from https://www.nato.int/cps/en/natohq/topics_68372.htm

Clausewitz, C. von. (1918). On War (J. J. Graham, Trans.). London: Kegan Paul, Trench, Trubner & Co. Retrieved from https://oll.libertyfund.org/titles/clausewitz-on-war-vol-1#lf1380-01_label_056

COM(2012) 586 final. (2012, 3 Oct). Communication from the Commission to the European Parliament and the Council, The EU Approach to Resilience: Learning from Food Security Crises.

COM(2016) 410 final. (2016, 5 Jul). 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.

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

Countering disinformation. (2019, 11 Mar). EEAS. Retrieved from https://eeas.europa.eu/topics/countering-disinformation/59411/countering-disinformation_en

Courtey, C. K. (2019). Working with NATO to Address Hybrid Threats. *The Foreign Service Journal AFSA*. Retrieved from https://www.afsa.org/working-nato-address-hybrid-threats

D'Anieri, P., & Kuzio, T. (2019). Ukraine after five years of conflict. *Eurasian Geography and Economics*, *60*(1), 1–5. DOI: https://doi.org/10.1080/15387216.2019.1635512

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. (2016). L 194/1.

EU2019FI. (2019). Common action to counter hybrid threats. Finland's Presidency of the Council of the European Union. Retrieved from https://eu2019.fi/en/backgrounders/hybrid-threats

EUGS 2016. (2016). The European Union Global Strategy for the Foreign and Security policy. Retrieved from https://eeas.europa.eu/topics/eu-global-strategy/17304/global-strategy-european-unions-foreign-and-security-policy_en

EU-NATO cooperation – Factsheet. (2019, 11 Jun). EEAS. Brussels. Retrieved from https://eeas.europa.eu/headquarters/headQuarters-homepage/28286/eu-nato-cooperation-factsheets_en

EUvsDisinformation [webpage]. (n.d). Retrieved from https://euvsdisinfo.eu/

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, 17 Jun). Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

Górnikiewicz, M. A. (2018). *Prognozowanie Kulturowe Zagrożeń Bezpieczeństwa Narodowego i Międzynarodowego*. Warszawa: WAT.

Hagelstam, A., & Narinen, K. (2018, 23 Nov). Cooperating to counter hybrid threats. *NATO Review Magazine*. Retrieved from https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

Hamilton, D. S. (Ed.). (2017). *Forward Resilience: Protecting Society in an Interconnected World*. Washington, DC: Center for Transatlantic Relations.

Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats. (2019). Council of the European Union. Retrieved from https://data.consilium.europa.eu/doc/document/ST-10027-2019-INIT/en/pdf

Hybrid CoE. (n.d.). The European Centre of Excellence for Countering Hybrid Threats. Retrieved from https://www.hybridcoe.fi/what-is-hybridcoe.

Ismay, H. L. (1957). Lord Ismay's Report to the Ministerial Meeting of the North Atlantic Council in Bonn, (APRIL 1952 – APRIL 1957). Retrieved from http://archives.nato.int/nato-april-1952-april-1957-text-of-lord-ismays-report-to-ministerial-meeting-of-north-atlantic-council-in-bonn-may-1957

Jacuch, A. (2017). Civil Preparedness – NATO Civil Experts Capability. *Defence Science Review*, *3*, 135–143.

Jacuch, A. (2018). Odpowiedź NATO na wyzwania i zagrożenia bezpieczeństwa i obronności w XXI wieku. Strategia NATO. Cywilne przygotowania obronne. In Z. Trejnis (Ed.), *Wyzwania i zagrożenia bezpieczeństwa i obronności RP w XXI wieku* (pp. 205–229). Warszawa: Wydawnictwo Aspra.

Jacuch, A. (2019a). Civil Preparedness – Military Mobility. In M. Banasik (Ed.), *Security and Russian Threats* (pp. 231–245), Kielce: The Jan Kochanowski University.

Jacuch, A. (2019b). Disaster response mechanisms inn EU and NATO. *Przegląd Europejski*, *3*(53), 67–81.

JOIN/2013/01 final. (2013). 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 (2016) 18 final. (2016). Joint communication to the European Parliament and the Council: "Joint Framework on countering hybrid threats – a European Union response".

JOIN (2017) 450 final. (2017). 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) 21 final. (2017). Joint Communication to The European Parliament and The Council, Brussels, A Strategic Approach to Resilience in the EU's external action.

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

JOIN (2018) 36 final. (2018). 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 (2019) 12 final. (2019). 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.

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. (2018, 10 Jul).

NATO Backgrounder. (2016). NATO's Role in Civil Emergency Planning. Retrieved from https://www.igsu.ro/documente/SAEARI/NATO_CEP.pdf

NATO Brussels Summit Declaration. (2018, 11 Jul). Available at https://www.nato.int/cps/en/natohq/official_texts_156624.htm

NATO London Summit Declaration. (2019, 4 Dec). Available at https://www.nato.int/cps/en/natohq/official_texts_171584.htm

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

NATO Wales Summit Declaration. (2014, 5 Sep). Available at https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO Warsaw Summit Communiqué. (2016, 9 Jul). Available at https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO's response to hybrid threats. (2019, 8 Aug). NATO Website. Retrieved from https://www.nato.int/cps/en/natohq/topics_156338.htm

New words. (2015). Wojna hybrydowa. Warsaw University. Retrieved from http://nowe-wyrazy.uw.edu.pl/haslo/wojna-hybrydowa.html?pdf=1

NIS Implementation Tracker. (2019, 22 Mar). Retrieved from https://www.digitaleurope.org/resources/nis-implementation-tracker/

Phys.org. (2014). Ukraine's computers 'targeted by powerful virus': experts, News and Articles on Science and Technology. Retrieved from https://phys.org/news/2014-03-ukraine-powerful-virus-experts.html

Piekarski, M. (2019). Polish Armed Forces and hybrid war: Current and required capabilities. *The Copernicus Journal of Political Studies*, *1/2019*, 43–64. DOI: http://dx.doi.org/10.12775/CJPS.2019.003

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

Proposal for a European Cybersecurity Competence Network and Centre. (2018). EEAS. Retrieved from https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

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

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.

Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No. 460/2004.

Resilience and Article 3. (2020, 31 Mar). Retrieved from https://www.nato.int/cps/en/natohq/topics_132722.htm

Ries, T. (2016). Forward Resilience in Context. In D. S. Hamilton (Ed.), *Forward Resilience, Protecting Society in an Interconnected World* (pp. 1–16). Washington, DC: Center for Transatlantic Relations.

Sari, A. (2020). Legal resilience in an era of grey zone conflicts and hybrid threats. *Journal Cambridge Review of International Affairs*, *19*(1), 62–70. DOI: https://doi.org/10.1080/09557571.2020.1752147

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

Thiele, R. D. (2016). Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective. *ISPSW Strategy Series: Focus on Defense and International Security*, *449*, 1–8.

Wieslander, A. (2016). How NATO and the EU can Cooperate to Increase Partner Resilience. In D. S. Hamilton (Ed.), *Forward Resilience, Protecting Society in an Interconnected World* (pp. 137–148). Washington, DC: Center for Transatlantic Relations.

Yaniz, F. (2020). NATO-EU Cooperation: Milestones and challenges ahead. In J. M. Ramírez & J. Biziewski (Eds.), *Security and Defence in Europe* (pp. 217–231). New York, NY: Springer International Publishing.

Zero-Sum? Russia, Power Politics, and the post-Cold War Era. (2015). Session at the Brussels Forum with participation of NATO Secretary General Jens Stoltenberg. Retrieved from https://www.nato.int/cps/en/natohq/opinions_118347.htm?selectedLocale=en