Executive summary

The EU, NATO and the Eastern Partnership countries are facing a range of security challenges and risks. Hybrid threats are a permanent feature of today's security environment and a part of the current EU, NATO, and the Eastern Partnership countries security landscape. In a period of rapid changes in the security environment and external pressures, it is important to intensify cooperation between the EU, NATO, and the Eastern Partnership countries and to make further progress on common collaborative approaches against hybrid threats. The paper focuses on different areas of the EU-NATO cooperation against hybrid threats and argues that shared resilience against shared threats can lead to a better synchronization of efforts in countering hybrid threats. A case study on the Eastern Partnership countries is introduced in this research and is examined in the paper.

Key research questions:

- How do you see the complementarity of the EU-NATO approach in tackling hybrid warfare in the Eastern Partnership countries?
- What steps should be undertaken by the EU and NATO to strengthen their shared capacity of action against Russia's hybrid warfare tactics?

Key findings:

- Shared resilience against shared threats is a driving force for an adaptation towards security risk reduction and one of the comprehensive mechanisms for a strong institutional cooperation between the EU and NATO.
- Looking at NATO's 2030 adaptation and the EU's growing geopolitical ambitions, a further partnership between the EU and NATO can only strengthen the EU-NATO understanding of security threats and can lead to a better responsiveness.
- Inspired by NATO's commitments for seven so-called baseline requirements, the EU has set up the EU resilience baselines to improve the preparedness, protection, and recovery of critical sectors from hybrid threats. A further knowledge transfer between the two organizations and a shared awareness and assessment of joint vulnerabilities and security risks will contribute towards the deterrence against hybrid threats.
- The EU and NATO are committed to strengthening the resilience of the Eastern partnership countries through the European Neighborhood Policy toolkit and NATO's 'Projecting Stability' activities. Creating a better synergy between those mechanisms, tools and financial instruments will further foster security in the Eastern neighborhood.

- With regard to countering hybrid threats in the Eastern Partnership region, the EU-NATO tools and instruments combine situational awareness, information sharing, training and exercises, confidence-building measures, building interoperability for operational purposes, security capacity-building and reassurance instruments, and reinforcement of common institutional cooperation. A better synchronization of common efforts in the detection, prevention, and response to hybrid activities in the Eastern Partnership region and the complementary nature of the EU-NATO means will foster resilience of the Eastern partners. A transfer of NATO's resilience guidelines knowledge from NATO member states to the Eastern Partnership countries will improve synergies between institutions and the Eastern Partnership countries.
- Further outreach to the like-minded community of partners and a tailored communication and outreach campaigns to different audiences such as the private sector, local authorities, civilian and military actors, or the intelligence community can help to form a better public awareness of hybrid threats in the Eastern Partnership countries.
- Improving institutional governance and the capacity building of local communities, intelligence services, armed forces and anti-corruption authorities are crucial in the Eastern Partnership countries to enhance social resilience.
- Further differentiating between partners with signed Association agreements and upgrading the Eastern Partnership policy with security instruments will be necessary to make the EU a more assertive geopolitical and security player in the Eastern neighborhood.

Shared resilience against shared threats: EU-NATO and the Eastern partners[1]

In a period of geopolitical shocks, intensifying competition, regional shifts, external pressures, and rapid changes in the security environment, it is important to pay attention to instability drivers and threats that can affect the EU and NATO and their partners.

The existence of hybrid threats is recognized by the EU, NATO, and their partners. These threats undermine governance, leverage indirect forms of power, erode trust in government institutions, create systemic vulnerabilities and societal polarization and affect decision-making processes.

The EU Security Union Strategy adopted in July 2020 and the NATO reflection report "NATO 2030: United for a New Era" published in November 2020 acknowledge the destabilizing nature of hybrid threats and their evolving nature. The EU and NATO also recognize the importance of further cooperation and coalitions between nations and partners in countering hybrid threats and they stress the need for a reinforcement of links between Allies and partners to make further progress on common collaborative approaches and policy toolkits against hybrid threats.

From the EU and NATO perspective, shared resilience, the identification of key vulnerabilities and a shared risk assessment demand a synchronization of efforts between partners, member states, civil and private sectors, and the EU-NATO institutions to contribute towards the deterrence against hybrid threats. As a first line of defense, shared resilience requires a shared understanding of security threats as well as a shared awareness and assessment of joint vulnerabilities and security risks. It also demands flexibility, institutional adaptability, responsiveness, strong leadership and cooperation, knowledge transfer and a rapid, agile, and efficient decision-making process.

Considering that hybrid threats may be directed at an adversary's vulnerabilities across the full spectrum of diplomatic, informational, military, economic and financial, intelligence and legal

[1] Research paper is written by Dr. Vira Ratsiborynska (Sciences Po), Adjunct Professor on NATO and transatlantic approaches to security and Global politics, Vrije Universiteit Brussel (VUB), Brussels, Belgium.

dimensions, the tripartite EU-NATO-partners cooperation itself would help to reinforce political legitimacy within state boundaries and to create resilience against malign influence.

This paper will elaborate on effective EU-NATO collaborative approaches against hybrid threats and will present a case study of the Eastern Partnership countries. The Eastern Partnership countries (EaP)[2] constitute a focal point for Russia's power projection spectrum as grey areas that the Kremlin will use in its hybrid activities against European countries.[3] The Eastern Partnership region as a whole can be considered by the defence community as a contested area of influence between Russia and the West which requires thorough attention from the different international players, in particular the European Union (EU) and North Atlantic Treaty Organization (NATO).

One of the EU-NATO objectives or the strategy to counter hybrid threats in wider Europe and the Eastern Partnership region itself can be resilience. The research work presented here includes recommendations on how to diminish the hybrid security risks in Europe through models of EU-NATO security cooperation and an enhancement of resilience against hybrid threats in the Eastern Partnership region. Particular attention should be devoted to a strategy of minimizing security risks from Russia's hybrid threats to Europe itself; to the strengthening of Euro-Atlantic cooperation and to developing the EU-EaP-NATO cooperation focusing on strengthening the region's societal resistance and operational resilience against Russia's hybrid warfare tactics and on facilitating peace solutions. To better counter Russia's hybrid threats and to achieve greater stability of the Eastern Partnership region, an optimal balance of military deterrence, non-military measures, and cooperative tools is required.

Resilience from the EU's and NATO's perspectives: From declaration to action

Resilience has become a central concept of EU and NATO security policies since 2016. Such important strategic documents as the Global Strategy for the European Union's Foreign and Security Policy (2016), the Joint Framework on countering hybrid threats (2016), the Joint

[2] The Eastern Partnership program is the EU's initiative to improve its political and economic relations with the post-Soviet states of Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. EU-Eastern Partnership countries relations were to be promoted through trade and economic agreements such as the Association agreement, but also through democratic institution-building and multilevel cooperation between the EU and the Eastern Partnership countries.

[3] Research paper is limited to Russia's hybrid activities in the Eastern neighborhood, no reference to Chinese hybrid activities in the Eastern neighborhood.

Warsaw Summit communiqué (2016), the Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (2018) as well as the NATO 2030 Expert Group's Report "United for a New Era" from 2020 refer extensively to the concept of resilience.

Resilience is defined by the EU as "the ability of an individual, a household, a community, a country or a region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development".[4] In many NATO documents, resilience refers to a "combination of civil preparedness and military capacity" where civil preparedness is described as "all measures and means taken in peacetime, by national and Allied agencies, to enable a nation to survive an enemy attack and to contribute more effectively to the common war effort".[5] NATO documents also state that resilience "can be measured by the ability to retain credible forces and conduct successful operations in spite of surprise or strategic shock".[6]

In 2016 the Heads of State and Government of NATO countries at the Warsaw Summit made an explicit commitment to enhance resilience. The members of the Alliance agreed on commitments for seven so-called baseline requirements that reflect the nations' view on resilience. The seven baseline requirements are the "assured continuity of government and critical government services; resilient energy supplies; ability to deal effectively with uncontrolled movement of people; resilient food and water resources; ability to deal with mass casualties; resilient civil communications systems and resilient civil transportation systems".[7] The progress achieved in meeting these resilience commitments is supported by NATO's Resilience Advisory Support Teams that help the countries in building this requirement.[8]

Furthermore, a principle of resilience is embedded in article 3 of the Washington Treaty that requires all NATO Member States to "maintain and develop their individual and collective

[4] European Commission, "Building resilience: The EU's approach", Factsheet, 2016, available here: https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf
[5] Civil-military cooperation center of excellence, "Resilience through civil preparedness", Haque, 2017, available here: https://www.cimic-coe.org/resources/fact-sheets/resilience-through-civil-preparedness.pdf
[6] NATO, SACT, Framework for Future Alliance Operations, August 2015, pp.19-20, available here: https://www.act.nato.int/images/stories/media/doclibrary/ffao-2015.pdf
[7] North Atlantic Treaty Organization, Commitment to enhance resilience issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016, available here: https://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en
[8] Allied Command Transformation, Building resilience. Collaborative proposals to help nations and partners, June 2017.

capacity to resist armed attack".[9] According to the reflection report "NATO 2030: United for a New Era", "building resilience across Allied populations is the primary responsibility of Allies themselves" and NATO pays a supportive role and " could offer a surge capacity to individual countries whose capabilities may be overwhelmed by e.g. a terrorist attack involving non-conventional means including chemical, biological, or radiological substances".[10] The NATO Allies are maintaining civilian preparedness as a blueprint for collective defense. Nations are constantly intensifying civil-military cooperation which is essential for addressing any crisis and are adapting their deterrence and defense posture to ensure readiness and to respond to security challenges. Within collective defense, crisis management and cooperative security (NATO's three core tasks) resilience is an underlying condition 'for a robust defensive posture". Resilience is an enabler "for an appropriate engagement of multiple challenges" before any crisis occurs (crisis management) and a "support development of partners' resilience" (cooperative security).[11]

Looking at resilience and the common EU-NATO approaches to resilience and countering hybrid threats, resilience requires "preparation, prevention, protection, promotion and transformation policies", as well as an involvement of institutions and citizens.[12]

After the EU and NATO have analyzed an institutional imperative to build up resilience against hybrid threats, at the Warsaw Summit in 2016 they agreed on the Joint Declaration. This included the identification of more than forty proposals in seven areas of cooperation such as hybrid threats, operational cooperation including maritime issues, cyber security, defense capabilities, industry and research, capacity building and exercises.[13] The 2018 EU-NATO Joint Declaration then stated that the EU and NATO had "increased[..]ability to respond to hybrid threats" and common institutional work was conducted on reinforcement of

[9] North Atlantic Treaty Organization, the North Atlantic Treaty, Washington, April 1949, available here: https://www.nato.int/cps/en/natolive/official_texts_17120.htm
[10] NATO 2030: United for a new era, Analysis and recommendations of the reflection group appointed by the NATO Secretary General, November 2020, available here: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf
[11] NATO, "Building resilience across the Alliance", HQ SACT, pp.5, January 2016
[12] European Commission, JRC, Building a scientific narrative towards a more resilient EU society, 2017, available here: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC106265/jrc106265_100417_resilience_scienceforpolicyreport.pdf
[13] Council of the European Union, EU-NATO Joint Declaration, 8 July 2016, available here: https://www.consilium.europa.eu/en/press/press-releases/2016/07/08/eu-nato-joint-declaration/
And Council of the European Union, Infographic-EU-NATO Joint Declaration, available here: https://www.consilium.europa.eu/en/infographics/eu-nato-joint-declaration/

preparedness for crisis and resilience, disinformation and cyber security.[14] Parallel and coordinated exercises (PACE) between the two organizations with the participation of NATO and EU Member States have been taking place every two years since 2016.[15] The exercises also identify lessons to support partners in security and defense capacity-building.[16] Based on the outcome of these exercises, a methodological revision of the EU operational protocol for countering hybrid threats (EU Playbook) was conducted.[17]

Since 2016 the Member States have agreed to monitor security risks related to hybrid threats and "identify indicators of hybrid threats, incorporate these into early warning and existing risk assessment mechanisms, and share them as appropriate".[18] Special emphasis was given to the improvement of situational awareness and enhancement of a comprehensive approach on hybrid threats between the different organizations and bodies. The "EU playbooks" have outlined cooperation with partner organizations as necessary to improve information sharing and enhance situational awareness. A Joint staff document from 2019 has reported on progress achieved in countering hybrid threats and resiliency aspects. These aspects include an allocation of additional funds to a network of practitioners handling hybrid threats, the development of hybrid threat-related indicators and vulnerability indicators for the resilience and protection of critical infrastructure, the work in progress for identifying new mechanisms on the EU Foreign Direct Investments Screening Regulation, a further development of the Rapid Alert System to fight against disinformation and election interference.[19]

Some tangible progress has been achieved by the EEAS Task Forces (East, Western Balkans, South) who are working on the monitoring of disinformation, the enhancement of citizens'

[14] Council of the European Union, EU-NATO Joint Declaration, 10 July 2018, available here: https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[15] Ibid.
[16] EU and NATO, Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, 16 June 2020, available here: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf
[17] European Commission, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, May 2019, Brussels, p. 23.
[18] European Commission, "Joint Framework on countering hybrid threats", Brussels, 6 April 2016, paragraph 2, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
[19] European Commission, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, May 2019, Brussels, available here: report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf (europa.eu)

awareness and media literacy campaigns etc.[20] The EU is also building up societal resilience against disinformation through the EU's strategic communication campaigns "InvestEU" (a Europe that delivers), "EUandME" (a Europe that empowers) and "EU Protects" (a Europe that protects).[21] The EU is also in process of implementing new initiatives that were incorporated in July 2020 EU Security Union Strategy. Such initiatives include a "set up of the EU resilience baselines to improve the preparedness, protection and recovery of critical sectors from hybrid attacks".[22] This initiative is important as the EU resilience baselines can provide a model for strengthening national resilience of the Member States.[23]

Reflecting upon the future of NATO in 2030, the reflection group appointed by the NATO Sec Gen has advanced a proposal for the establishment of a Centre of Excellence for Democratic Resilience dedicated to providing support to individual Allies, upon their request, for strengthening societal resilience to resist interference from hostile external actors in the functioning of their democratic institutions and processes".[24]

In terms of energy security and vulnerabilities in the energy sector, a diversification of energy supplies and an engagement of the Member States on the development of the Southern Gas Corridor, East Med Gas and US's LNG imports to Europe constitute a top priority for the EU and NATO communities. The EU institutions are also investing in the protection of critical infrastructure and have funded different projects through Horizon 2020 such as DEFENDER and SECUREGAS.[25] Furthermore, the "European Program for Critical Infrastructure Protection" also covers the protection of civilian infrastructure like airports and ports. The EU Space Programme as Copernicus "provides situational awareness through satellite images" which contributes to the situational awareness of the Member States with regard to the protection and monitoring of critical infrastructure.[26] NATO is focusing on the operational side of energy risk identification and assessment, the enhancement of the protection of critical

[20] Ibid.
[21] Ibid.
[22] European Parliament, SEDE-INGE Joint meeting, 25 February 2021, available online: https://multimedia.europarl.europa.eu/en/sede-inge-joint-meeting_20210225-1030-COMMITTEE-SEDE-INGE_vd
[23] Ibid.
[24] NATO 2030: United for a new era, Analysis and recommendations of the reflection group appointed by the NATO Secretary General, November 2020, available here: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf
[25] Ibid, p.7.
[26] Ibid, p.10

energy infrastructures and the reduction of energy vulnerabilities.[27]

In cyber security there is an ongoing cooperation of the Computer Emergency Response Team for the EU (CERT-EU) that shares threat assessment memos on the topics of the cyber, energy or digital domains with the national Computer Security Incidents Response Teams and the Computer Incident Response Capability of the North Atlantic Treaty Organization (NCIRC). The EU institutions are massively investing into different pilot projects on cyber security under Horizon 2020 and are also addressing cyber defense education through the Cyber Education, Training, Exercises and Evaluation platform. Cyber Europe 2018 and Cyber Coalition 2019 events between the North Atlantic Treaty Organization's staff and EU staff also have largely contributed to strengthening the capacity of Member States to deal with hybrid threats in the cyber domain.

Moreover, an ongoing close cooperation between the European Center of Excellence for countering hybrid threats and NATO Centers of Excellence, the Hybrid Fusion Cell of the EU intelligence and situation center and the NATO Hybrid Analysis branch provide Member States with additional platforms for sharing best practices and enhancing shared efforts in dealing with hybrid activities. The countries are constantly addressing hybrid threats through DIMEFIL[28] and are paying attention to the identification of "areas of interests or critical functions that a state should ensure are resilient against hybrid threat activity".[29]

This constant work in progress and the success of the EU and NATO in achieving resilience to and capacities to deal with hybrid threats rely not only on the resilience of their Member States but also on their partners, i.e., the Eastern Partnership countries, who deal with a wide spectrum of hybrid threats on a daily basis.[30]

Case study on the Eastern Partnership region and the evolution of hybrid threats

As recent events in the Eastern Partnership region demonstrate, Russia's hybrid warfare is constantly evolving and adapting. These events include the evolution of Russia's cyber security

[27] V. Ratsiborynska, "Russia's hybrid warfare in the form of its energy maneuvers against Europe: how the EU and NATO can respond together?", NATO Defense College, 2018

[28] Spectrum of specific powers such as Diplomatic, Information, Military, Economic, Finance, Intelligence, and Law Enforcement.

[29] European Commission, Hybrid CoE, The Landscape of hybrid threats: A conceptual model public version, November 2020, available here: https://www.hybridcoe.fi/wp-content/uploads/2021/02/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf

[30] NATO, "Building resilience across the Alliance", HQ SACT, January 2016

activities against Europe and the Eastern Partnership countries, the build-up of military bastions inside the territories of the Eastern Partnership countries, the development of anti-access area denial capabilities and information warfare with increasingly influential content. Russia is also intensifying its military presence in the Eastern neighborhood while exerting external pressure on the EU and the international community.

As of the end of 2020, a Russian presence has been identified in all six Eastern Partnership countries.[31] In 2020 Russia demonstrated its ability to assert its military posture in the conflict between Armenia and Azerbaijan and presented itself as one of the successful and credible security guarantors and mediators in the conflict between these parties.[32] Russia has also deepened its military ties with Belarus by conducting several military exercises with Belarus in 2020 and also re-emphasized its discourse towards a bigger integration in the military domain.[33] All these moves are accompanied with an economic and political acceleration towards a completion of the Union State integration.[34]

In the Eastern part of Ukraine Russia pursues its low-cost asymmetrical approaches and at the same time devotes a significant attention to the militarization and nuclearization of the occupied Crimean Peninsula and to the modernization of the Black Sea Fleet.[35] Furthermore, the Kremlin focuses on the Black Sea region as a maritime logistics, trade and energy hub that connects Russia's Southern and Western areas of interest. The littoral states that belong to the Eastern Partnership regional framework i.e., Ukraine and Georgia as well as those that are located nearby i.e., Armenia, Azerbaijan, Moldova, and Belarus are of vital importance for Russia's security, energy, and trade interests. Russia is also striving to achieve its national

---

[31] V. Ratsiborynska, "When Hybrid Warfare supports ideology: Russia Today", *NATO Defense College*, Rome, 2016

[32] N. Melvin, When the chips are down: Russia's stance in the current Azeri-Armenian confrontation, RUSI, October 2020, available here: https://rusi.org/commentary/when-chips-are-down-russias-stance-current-azeriarmenian-confrontation?utm_source=RUSI+Newsletter&utm_campaign=b605f43c71-EMAIL_CAMPAIGN_2020_09_10_09_43_COPY_01&utm_medium=email&utm_term=0_0c9bbb5ef0-b605f43c71-47838786

[33] VPK, "The unification of Russia and Belarus will begin with the creation of a single army", September 2020, available here: https://www.ng.ru/armies/2020-09-13/2_7962_army.html

[34] Ibid.

[35] Foreign intelligence service of Ukraine, White Book 2021, January 2021, available here: https://szru.gov.ua/download/white-book/WB-2021.pdf
And UNIAN, Russia deploys Bastion coastal defense missile system in Crimea, January 2021, available here: https://www.kyivpost.com/ukraine-politics/unian-russia-deploys-bastion-coastal-defense-missile-system-in-crimea.html?cn-reloaded=1

strategic security objectives in the energy domain which are aimed at controlling energy export routes to the EU. Moscow is seeking to finalize its vital energy project Nord Stream 2 that undermines national interests of Ukraine and also puts Europe at a security risk.

All these Russian actions demonstrate to the international community that the Eastern Partnership region represents one of Russia's regional areas of interest where it executes its power projection role and where a high spectrum of military and non-military means as well as new capabilities across multiple domains are simultaneously applied. Russia's actions and its creation of grey zones in the Eastern neighborhood prevent the Eastern Partnership countries from accession to NATO and significantly minimize their ability to absorb European norms and values.

Figure 1: Territorial conflicts in the Eastern periphery of the European Union[36]

[36] S. Pugsley and F. Wesslau (eds.), Life in the Grey Zones – Reports from Europe's breakaway regions, European Council for Foreign Relations, original map, adapted by the author.

Evolution of Russian future strategic thinking and hybrid threats

In different publications the Chief of the General Staff of the Armed Forces of Russia Valery Gerasimov has stated that the successful execution of hybrid warfare requires modernized and upgraded military capabilities combined with non-military means. General Gerasimov writes that "work on the question of preparation of information and conduct of actions of information character is the most important task of military science".[37] In the current military discourse Moscow prioritizes principles of interconnectivity between military and non-military methods while paying attention to "traditional environments as land, sea, air, space and cyberspace, but also to new ones such as social, digital, energy and others".[38] Moreover, Russia's strategy of limited actions in the execution of hybrid activities abroad is directed towards a more inclusive approach which aims at integrating non-military tools with C4ISR[39], digital technologies, robotics, unmanned systems, and electronic warfare under the control of the Russian National Defense Management Center.[40] Moscow is continuously improving its military capabilities by shaping its forces into expeditionary forces based on a coalition of partners. Expeditionary warfare and coalition-based hybrid warfare have become a part of the military adaptation of Russian forces in its future strategic thinking.

Domestically, the Russian Federation has begun making changes in its defense organization and the National Guard has been created to counter "the trend of military dangers and threats shifting into the informational space and domestic sphere of Russia".[41] President Vladimir Putin has stated numerous times that Russia will take all necessary actions to improve the potential of its strategic nuclear forces, to consolidate its military forces, to strengthen its abilities to "adequately respond" to a potential technologically advanced state-level adversary.

As demonstrated, Russia's strategy and its policymaking regarding the use of its hybrid warfare tools and methods are progressing towards a more deterrent approach that successfully

[37] V. Gerasimov, Vektory Razvitiya Voennoi Strategii, Krasnaja Zvezda, March 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/
[38] Arms expo, "Alexander Smolovy: "Generator of breakthrough ideas and proposals", January 2021, https://www.arms-expo.ru/news/novye-razrabotki/aleksandr-smolovoy-generator-proryvnykh-idey-i-predlozheniy/?mc_cid=d7f9ed37f6&mc_eid=fed21c605f
[39] C4ISR, acronym stands for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.
[40] Andrew Monaghan, Dealing with the Russians, 2019, p.p.121.
[41] RSInsights, Moscow's Strategy of limited actions", 28 January 2021

combines different hybrid warfare tactics causing uncertainty and unpredictability in an international security environment. A synergy between conventional and unconventional means as well as Russia's strategy of limited actions that "defend and promote national interests" outside of Moscow's borders also provides a sophisticated basis for a modern development of Russia's current and future paradigm of modern warfare.[42] Since uncertainty, unpredictability and strategic surprises prevail in Russia's actions in the Eastern Partnership region, security challenges and risks remain critical points of the EaP-EU-NATO cooperation.

The Kremlin's hybrid warfare and its dynamic character represent a serious challenge to the international order and are undermining the EU's security. Russia's bastion strategy and the cyber security and military trends that Moscow is developing in its hybrid warfare strategy against the Eastern Partnership region show that these questions urgently need to be studied and analyzed to be able to elaborate an efficient counterstrategy and to develop possible prospects of conflict resolution in the region.

Resilience has become one of the means to address hybrid threats and to strengthen the institutional capacities of the Eastern Partnership region's governments to deal with a wide range of hybrid threats. Moreover, resilience can become a driving force for an adaptation towards security risk reduction and one of the comprehensive mechanisms for a strong institutional cooperation or for sharing best practices on questions of hybrid threats and security risk assessment between the Eastern Partnership countries, the EU, NATO, and their Member States. Shared resilience is the core element of a first line of defense.

Shared resilience is a driving force for adaptation and a base of defense that helps to identify a threat, allows to come out with a proactive approach and limits the impacts of hybrid threats in such a way that the EU, NATO and the Eastern Partnership countries become powerful enough to respond in a coordinated and comprehensive way. In the best case, resilience is already preventing such attacks and forms part of the deterrence by denial which intends to convince the adversary "that an attack will not achieve its intended objectives".[43] The main components of operational resilience should include agile and adaptable military forces reinforced by all

[42] V. Gerasimov, Vektory Razvitiya Voennoi Strategii, Krasnaja Zvezda, March 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/

[43] W. Roepke, H. Thankey, Resilience: the first line of defense, NATO review, February 2019 available here: https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

other capabilities for countering hybrid threats and should be combined with soft power elements such as institutions, strategy-making, training, and exercises etc.

As an essential base of credible defense, resilience also requires a strong military and civilian connectivity and synchronization to deter hybrid threats. Since hybrid warfare exploits vulnerabilities of governance and targets civil society, a permanent interaction between governments, people and the civil-military interface is needed to ensure that all stakeholders are engaged at a state and individual level to counter threats and to respond to future security challenges.

EU and NATO combined approaches: The European Neighborhood Policy and NATO's 'Projecting stability' to the Eastern neighborhood through different means with resilience as a core

The Warsaw Summit communiqué from 2016 makes a reference to partner countries and states that "NATO's resilience can be enhanced […] by strengthening the resilience of partner countries in the Alliance's neighborhood" and that "if NATO's neighbors are more stable, NATO is more secure".[44] The EU has similar objectives in its European Neighborhood Policy launched in 2004 and focuses on stabilizing its neighborhood in political, economic and security terms, "promoting key EU interests of good governance, democracy, rule of law and human rights, and facilitating cooperation at regional level".[45] Creating synergies with partner countries regarding risk reduction, fostering stability, security and prosperity in the neighborhood are important priorities for the EU's European Neighborhood policy and NATO's 'Projecting stability'.

Formalized at the 2016 Warsaw Summit, NATO's 'Projecting stability' is recognized as a set of activities "coherently articulated and comprehensively developed, which influence and

[44] Meyer-Minnemann, "Resilience and Alliance Security: The Warsaw Commitment to enhance resilience", *Forward Resilience: Protecting Society in an interconnected world*, p.3, available here: https://archive.transatlanticrelations.org/wp-content/uploads/2016/12/resilience-forward-book-meyer-minnemann-final.pdf
And NATO Heads of State and Government, "The Warsaw Declaration on Transatlantic Security", 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133168.htm
[45] European Commission, European neighborhood policy, available here: https://ec.europa.eu/info/policies/european-neighbourhood-policy_en

shape the strategic environment to make it more secure and less threatening".[46] NATO's "Projecting Stability" toolkit in the Eastern neighborhood revolves around the reduction of security threats, promoting internal stability, the anticipation of crises in the immediate neighborhood and ensuring that the Eastern Partnership neighbors become security providers for themselves.[47] It includes building security capacity and improving capabilities through education, training, exercises, providing advice on institutional reforms in the defense sector, strengthening interoperability and institutional capacity and developing partnership programs in the defense and security sectors to enhance the quality of governance and resilience of neighboring states.[48]

The EU and NATO's well-developed policies provide the Eastern Partnership countries with a set of tools and instruments that enhance the partners' own national capabilities and make them more agile, adaptive, and resilient.

With regard to countering hybrid threats in the Eastern Partnership region, the EU-NATO tools and instruments combine situational awareness and information sharing, training and exercises, confidence-building measures, building interoperability for operational purposes, security capacity-building and reassurance instruments, and reinforcement of common institutional cooperation. The EU and NATO are devoting resources and expanding the partnership toolkits on resilience questions. This leads to a better synchronization of common efforts in the detection, prevention, and response to hybrid activities in the EaP region. Common work on shared resilience with the Eastern Partnership countries contributes to a better stability in Europe and leads to a better understanding of the common operational picture between the Eastern Partnership countries. Hybrid risk surveys with Georgia and Moldova are identifying key vulnerabilities and contributing to a better development of indicators for improving the resilience of different sectors.

Looking at the diverse instruments that the EU and NATO are applying to counter hybrid threats, it is important to stress the complementary nature of the EU-NATO means. In the *domain of information*, NATO and the EU are working closely with the EaP countries to share

[46] NDC Research Paper, "Projecting Stability: Elixir or Snake Oil" edited by Ian Hope, Research Division, December 2018
[47] NATO, Partnerships: projecting stability through cooperation, June 2020, available here: https://www.nato.int/cps/en/natohq/topics_84336.htm
[48] Ibid.

best practices on how to identify fake news and disinformation. Media literacy campaigns, twinning[49] and exchange programs on these questions are available to the EaP countries through the European Neighborhood Policy instruments. The European External Action Service's East StratCom Task Force established in 2015 to counter Russian disinformation campaigns is helping the Eastern Partnership countries' citizens to "develop resistance to digital information and media manipulation".[50] Monitoring of the information environment, exposing facts and countering disinformation, support of free independent media, situation awareness, sharing best practices, and credible public communications are the most common EU-NATO instruments to deal with hybrid threats in the domain of information. Diverse public diplomacy campaigns that engage different audiences in the Eastern Partnership countries, especially media professionals, the young population, opinion makers, and civil society can strengthen the EU-NATO approaches in dealing with disinformation in the EaP countries.[51] Recognizing disinformation and improving mental preparedness against disinformation in the EaP countries combined with media literacy and risk management culture are the key factors that are needed to foster resilience in the domain of information and where further support from the EU and NATO is required.

In the *cyber domain* the EU provides numerous financial resources to the EaP countries such as the 'Instrument contributing to Stability and Peace (IcSP)', the 'European Neighborhood Instrument', and 'Capacity Building and Cooperation to enhance Cyber Resilience' that help to create a cyber-resilient environment in the EaP countries. The EU4Digital program is aimed at enhancing the cyber-resilience and criminal justice capacities of the Eastern Partnership countries and at combating cybercrime. Through this program the EU is intending to improve the EaP's critical information infrastructure resilience and to "decrease the risk of disruption or failure of network information systems".[52] Through the Instrument contributing to Stability and Peace and under the EU4Digital initiative, the EU institutions are reinforcing the cybersecurity of elections in the EaP countries by providing different types of training and

[49] Twinning is a European Union instrument for institutional cooperation between Public Administrations of EU Member States and of beneficiary or partner countries.
[50] EUvsDisinfo, available here: https://euvsdisinfo.eu/about/
[51] Interview with EU official, Chatham House rule, February 2021
[52] EU4Digital, Cybersecurity guidelines for the Eastern Partner countries, June 2020, available here: https://www.euneighbours.eu/sites/default/files/publications/2020-12/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf
https://ec.europa.eu/neighbourhood-enlargement/sites/default/files/c_2018_8184_f1_annex_en_v1_p1_1000418.pdf

exchanges between cyber experts of the EU Member States and representatives of the EaP countries.[53] There are different pilot projects under development that aim at amplifying the cyber capacity building and security sector reform of the EaP countries.

NATO's Communication and Information Agency (NCIA) and the NATO Industry Cyber Partnership are collaborating on the further development of technical cooperation with the Eastern Partnership countries. For example, Ukraine's signature of the Memorandum of agreement with the NCIA in 2015 has facilitated the process of the implementation of the NATO-Ukraine Trust Fund on Consultation, Command, Control and Communication.[54] The NCIA is strengthening its cooperation with Ukraine and Georgia to help modernize their Command, Control, Communication and Computer capabilities. Building robust and resilient CIS capabilities is important for these Eastern Partnership nations who aspire to join NATO and need to meet NATO's standards. Furthermore, the NCIA provides technical advice in the domain of cyber security and enhances the national capabilities of the EaP countries. At the end of January 2021 for example a new Cyber Incident Response Capability for the Moldovan Armed Forces was established to increase cyber defense capabilities and Moldova's capacity to respond to cyber threats.[55] Different workshops and conferences on cyber security and defense with a participation of the EaP countries, NCIA and NATO's Cyber Incident Response Center and NATO-Industry Cyber partnership contribute to operational awareness on cyber security and foster knowledge transfer on cyber threats and information security. Further development of the network of relevant institutions dealing with cyber domain and the incorporation of the Eastern partners into threat information-sharing platforms can promote information sharing further, mitigate security risks, and enhance cyber resilience to better respond to cyber-attacks.

With respect to *energy security*, the EU regulatory framework provides further diversification, market liberalization, energy efficiency, the integration of European energy networks. Through the EU's strategy of diversifying suppliers, the Union is becoming less dependent on Russia's gas and is creating an interconnected and transparent gas market. The EU ensures compliance

[53] EU institutions, EU4Digital: Cybersecurity East, available here : https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/
[54] NCIA webpage, https://www.ncia.nato.int/about-us/newsroom/natoukraine-agreement-paves-the-way-for-further-technical-cooperation.html
[55] NATO, Cyber Incident Response Capability established in the Republic of Moldova with NATO support, January 2021, available here: https://www.nato.int/cps/en/natohq/news_180758.htm?selectedLocale=en

with the EU's internal market rules according to the principles set up in the Energy Union package and "A framework strategy for a resilient Energy Union with a forward-looking climate change policy".[56] The EU's focus in the Eastern Partnership countries is on diversification, the development of unconventional sources of energy, on the promotion of alternative energy projects and on the modernization of energy infrastructure.[57] NATO pays special attention to the protection of critical energy infrastructure in the EaP countries, energy risk assessment, situational awareness and identification of lessons learnt from energy supply disruptions. A better energy risk identification and a transfer of NATO's resilience guidelines knowledge from NATO member states to the Eastern Partnership countries will improve synergies between institutions and the EaP partners and maximize resilience efforts in energy security matters.[58]

Exercises and training with the EaP countries as well as the EU's Technical Assistance and Information Exchange (TAIEX) and twinning programs lead to a better transfer of knowledge, an enhancement of institutional capacity and to a better analysis of weaknesses in certain operational areas. NATO incorporates hybrid elements in its trainings with the EaP countries and lessons learnt from exercises improve strategic thinking on how to deal with the new spectrum of hybrid threats that has become the new normal in today's security environment.[59] Different types of exercises with the participation of the Eastern Partnership countries enhance the effectiveness of these countries' decision-making capacity to deal and to respond to the complexity of hybrid threats and contribute to the efficiency of crisis management response procedures. "Civil-military education, training for hybrid warfare […] with a focus on [rehearsing hybrid style attacks and how to match them, including the full integration of cyber and information warfare], joint conferences, joint working groups, and a maintaining of a balanced force for multiple responses" are essential to successfully deal with hybrid tactics.[60]

The *knowledge hubs* such as the European Centre of Excellence for Countering Hybrid Threats, the NATO Strategic Communication Center of Excellence, or the NATO Energy Security

[56] V. Ratsiborynska, Russia's hybrid warfare in the form of its energy manoeuvres against Europe: how the EU and NATO can respond together?, NATO Defense College, June 2018.
[57] Ibid.
[58] Interview with NATO official, February 2021
[59] NATO, London Declaration, December 2019, available here: https://www.nato.int/cps/en/natohq/official_texts_171584.htm
[60] Written interview with Prof. Dr. Robert Johnson, Director of the Oxford Changing Character of War Centre, University of Oxford.

Centre of Excellence, the NATO Cooperative Cyber Defense Centre of Excellence provide a venue for the EaP countries to increase their awareness of hybrid threats, to share, inform and further engage on resilience and hybrid threats. Further *outreach to the like-minded community of partners* can lead to innovation and to better preparedness to face a wide array of hybrid threats. Creation of synergies between different organizations can increase national capacities of partner states. Fostering cooperation with like-minded organizations engaged in the questions of rule of law and democratization in the Eastern Partnership countries such as the Council of Europe, OSCE, UN and others can ensure better complementarity with the EU-NATO approaches and can support local governance's efforts in achieving a better level of institutional readiness and preparedness to deal with hybrid threats.

On policy the EU's *sanction-based policy* towards Moscow is further *increasing costs* for Russia's actions in the EaP countries. In its messages towards Russia the EU calls for the cessation of violations in the Eastern part of Ukraine and for restoring the territorial integrity of Ukraine, Georgia, and Moldova.[61] At the same time the EU is pursuing its policies of dialogue, mediation and conflict prevention and is engaged in multilateralism and regional cooperation with the Eastern partners. The EU is supporting the EaP's reform processes that include anti-corruption measures, energy sector reforms, strengthening of the rule of law and efficient local governance etc. The EU's solid *macro-financial assistance programs* to the EaP countries and increase of trade deals constitute a basis for a further intensification of economic and political relations with the Eastern Partnership countries. The EU's framework for the *screening of investments* from non-EU countries focuses its efforts on the protection of critical infrastructure against foreign investments that can be used as part of a hybrid campaign in Europe. Nowadays growing emphasis is given to areas such as cyber security, the strengthening of institutional governance and institutional capacity, the fight against disinformation and the protection of critical infrastructure in the EaP countries. Furthermore, according to the 2020 policy guidance 'The Eastern Partnership beyond 2020: Reinforcing resilience-an Eastern Partnership that delivers for all', the EU institutions continue working with the Eastern Partnership countries for more resilient, sustainable, and integrated economies; for the rule of law and accountable institutions; toward environmental and climate change resilience; digital

[61] https://www.consilium.europa.eu/en/european-council/president/news/2021/03/03/20210301-pec-visit-georgia-moldova-ukraine/

transformation; and for fair and inclusive societies.[62] From NATO's side a dual-track approach of deterrence and dialogue towards Russia and a continuous capacity-building of the EaP countries provide a set of means to empower the EaP partners and to ensure persistent NATO support to them.

Further actions and work in progress for the Eastern Partnership region

As indicated by numerous security experts from the EU and NATO, the EaP governments should increase their efforts to better include civil society into resolving resilience issues and countering hybrid threats and to incorporate them into civil preparedness planning. Fostering societal resilience puts a strong emphasis on the capacity building of civil society and on a shared understanding of risks amongst different stakeholders, including the private sector.[63]

The private sector plays an important role in identifying different external threats and should be included in a list of priority stakeholders when dealing with hybrid threats, especially in the cyber and energy domains which requires public-private cooperation and effective counter strategies. Local authorities from the Eastern Partnership countries are other stakeholders that need to be integrated into a list of priority in capacity building as they deal with the hybrid spectrum of risks and vulnerabilities on a regular basis and often form the basis for building up resilience at a state and community levels.[64]

A development of complementary and cross-cutting cooperation between civilian and military actors, between national and local governments, EU and NATO institutions, public and private sectors, academia, and civil society will provide a broader spectrum of tools to use against hybrid threats.

A tailored communication and outreach campaigns to these audiences on hybrid threats and security risks associated with them is highly necessary and can help to form a better public awareness of hybrid threats. Effective operational cooperation and communication between the

[62] EEAS, Joint Communication: Eastern Partnership policy beyond 2020: Reinforcing resilience- an Eastern Partnership that delivers for all, March 2020, available here: https://eeas.europa.eu/headquarters/headquarters-homepage/76166/joint-communication-eastern-partnership-policy-beyond-2020-reinforcing-resilience-%E2%80%93-eastern_en

[63] Interview with security experts, March 2021

[64] Interview with security experts, March 2021

EU, NATO institutions and the Eastern Partnership countries will further raise public awareness and readiness to face external pressure. A regularly updated risk assessment process, analysis, and monitoring of indicators of hybrid actions should improve communication and address gaps in understanding the nature of hybrid threats and their evolving character amongst different stakeholders.

Improving institutional governance and the rule of law, capacity building of local communities, intelligence services and anti-corruption authorities are crucial in the EaP countries to enhance social resilience and to create a climate of public trust of democratic norms, values, and key democratic institutions. Building on local demands from these groups and empowering them, further investing in institutional capacity-building as well as providing more twinning to these actors are important drivers for structural reforms and for fostering EU-NATO-EaP cooperation.

"Restructuring the Eastern Partnership" to further "differentiate between partners with signed Association Agreements" will address ambitions of different EaP partner states in a better way. Ukraine, Georgia, and Moldova are showing their determination to continue economic, social, and political reforms in line with their European aspirations. The country reports from the EU institutions on Ukraine, Georgia, and Moldova indicate that more progress should be achieved in integrity building of their institutions, countering corruption, judicial reform legislation, and ensuring accountability of their local administrations. The EU and NATO are playing transformative powers for those partner countries and create a degree of interdependence that difficult to reverse as they have an impact on all reforms undertaken by them. Different pilot initiatives and programs within the EU and NATO cooperative instruments are offered to the EaP countries that address systemic governance vulnerabilities and offer a framework of Europeanization.

Further upgrading the EaP policy with security instruments in the coming years will be necessary to make the EU a more assertive geopolitical and security player in the Eastern neighborhood.[65] The recently adopted financial instrument 'European Peace Facility' is a right step on the path of the EU's geopolitical and security repositioning in the immediate

[65] Iulia Joja, "The EU's East: A way forward", Middle East Institute, March 2021, available here: https://www.mei.edu/publications/eus-east-way-forward
And interviews with security and EU experts and officials, February, and March 2021

neighborhood as it allows the EU not only "to support partner countries bilaterally in military and defense matters but also to provide military equipment to increase partners' defense capabilities".[66]

The development of strategic security partnerships with key neighbors in the East and the creation "of a security compact for the Eastern Partnership, comprising targeted support for intelligence services, cyber security institutions, and armed forces" will be beneficial to the Eastern Partnership countries and provide them with more reassurance.[67]

NATO's further adaptation and a "revision of NATO's mandate to deal with conflict in the grey zone" as well as fostering partnerships and networks on hybrid threats and boosting current initiatives in the Eastern neighborhood will further foster shared resilience between NATO, the EU institutions, and the Eastern Partnership countries.[68]

Conclusions:

Hybrid threats are a permanent feature of today's security environment and a part of the current EU, NATO, and the Eastern Partnership countries security landscape. NATO, the Eastern Partnership countries, and the EU have a common interest in working closely together in reducing their strategic, operational, and tactical vulnerabilities in different domains of national power and in maximizing their shared resilience efforts to respond to the current challenges of the security environment. A common adaptation to future challenges will mark a shift to a better common security vision and will reinforce their strategic thinking on shared security threats such as hybrid threats.

[66] https://eeas.europa.eu/headquarters/headquarters-homepage/46286/questions-answers-european-peace-facility_en

[67] Nicu Popescu and Gustav Gressel, "The best defense: Why the EU should forge security compacts with its eastern neighbors", *European Council on Foreign Relations*, November 2020, available here: https://ecfr.eu/publication/the-best-defence-why-the-eu-should-forge-security-compacts-with-its-eastern-neighbours/

[68] Interview with security official, March 2021
And M. Ozawa, "Adapting NATO to grey zone challenges from Russia", *NDC Research Paper No.17*, NATO Defense College, Rome, February 2021.