POLICY PAPER

EU, NATO AND UKRAINE

DREAM TEAM OR A TRIANGLE?

HANNA SHELEST, PHD
VIKTORIIA OMELIANENKO

UKRAINIAN PRISM

EU, NATO AND UKRAINE: DREAM TEAM OR A TRIANGLE?

Policy paper of the Ukrainian Prism's Security Studies Program, supported by the International Renaissance Foundation.

Authours:
Hanna Shelest, PhD, Security Studies Program Director, Foreign Policy Council "Ukrainian Prism"

Viktoria Omelianenko, Security Studies Program Fellow, Foreign Policy Council "Ukrainian Prism"

Contents

EU and NATO after 2014

Relations between NATO and the EU were institutionalised in the early 2000s due to steps taken by the EU to promote their greater responsibility in security matters. As soon as the EU started to express the will to play a role in security and defence matters (late 1990s), the question was posed of its relationship with NATO as the main defence actor in Europe. Since then, questions have been posed in different countries about what the EU would bring that NATO does not already do.[1] Fear of overlapping spheres of interest and responsibility, redistribution of the member-states financial resources, and search for the EU priorities and niche in the security sphere have become main discussion points for the next decade.

The year 2014 became an important milestone when the EU and NATO started reviewing their security priorities, especially in relations with partners. It also triggered a deeper dialogue and attempts to structure cooperation and coordination between the two organisations. Two developments led to the realisation that the status quo was untenable. First, Europe faced new threats and challenges emanating from the East and the South – and neither organisation had the whole range of tools needed to address the security environment changes. Second, the European Union laid the foundations for a common defence by building two defence pillars: The Permanent Structured Cooperation and the European Defence Fund. EU-NATO cooperation became the third pillar of European defence, underlining the organic link between the two organisations[2].

The EU Strategic Compass 2022 clearly stressed that "a stronger and more capable EU in security and defence will contribute positively to global and transatlantic security and is complementary to NATO, which remains the foundation of collective defence for its members."[3] Through the text, cooperation with NATO is emphasised in the issues of training and military capabilities (in line with NATO standards), counter-hybrid threats, including in the information sphere, cyber, airspace protection and access, arms control, crisis response and logistics, national defence planning, commitments in the Western Balkans and Ukraine. Among others, it was stated that "The transatlantic relationship and EU-NATO cooperation, in full respect of the principles set out in the Treaties and those agreed by the European Council, including the principles of inclusiveness, reciprocity and decision-making autonomy of the EU, are key to our overall security.[4]

In the respective section on NATO partnership, the future perspectives identified as further enhancement of the ongoing cooperation on political dialogue, information sharing, crisis management operations, military capability development and military mobility; deepening common work on enhancing maritime security and countering hybrid threats, including foreign information manipulation and securing cyberspace as well as the implementation of the Women, Peace and Security Agenda; expanding cooperation on emerging and disruptive technologies, climate change and defence, resilience and outer space.

---

[1] Thierry Tardy, EU-NATO relationship: Cooperation and competition, Anadolu Agency, 18.07.2023, https://www.aa.com.tr/en/analysis/opinion-eu-nato-relationship-cooperation-and-competition/2948527

[2] Alexandros Papaioannou, Strengthening EU-NATO relations, NATO Review, 16.07.2019, https://www.nato.int/docu/review/articles/2019/07/16/strengthening-eu-nato-relations/index.html

[3] A Strategic Compass for Security and Defence, 21.03.2022, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

[4] A Strategic Compass for Security and Defence, 21.03.2022, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

The 2022 NATO Strategic Concept[5] is more internally oriented, emphasising own capabilities of the Alliance with a regular focus on "European" security. Nevertheless, the first time the EU is mentioned is in the paragraph regarding human security – "Human security, including the protection of civilians and civilian harm mitigation, is central to our approach to crisis prevention and management" – where the EU mentioned along with the UN, OSCE, and the African Union.

The paragraph describing the EU-NATO relations in the Strategic Concept highlighted the spheres of priority cooperation that are not identical to the EU Strategic Compass – "issues of common interest, such as military mobility, resilience, the impact of climate change on security, emerging and disruptive technologies, human security, the Women, Peace and Security agenda, as well as countering cyber and hybrid threats and addressing the systemic challenges posed by the PRC to Euro-Atlantic security".

What is common in both documents is that the organisations, first and foremost, stress their unity and partnership, which is based on shared values. "Complementarity", among other things, has been a key message as the two organisations have been operating within one another's core policy areas in response to the Russian aggression.[6]

As of 2016, the three Joint Declarations on EU-NATO cooperation (2016, 2018, 2023) have allowed the two actors to institutionalise their cooperation, thus shaping to a degree their respective activities.

The 2016 Joint Declaration[7] emphasised the following spheres for cooperation: hybrid warfare and prevention, resilience building, maritime security and migration, cyber, defence industry and research, and joint training.

The 2018 Joint Declaration,[8] while confirming the 2016 priorities, also focused on the additional spheres for cooperation: military mobility, counter-terrorism, strengthening resilience to chemical, biological, radiological and nuclear-related risks, and promoting the women, peace, and security agenda.

The 2023 Joint Declaration[9] differs in its scope from the two previous ones, as it spends more attention on the current threats and challenges and what has been reached. Still, it also provided new insights into the further priorities for cooperation. In addition to countering Russian and Chinese threats, as well as helping Ukraine in its war against Russia, the Joint declaration stressed the growing geostrategic competition, resilience issues, protection of critical infrastructures, emerging and disruptive technologies, space, the security implications of climate change, as well as foreign information manipulation and interference.

In 2016 and 2017, the EU and NATO endorsed lists of measures to advance how NATO and the EU should work together[10]. Seventy-four actions are foreseen in the seven areas of cooperation: countering hybrid threats, operational cooperation including maritime issues, cyber security and defence, defence capabilities, defence industry and research, parallel and coordinated exercises, and defence and security capacity building. Despite some measures being limited by 2018 in terms of

---

[5] The 2022 NATO Strategic Concept, NATO official website, June 2022, https://www.nato.int/strategic-concept/

[6] Baris Celik, Ukraine war is blurring the lines between Nato and the EU on defence policy, 1.03.2023, The Conversation, https://theconversation.com/ukraine-war-is-blurring-the-lines-between-nato-and-the-eu-on-defence-policy-200849

[7] Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 8.07.2016, https://www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en

[8] Joint Declaration on EU-NATO Cooperation, 10.07.2018, https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=en

[9] Joint Declaration On EU-NATO Cooperation by The President Of The European Council, The President of the European Commission and The Secretary General of the North Atlantic Treaty Organization, 10.01.2023, https://www.nato.int/cps/en/natohq/official_texts_210549.htm

[10] Relations with the European Union. NATO official website, 25.07.2023, https://www.nato.int/cps/en/natohq/topics_49217.htm?

implementation, no new plans have been developed, but the annual implementation reports presented evaluating the mentioned 2016 and 2017 actions.

Military mobility, resilience and cyber security became the topics of the biggest practical efforts' application. For example, in 2017, the Netherlands took the lead in developing military mobility as a project in the Permanent Structured Cooperation (PESCO).[11] By November 2022, the United States, Canada, Norway, and the UK joined the project. Military mobility became one of the priorities for EU-NATO cooperation, according to the joint declarations. Supply of military equipment and ammunition to Ukraine, as well as a movement of the NATO member-states forces closer to the Eastern Flank and an increased number of military drills, provided both organisations with enormous lessons learned material that can be used for the next action plans preparations and adjustments of the recommendations.

In January 2023, NATO and the EU agreed to create a taskforce on resilience and critical infrastructure protection. Considering Russia's attempts to weaponise energy and sabotage the Nord Stream pipelines in September 2022, the joint taskforce focused, among others, on making critical infrastructure, technology and supply chains more resilient to potential threats and taking action to mitigate potential vulnerabilities.[12] Moreover, on 29 June 2023, the NATO Secretary General took part in the European Council, where he welcomed NATO-EU cooperation on the resilience of critical infrastructure and the assessment report, which suggested concrete ways to further develop ties – including through more information exchanges, work to identify alternate transport routes for civilian and military mobility; and closer ties in security research.[13]

The range of subjects discussed between NATO and the EU has expanded considerably over the past several years. Political dialogue covers the full spectrum of issues relevant to both organisations, including the geopolitical implications of COVID-19, cyber and hybrid threats, Russia, China, the Western Balkans, the Middle East and Afghanistan. Since Russia's illegal annexation of Crimea in 2014, and especially since Russia escalated its war of aggression with its full-scale invasion of Ukraine in 2022, both organisations have worked to make sure that their actions complement each other, especially with regard to Russia and assistance to Ukraine.[14] Emphasising the importance of the partnership, both the EU's Strategic Compass and NATO's Strategic Concept called for further enhancing cooperation in areas of mutual interest, including military mobility, hybrid, cyber and climate change-related threats, outer space, and emerging and disruptive technologies.[15]

---

[11] PESCO Projects. Military Mobility. https://www.pesco.europa.eu/project/military-mobility/

[12] Relations with the European Union. NATO official website, 25.07.2023, https://www.nato.int/cps/en/natohq/topics_49217.htm?

[13] Secretary General at European Council: NATO-EU cooperation is key to supporting Ukraine, responding to key security challenges, NATO Official website, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216639.htm?selectedLocale=en

[14] Relations with the European Union. NATO official website, 25.07.2023, https://www.nato.int/cps/en/natohq/topics_49217.htm?

[15] Jan Joel Andersson, European Defence Partnerships, Brief #3, EUISS, February 2023

Cyber Resilience Case Study

Development of the technologies has posed challenges for many countries on how to keep pace with the advancements and, at the same time, address the new risks – especially the growing competition and the malicious hybrid and cyber activities. The EU and NATO actively address such challenges in their respective policies and joint cooperation with mutually reinforcing and complementary efforts.

The EU

The cooperation of the EU and NATO in the digital domain, especially cyberspace, is largely defined by the internal agenda of the two organisations. Digital policy has been a cross-cutting line in the EU policies in the number of other procedures from social to industry and security.[16] In 2013, the EU released the first cyber security strategy, updated in 2017, focusing on better protection of critical infrastructure and advancing resilience in the cyber domain. The current cyber security strategy was released in December 2020.

Considering the Russian attacks in Ukraine in 2014 and the growing number of cyber-attacks, the EU included cyber policy in its external policy priorities with the Conclusion of the Council of the EU on Cyber Diplomacy dated 2015. In 2017, the EU launched its Cyber Diplomacy toolbox that legitimises the use of the measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures toward countering and responding to malicious cyber activities. Council Conclusions of 2017 stressed that a particularly serious cyber incident or crisis could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause and/or the Mutual Assistance Clause.[17] In addition, there are eight PESCO cyber-related projects.[18]

In 2018, the EU identified cyberspace as a domain of military operations.[19] Since then, starting from the launch of the EU Cyber Defence Policy Framework, the EU has clearly defined its commitment to fostering its cyber defence with six objectives, including closer cooperation with NATO to avoid "unnecessary duplication and ensure coherence and complementarity of efforts".[20] The recent EU Strategic Compass, where the word 'cyber' is mentioned 45 times, states that cyberspace has become

[16] European Commission, 2030 Digital Compass: The European way for the Digital Decade, 2022, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[17] Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Council of the EU, 20.11.2017, https://www.consilium.europa.eu/media/31666/st14435en17.pdf

[18] Cyber-related PESCO projects, November 2019, https://eucyberdirect.eu/atlas/sources/cyber-related-pesco-projects

[19] Annegret Bendiek, Raphael Bossong, "The EU's Revised Cybersecurity Strategy", German Institute for International and Security Affairs, SWP, November 2017, https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf

[20] EU Cyber Defence Policy Framework (2018 update), Council of the EU, 19.11.2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

an area for competition. It also established the Hub for EU Defence Innovation (HEDI) in the European Defence Agency – an important boost for the EU's engagement in innovations. [21]

Last but not least, the 2022 Joint Communication of the European Commission on EU Policy on cyber defence states that the Russian invasion of Ukraine has been a 'wake-up call' and that "the EU needs to take on more responsibility for its own security" via ensuring its technological and digital sovereignty in the cyber field. The number of proposed initiatives mention the need for the establishment of an EU Cyber Defence Coordination Centre (EUCDCC) supporting enhanced situational awareness within the defence community, including all EU military CSDP commanders and the establishment of a new Military Computer Emergency Response Team Operational Network (MICNET) supported by European Defence Agencies. As one of the needs of the EU is also to protect its businesses and citizens, the EU pays special attention to the resilience of the EU cyber security ecosystem at the domestic level that is embodied in the update of the Directive on security of network and information systems (NIS) to NIS2, design of the EU Cyber resilience Act that lay down cybersecurity requirements for products with digital elements aiming to reduce the attack surface in dual-use products and EU Cyber Solidarity Act in May 2023 that aims to create the "Cybersecurity Shield" and establish operation residence in the domain while also introducing Cybersecurity Academy initiative.[22]

The cooperation with NATO is specifically outlined in the Communication, for which in July 2023, the Parliament released the draft opinion with amendments in terms of the efforts for "compatibility with NATO concepts and doctrine on cyber defence to the maximum extent possible",[23] while the cooperation is defined in the field of cyber defence training, education, situational awareness and exercises.

NATO

The protection of information systems and communication has been on the NATO agenda for a long time, including the two dimensions – its own cyber security and the cyber security of its allies. With the evolving threats, the NATO cyber policy ecosystem has also been advancing. For the first time, NATO placed cyber defence on the Alliance's political agenda at its Prague summit in 2002. With the attacks on Estonia in 2007, NATO responded with the Policy on Cyber Defence and established the Tallinn Centre – NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). With the attacks on Ukraine and the start of the war, NATO allies recognised that a cyber-attack could be grounds to invoke Article 5 of NATO's founding treaty – what became a milestone in the Alliance policies. Moreover, in 2016, NATO recognised cyberspace as a domain of operations in which NATO must defend itself. In 2018, Allies founded the Cyberspace Operations Centre in Belgium, which provides situational awareness and protects NATO's own networks by providing centralised and round-the-clock cyber defence support.[24]

The Madrid Summit 2022 set another important milestone that emphasised the need for civil-military partnership and industry cooperation. Moreover, NATO established the Defence Innovation Accelerator

---

[21] Council of the European Union, A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values, and interests and contributes to international peace and security, Council of the EU, 21.03.2022, https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

[22] Omelianenko V. EU's and Ukraine's approaches to digital diplomacy in the geopolitics of technologies, Ukrainian Prism, 2023, http://prismua.org/en/english-eus-and-ukraines-approaches-to-digital-diplomacy-in-the-geopolitics-of-technologies/

[23] Joint Communication to The European Parliament and The Council. EU Policy on Cyber Defence, 10.11.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52022JC0049#footnote60

[24] Cyber defence, NATO Official website, 14.09.2023, https://www.nato.int/cps/en/natohq/topics_78170.htm

(DIANA) and launched a multinational Innovation Fund to bring together governments, the private sector, and academia to bolster technological development.[25]

In June 2023, NATO founded the world's first-ever multi-sovereign fund – the NATO Innovation Fund (NIF) to invest 1 billion euros in early-stage start-ups and other venture capital funds developing dual-use emerging technologies of priority to NATO.[26] At the Vilnius summit in 2023, NATO also defined a new concept for cyber defence with three levels – political, military, and technical as well as launched the Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts in response to significant malicious cyber activities.[27]

EU-NATO cooperation

As cyber security and especially cyber defence have been on the agenda of both actors, the domain is crucial for the bilateral cooperation between NATO and the EU. As the two organisations increased their efforts to counter hybrid threats, cyber defence became one of the areas of 'strengthened cooperation' between NATO and the EU.[28]

The first Joint EU-NATO Declaration concluded in Warsaw in July 2016 outlined the cooperation built around the following dimensions – interoperability in cyber defence requirements and standards, cyber defence research and technology innovation cooperation, cooperation on training for mutual staff participation and cyber exercises through reciprocal staff participation, including in Cyber Coalition and Cyber Europe exercises.[29] Within the set proposals presented in 2016 and 2017, 22 actions out of 74 were dedicated to the cyber sphere.[30] What needs to be emphasised is the EU Council's Conclusions to implement the joint Declaration, stating that the Joint Declaration gives the impetus to support the resilience and capacity building in Western Balkans, the Eastern and Southern Neighbourhoods.[31]

Another crucial area where cooperation was established in 2016 is information sharing in the domain of cybersecurity at the operational and strategic levels. The Technical Arrangement on Cyber Defence was signed in February 2016 between NATO's Computer Incident Response Capability and the EU's Computer Emergency Response Team to improve cyber incident prevention, detection, and response in both organisations, in line with their decision-making autonomy and procedures.[32] The 2018 Joint Declaration mentioned that the EU and NATO timely exchanged information on cyber-attacks,

---

[25] Madrid Summit Declaration, NATO Official website, 29.06.2022, https://www.nato.int/cps/en/natohq/official_texts_196951.htm

[26] NATO launches Innovation Fund, NATO Official website, 30.06.2022, https://www.nato.int/cps/en/natohq/news_197494.htm

[27] Vilnius Summit Communiqué, NATO Official website, 11.07.2023, https://www.nato.int/cps/en/natohq/official_texts_217320.htm

[28] Cyber defence, NATO Official website, 14.09.2023, https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en

[29] Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, NATO Official website, 6.12.2016, https://www.nato.int/cps/uk/natohq/official_texts_138829.htm?selectedLocale=uk

[30] EU-NATO cooperation: what has been achieved so far? Clingendael Report, October 2021, https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/

[31] EU-NATO cooperation: Council adopt conclusions to implement Joint Declaration, Council of the EU, 6.12.2016, https://www.consilium.europa.eu/en/press/press-releases/2016/12/06/eu-nato-joint-declaration/

[32] EU and NATO cyber defence cooperation, EEAS, 10.02.2016, https://www.eeas.europa.eu/node/3667_en

confronted disinformation and generally addressed hybrid threats while building the resilience of their members and partners. [33]

The third declaration signed in Brussels in January 2023 states that the EU and NATO achieved "unprecedented progress across all areas of cooperation", also mentioning hybrid and cyber threats. At the same time, the declaration strived to address resilience, especially that comes from the protection of critical infrastructures emerging and disruptive technologies.[34] These areas need to be considered in detail as they are actively developing now both at the level of the EU-NATO cooperation and at the separate tracks.

On 16 March 2023, the EU and NATO established a Taskforce on the resilience of critical infrastructure. The assessment report dated July 2023 defines critical infrastructure as the important element of the strategic partnership and cooperation between the two organisations, especially considering Russia's war of aggression against Ukraine and the large number of attacks against the critical infrastructure. The Assessment report set the number of tasks in the recommendations to be implemented by the EU-NATO Structured Dialogue on Resilience. Among 14 recommendations, the following are mentioned:

- the Parallel and Coordinated Assessments of the threats to critical infrastructure,
- strengthening the Structured Dialogue on Resilience that needs to consider the observations from Russia's war of aggression against Ukraine regarding the resilience of critical infrastructure,
- holding dedicated scenario-based discussions between staffs,
- promoting the exchange of best practices between civilian and military actors on the implementation of relevant cyber-related policies and legislation,
- identifying synergies and potential areas of cooperation in security research activities related to critical infrastructure, including challenges related to new technologies or supply chain security.[35]

Another mention comes for the emerging and descriptive technologies, as both the EU and NATO have actively started to develop defence innovations with the available instruments – EU's HEDI and NATO's DIANA have accelerators and test centres for the best and brightest deep tech innovators in the Alliance. Emerging and developing technologies and deep tech is the sphere where the EU and NATO need close cooperation rather than competition to foster the development of technologies in defence and security across the members and allies.

---

[33] 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, Council of the EU, 10.07.2018, https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

[34] Joint Declaration on EU-NATO Cooperation, 10.01.2023, Council of the EU, https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/

[35] EU-NATO Task Force On the Resilience of Critical Infrastructure. Final Assessment Report, June 2023, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

EU, NATO, and Ukraine

Russian full-scale invasion on 24 February 2022 became an important momentum to test the possibility of joint actions, coordinated position and ability to act for the EU and NATO. This moment also appeared vital to assessing their ability to share responsibility to avoid overlapping and multiply efforts results. The leadership of the two organisations met immediately on the first day of the invasion to coordinate their positions[36], which was a good sign of readiness.

The EU Strategic Compass for Security and Defence[37] was adopted in March 2022, so it could not fully reflect the changing realities of European security due to the full-fledged Russian invasion. However, in the summary, it was already clearly stated that member states "committed to defend the European security order. Sovereignty, territorial integrity and independence within internationally recognised borders should be fully respected. Supporting Ukraine in facing Russia's military aggression, we are showing an unprecedented resolve to restore peace in Europe, together with our partners".

NATO Strategic Concept had been adopted six months after the war started, however, it also predominantly had been agreed before the war and received only minor changes focusing on Russian aggression and support to Ukraine. The 2022 Strategic Concept elaborated on crisis prevention and management, recognising common challenges. However, the approach remained the same – partners are seen purely as recipients of security support from NATO, and their contribution of experience and knowledge is neglected despite the opposite situation being salient on the ground.[38]

The Madrid NATO summit communique in 2022 mentioned the Alliance's commitment to help Ukraine improve its cyber defences and resilience. In 2023, Ukraine signed the agreement on accession to the NATO Cooperative Cyber Defence Centre of Excellence, consisting of 25 NATO Allies and four partner nations.[39] In practical terms, Ukraine has become integrated into a number of NATO initiatives. For example, in 2023, Ukraine joined the largest in the world cyber training – Locked Shields.[40] The partners also concluded the Roadmap for cooperation with the agreement of Ukraine's participation in Crossed Swords 2023 cyber training. Moreover, in May 2023, NATO and Ukraine launched a High-level dialogue on Innovation and Disruptive Technologies,[41] aiming to expand the existing NATO-Ukraine partnership by exchanging views on the development of innovation ecosystems for both commercial and defence needs, and by sharing lessons learned from Ukraine.

---

[36] Andreas Rogal, EU and NATO coordinate response to Russia's invasion of Ukraine, The Parliament Magazine, 24.02.2022, https://www.theparliamentmagazine.eu/news/article/eu-and-nato-coordinate-response-to-russias-invasion-of-ukraine

[37] A Strategic Compass for Security and Defence, 21.03.2022, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

[38] Hanna Shelest, Alija Kozljak, Peter Lidén, Tengiz Pkhaladze, After Madrid: NATO, Aspirants and Enhanced Opportunity Partners, Ukrainian Prism, 2022, http://prismua.org/en/nato-after-madrid/

[39] Ukraine has signed an agreement on accession to the NATO Cooperative Cyber Defence Centre of Excellence, State Service of Special Communications and Information Protection of Ukraine, 19.01.2023, https://cip.gov.ua/en/news/ukrayina-pidpisala-ugodu-pro-priyednannya-do-ob-yednanogo-centru-peredovikh-tekhnologii-z-kiberoboroni-nato

[40] Catherine Stupp, NATO Cyber Game Tests Defenses Amid War in Ukraine, Wall Street Journal, 18.04.2022, https://www.wsj.com/articles/nato-cyber-game-tests-defenses-amid-war-in-ukraine-11650274203?tpl=cs

[41] NATO and Ukraine boost partnership through greater cooperation on science, technology and innovation, NATO official website, 25.05.2023, https://www.nato.int/cps/en/natohq/news_215006.htm

From the beginning, the EU-NATO relationship was both about complementarity/cooperation and about competition in the crisis management market.[42] The scale of the Russian invasion in Ukraine became a proper testing ground for which of these approaches prevail – complementarity or competition.

The original vision was that the EU has significant expertise in a wide range of policy areas, including trade, sanctions, energy and refugees. With the EU's recent membership vision for Ukraine, Brussels' toolkit would be highly relevant not only for tackling Moscow but also for the reconstruction of a post-conflict Ukraine. NATO was considered the primary platform for the West's military presence against Russia's aggression and a provider of the most reliable venue for the US and Canada to coordinate their policies with their European counterparts. Furthermore, as a nuclear alliance, NATO was referred to as the West's first collective response to Russia's threats to go nuclear in Ukraine[43].

While the EU and NATO are focused on the defence cyber capabilities, Ukraine has significantly advanced on the cyber offensive and the development of military innovations. The secret weapon in Ukraine's fight against Russia's advantages in terms of conventional military might, workforce, and resources is people – around 300,000 IT professionals that have comprised the vivid IT ecosystem over the years.[44] With the Russian full-scale invasion and the constant attacks before it, more than 200,000 volunteers joined the IT Army that, within a year, has run 153 operations with more than 400 Russian companies attacked.[45] Another significant advancement of Ukraine is in developing innovation and start-ups, especially in defence. Ukraine prioritises advancing such innovations through the development of a dynamic venture capital investment ecosystem and support of Ukrainian start-ups. Ukraine's flagship BRAVE1 is a tech cluster for developing the country's defence tech industry. It was launched in spring 2023 by Ukraine's Ministry of Digital Transformation, Ministry of Defence, Ministry of Economy, Ministry of Strategic Industries, the National Security and Defence Council, and the General Staff of the Armed Forces of Ukraine. The platform accelerates companies and defence tech start-ups to find partners and gain assistance with the cluster. By midsummer 2023, BRAVE1 had registered approximately 400 projects, with almost 200 undergoing military testing.[46]

EU and NATO have been providing crucial support to Ukraine in terms of the modernisation of Ukraine's cyber security ecosystem since 2014 – especially regarding the protection of Ukraine's critical infrastructure, provision of the experience and strengthening the capabilities of Ukraine in the regulatory and institutional dimensions.

Back in 2014, Ukraine did not have a modern cybersecurity system, including the lack of the necessary institutions for crisis-responses mechanisms. In 2016, the first Cyber Security Strategy was approved to align with the EU cyber security standards and strengthen the security of private enterprises and the state of critical information infrastructure (CII). [47] In June 2021, the new Cyber Security Strategy was presented by the National Security and Defence Council. It included regulations of all the cybersecurity

---

[42] Thierry Tardy, EU-NATO relationship: Cooperation and competition, Anadolu Agency, 18.07.2023, https://www.aa.com.tr/en/analysis/opinion-eu-nato-relationship-cooperation-and-competition/2948527

[43] Baris Celik, Ukraine war is blurring the lines between Nato and the EU on defence policy, 1.03.2023, The Conversation, https://theconversation.com/ukraine-war-is-blurring-the-lines-between-nato-and-the-eu-on-defence-policy-200849

[44]Mykhailo Fedorov, Ukraine's vibrant tech ecosystem is a secret weapon in the war with Russia, Atlantic Council, 17.08.2023, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-vibrant-tech-ecosystem-is-a-secret-weapon-in-the-war-with-russia/

[45] TG Chanel of the IT Army of Ukraine, https://t.me/s/itarmyofukraine2022

[46] Brave 1, https://brave1.gov.ua

[47] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", Указ Президента України; 15.03.2016, https://zakon.rada.gov.ua/laws/show/96/2016#Text

systems built within the eight years of cyber resilience and deterrence, where cooperation with NATO and the EU is clearly defined as the priority.[48]

As for the EU, the integration of Ukraine into the EU Digital Single Market with the significant work done since 2018 is already embodied in such practical outcomes as the recognition of Diia.Signature-EU to be used to sign documents or contracts valid in both Ukraine and the EU; inclusion of the roaming in the EU-Ukraine Association Agreement, accession of Ukraine to the Digital Europe Program, but most importantly, update of Ukraine's legislation in the telecommunications, electronic services, and cyber security. In 2017-2018, with TAIEX technical assistance, the EU realised a number of projects to establish a private-public partnership in cybersecurity and to increase the skills of policymakers.[49]

Moreover, just before Russia's invasion, the Lithuanian defence ministry announced the deployment of the EU Cyber Rapid Response Team (CRRT) in Ukraine – a project born from the EU military cooperation.[50] Eight to twelve cybersecurity experts from EU countries like Estonia, Poland, and Romania assist Ukraine's cyber defence in protecting its networks. Last but not least, the EU has provided 29 million euros to increase Ukraine's cyber and digital resilience. Out of this, 10 million euros was used for cyber security equipment, software, and other related support, while 19 million euros was used to support resilient digital transformation.[51]

The EU Advisory Mission of Ukraine has provided training assistance to Ukrainian security services and was the platform for discussing law practices in the Ukrainian cyber domain. Recognising Ukraine's unique experience of resilience against Russian cyber-attacks, since 2021, the EU and Ukraine have conducted a Cyber Dialogue on mutual cooperation. Further EU support to Ukraine has been provided in line with the implementation of the Cyber Security Strategy and the harmonisation with the EU Cybersecurity legislation – NIS and NIS2 Directives and the recent Cyber Resilience Act and Cyber Solidarity Acts. In the coming 3rd Cyber Dialogue, Ukraine needs to continue discussing further support of the regulation harmonisation and the outlined goals in the Plan on the realisation of the Strategy of the Foreign Policy Ukraine – joining the PESCO projects and stronger cooperation with ENISA.[52]

As for NATO, in 2014, two Trust funds were launched dedicated to cyber and digital spheres – the Command, Control, Communications and Computers (C4) Trust Fund and the Cyber Defence Trust Fund.[53] In practical terms, NATO provided the technical equipment and software for Ukraine within the framework of the first stage of the Trust Fund for the Security Service of Ukraine and other institutions that had to be incorporated into the general infrastructure system. Moreover, the further development of the capabilities of the Trust Fund included the creation of cyber security centres in the system of the Armed Forces of Ukraine and the National Police with their subsequent integration into the national network of situational centres.[54]

---

[48] The working group at the NCCC at the NSDC of Ukraine approved the draft Cybersecurity Strategy of Ukraine, National Security and Defence Council of Ukraine, 4.03.2021, https://www.rnbo.gov.ua/en/Diialnist/4838.html

[49] Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the CyberSphere, Centre for Global Studies "Strategy XXI", 2016, http://www.encouncil.org/wp-content/uploads/2019/10/ENG-Ukraine-EU-NATO-cooperation-to-counter-hybrid-threats-in-cyber-sphere.pdf

[50] Ukraine: EU deploys cyber rapid-response team, BBC, 22.02.2022, https://www.bbc.com/news/technology-60484979

[51] Ukraine and EU held the second round of the UA-EU Cybersecurity Dialogue, EEAS, 29.09.2022, https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en

[52] Про затвердження плану дій з реалізації Стратегії зовнішньополітичної діяльності України, Cabinet of Ministers of Ukraine, 18.04.2023, https://zakon.rada.gov.ua/laws/show/327-2023-%25D1%2580%23Text

[53] NATO-Ukraine Trust Funds, NATO official website, 1.09.2022, https://www.nato.int/cps/en/natolive/topics_153288.htm

[54] У Києві підписали договір про постачання обладнання НАТО для кіберзахисту, Ukrinform, 04.07.2017, https://www.ukrinform.ua/rubric-society/2259204-u-kievi-pidpisali-dogovir-pro-postacanna-obladnanna-nato-dla-kiberzahistu.html

In 2017, NATO committed to help Ukraine improve its cyber security after a large-scale cyber-attack that paralysed the computer networks of ministries, banks, enterprises, and media across the country while Secretary General Jens Stoltenberg announced the creation of a special fund to assist Ukraine in strengthening its defence against cyber-attacks.[55] On 17 January 2022, the NATO Communications and Information Agency (NCI Agency) and Ukraine signed a renewed Memorandum of Agreement to continue their work together on technology-related projects.[56]

Cyber policy has been part of the Annual National Programs (ANP) for Ukraine. ANP 2021[57] stated the need for Ukraine to increase the cyber defence of the Ministry of Internal Affairs, implementation of the regulatory acts for increasing cyber resilience, roll-out the training system for the cyber specialists and a number of other points.

The first months of the full-fledged war demonstrated that NATO and the European Union continued to walk the tightrope between helping Ukraine defend itself and avoiding escalation into a direct conflict with Russia. NATO allies committed to provide Ukraine with more defensive weapons, plus new "cybersecurity assistance" and "equipment to help Ukraine protect against biological, chemical, radiological, and nuclear threats." The European Union agreed to double its support to the Ukrainian Armed Forces through the European Peace Facility to one billion euro.[58]

However, in the course of the war, this shared vision of initial priorities blurred, and the EU has continued acting beyond its historical division of labour with NATO, according to which the EU would deal with civilian aspects of the conflicts and leave military matters to the Alliance. For instance, the EU has mobilised its European Peace Facility to provide 3.6 billion euro in support of Ukraine's armed forces, trained by the EU Military Assistance Mission (EUMAM). There has also been an increased awareness within the EU of the need for stronger defence capabilities, increased defence expenditures, collaborative defence procurement and dealing with strategic shortfalls in an environment of hybrid warfare where large-scale conventional armies are accompanied by more mobile forces and modern technologies[59].

In February 2023, The European Union, NATO, and Ukraine held their first-ever meeting in a trilateral format, where the sides discussed ways to improve the weapons and ammunition procurement system to continue support of Ukraine.[60] For the time being, security and military support, first of all, weapons and ammunition supply, have remained the main focus of trilateral cooperation.

At the same time, a higher level of defence cooperation is difficult to achieve without a formal agreement on how to share classified information. While the EoP status of Ukraine opened certain windows of opportunity, the total access is still limited due to the non-member status and war. Also, the compatibility between the NATO Defence Planning Process (NDPP) and the EU's Capability

---

[55] Roland Oliphant and Cara McGoogan, Nato warns cyber attacks 'could trigger Article 5' as world reels from Ukraine hack, The Telegraph, 28.06.2017, https://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransomware-attack-cripples/

[56] NATO Agency and Ukraine reaffirm commitment to technical cooperation, NCIA, 17.01.2022, https://www.ncia.nato.int/about-us/newsroom/nato-agency-and-ukraine-reaffirm-commitment-to-technical-cooperation.html

[57] Annual National Programme Ukraine-NATO 2021, Decree of the President of Ukraine, 11.05.2021, https://www.president.gov.ua/documents/1892021-38845

[58] Sean Monaghan and Pierre Morcos, NATO and the European Union Show Unity and Resolve in Brussels, CSIS, 29.03.2022, https://www.csis.org/analysis/nato-and-european-union-show-unity-and-resolve-brussels

[59] Baris Celik, Ukraine war is blurring the lines between Nato and the EU on defence policy, 1.03.2023, The Conversation, https://theconversation.com/ukraine-war-is-blurring-the-lines-between-nato-and-the-eu-on-defence-policy-200849

[60] EU, NATO and Ukraine discuss procurement of arms and ammunition in first trilateral meeting, EU NeighborsEast, 23.02.2023, https://euneighbourseast.eu/news/latest-news/eu-nato-and-ukraine-discuss-procurement-of-arms-and-ammunition-in-first-trilateral-meeting/

Development Plan (CDP) remains a source of contention[61] for organisations themselves, thus affecting interaction with their respective partners on the issue.

Russia's military aggression against Ukraine has confirmed the urgent need to substantially enhance the armed forces' military mobility. Such a "military Schengen" had been under consideration even pre-war. However, in 2022-2023, this question again gets a top priority. The necessity to deliver weapons and machinery to Ukraine, resulted in the organisation of a unique logistical process, hence raising the question of who should be in charge: the EU, under which transport and borders sphere are, or NATO, which is in charge of military supply. The EU declared that they would strengthen dual-use transport infrastructure across the trans-European transport network in order to promote rapid and seamless movement of military personnel, materiel and equipment for operational deployments and exercises, working in close cooperation with NATO and other partners. They also aimed to agree on new commitments to accelerate and harmonise cross-border procedures, identify ways to sustain short-notice large-scale movements, invest in the digitalisation of armed forces and develop cutting-edge, energy-efficient capabilities that guarantee the ability to respond quickly and operate in non-permissive environments, taking into account the constitutional requirements of certain Member States.[62]

[61] Jan Joel Andersson, European Defence Partnerships, Brief #3, EUISS, February 2023

[62] A Strategic Compass for Security and Defence, 21.03.2022, https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

Possible directions of cooperation

The following is the list of actions (measures) proposed in the respective 2016[63] and 2017[64] sets of proposals on the implementation of the Joint EU-NATO Declarations. It excludes those concrete actions, such as organising specific exercises in 2017 or 2018, and concentrates on those with a long-term implementation period, thus opening perspectives for Ukraine's involvement.

	Endorsed measure	**Ukraine possible participation**
	1. Countering hybrid threats	
1	Encourage participation by EU and NATO as well as EU Members States and NATO Allies in the work of the "European Centre for Countering Hybrid Threats."	Ukraine had different cooperation formats with Hybrid CoE, however, a full membership should be considered similar to membership in Energy CoE.
2	Staff-to-staff sharing of time critical information between the EU Hybrid Fusion Cell and the relevant NATO counterpart, including by exchanging the analysis of potential hybrid threats.	Considering the complexity of the Russian and Chinese attacks, which often cover both Ukraine and the member states, and Ukraine's EOP status, a coordination mechanism for sharing information should be established.
3	Intensify cooperation and undertake shared trend analysis of misinformation, including through social media targeting the EU and NATO.	Ukraine can join such efforts as the previous research demonstrated an often interdependence and interconnection of misinformation campaigns targeted against Ukraine and member-states.
4	Enhance mutually reinforcing efforts regarding support for stratcom capabilities of partner countries, including through coordinated or joint trainings and sharing of platforms.	Ukraine can join efforts providing cases, lessons and trainers, as its experience can be useful for other NATO and EU partners around the globe.
5	Encourage cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS Stratcom division (specifically task forces East and South), including further joint trainings/seminars.	Ukrainian experts can be added as advisors to both centres, considering that a lot of disinformation is currently connected to Ukraine's issues.

[63] Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 06.12.2016, https://www.nato.int/cps/en/natohq/official_texts_138829.htm?selectedLocale=en

[64] Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, 05.12.2017, https://www.nato.int/cps/en/natohq/official_texts_149522.htm

6	Enhance preparedness, inter alia, by holding regular meetings at staff-to-staff level.	Candidate states can be invited on an ad hoc basis.
7	Bearing in mind the EU's crisis response procedures, including the Integrated Political Crisis Response arrangements (IPCR) and NATO's Crisis Response System, seek to synchronise the two organisations' parallel crisis response activities with the goal of providing coherent support in response to hybrid threats.	Considering Ukraine's experience and lessons learnt on hybrid threats response, as well as the previously developed NATO-Ukraine Platform on Countering Hybrid Warfare, it can be widened to the EU-NATO-Ukraine format.
8	Staff contacts will be intensified, including cross-briefings to respective bodies on resilience requirements.	See previous
9	Assess requirements, establish criteria and develop guidelines in the context of greater coherence between the EU Capability Development Plan (CDP) and the NATO Defence Planning Process (NDPP).	n/a
10	Intensify relations among actors at staff level engaged in countering hybrid threats and strengthen cooperation, including: In developing their approaches to operate in the domain of Publicly Available Information including processes and tools of collecting, analysing, and disseminating as well as exchanging of unclassified products.	Candidate states can be invited on an ad hoc basis.
11	Strengthen cooperation at staff level on threat assessments, including terrorism, emanating from the South and the East; Consider contributions by the NATO Hub for the South, as appropriate.	Considering the interdependence of the Ukrainian and Syrian fronts for Russian activities, Ukraine can be involved ad hoc.
12	Examine possibilities to regularly exchange information between EU and NATO staffs, including relevant Agencies, on countering terrorist threats.	n/a
13	Map and analyse, by 2018, gender indicators in early warning systems/analysis, including those indicators that could improve situational awareness and preparedness, in support of UNSCR 1325 (2000).	Having experience of NATO and the EU and respective Ukraine's national plan for UNSCR 1325, the same analysis can be done for Ukraine.
14	Coordinate strategic communications messaging on security threats where appropriate, including terrorism related issues.	As Russian propaganda is often aimed simultaneously at Ukraine and its partners, some messages' coordination should include both member-states and partner and candidate states.

15	Strengthen staff-to-staff cooperation on civil preparedness, including risk assessments, medical evacuation (MEDEVAC), mass casualty incidents, and population movement.	These points are within the resilience concept, where Ukraine and NATO already had a joint exercise and which is included in bilateral tracks between Ukraine and organisations.
16	Develop a programme of staff-to-staff scenario-based discussions and workshops designed to promote mutual understanding of hybrid crisis management, in line with the respective playbook/operational protocol, as well as the implications on capability development.	Ukraine can join such tabletop exercises, sharing experience of the existing protocols or real situations response.
17	The European Centre of Excellence for Countering Hybrid Threats could facilitate scenario-based discussions, workshops and exercises.	Ukraine is already in cooperation with the Centre.
18	NATO and the EU staffs to map their civil preparedness efforts between NATO's Resilience Baselines and the EU's Prevention and Preparedness work-streams.	n/a
19	Building on established practice and applied procedures, explore the inclusion, where appropriate, of EU staff in the NATO Resilience Advisory Support Teams and other assistance teams and NATO staff in relevant EU advisory prevention and preparedness missions conducted under the Union Civil Protection Mechanism.	Ukraine can be invited into such teams upon the agreement of the receiving states.
	2. Operational cooperation, including maritime issues	
20	By December 2016, enhance cooperation and coordination between Operation Sea Guardian and EU NAVFOR MED Sophia in the Mediterranean.	n/a
21	Building upon synergies between the EU operation and NATO in the Aegean, NATO and EU will study opportunities, in the first semester of 2017, for further maritime cooperation between them.	Ukraine should promote the idea of such NATO-EU cooperation spreading to the Black Sea.
22	In support of the above goals, EU and NATO will continue to make full use of the mechanism on Shared Awareness and De-confliction in the Mediterranean (SHADE MED).	n/a

23	Compile during the first semester of 2017 an overview of relevant maritime exercises by respective organisations with a view to identifying further opportunities for possible interaction.	n/a
24	Increase the frequency of meetings with partners participating in respective operations.	Ukraine has experience participating in maritime operations under the EU and NATO auspices, so despite the inability to continue full participation, it can still be involved at the level of the military representatives in Brussels.
25	Building on experience in the Mediterranean Sea and the Horn of Africa explore further possibilities for mutual logistical support and information sharing between staffs on operational activities, including on irregular migration, when the EU and NATO consider or conduct activities in the same theatres. In addition, consider further possibilities for maritime cooperation.	Ukraine should promote the idea of such NATO-EU cooperation spreading to the Black Sea, as well as sharing experiences of the Black Sea activities and Russian actions in the region that can be used as lessons learned for other regions.
	3. Cyber security and defence	
26	EU and NATO will exchange concepts on the integration of cyber defence aspects into planning and conduct of respective missions and operations to foster interoperability in cyber defence requirements and standards.	Building upon the NATO Trust Fund on cyber security and Ukrainian experience in countering cyber threats, a trilateral experience exchange and regular consultations can be established.
27	In order to strengthen cooperation on training, as of 2017, EU and NATO will harmonise training requirements, where applicable, and open respective training courses for mutual staff participation.	Partner states and candidates should be invited to such training.
28	Foster Cyber Defence Research and Technology Innovation cooperation… EU and NATO will enhance interoperability in cyber defence standards by involving industry where relevant.	Considering the last nine years' increased capacity of the Ukrainian IT sector, in particular, in the defence sector, Ukraine may be invited to such cooperation.
29	Strengthen cooperation in cyber exercises through reciprocal staff participation in respective exercises.	Partner states and candidates should be invited to such training.

30	Exchange between staffs relevant good practices concerning the cyber aspects and implications of crisis management and response, as well as operational aspects of cyber defence, such as analysis of threats and malware information.	See previous points.
	4. Defence capabilities	
31	Pursue coherence of output between the NATO Defence Planning Process and the EU Capability Development Plan through staff to staff contacts.	n/a
32	Seek to ensure that capabilities developed multinationally by Allies and Member States are available for both NATO and EU operations.	n/a
33	Pursue complementarity of multinational projects/programmes developed within NATO Smart Defence and EU Pooling & Sharing, in areas of common interest, such as air-to-air refuelling, air transport, satellite communications, cyber defence and Remotely Piloted Aircraft Systems.	Ukraine should be considered as a possible participant in the smart defence projects, in particular in the North-West of the Black Sea.
34	Further contribute to the coherence of multinational efforts, by reflecting multinational projects developed in an EU context, as relevant, in the capability roadmaps supporting NATO defence planning priorities, and by taking into account multinational projects developed in a NATO context in deriving Priority Actions in the framework of the EU's Capability Development Plan.	n/a
35	Continue closer cooperation between NATO and EU/EDA experts in the field of Military Aviation with a view to ensuring complementary efforts in the interest of defence and security in Europe especially as regards the development of a Military Aviation Strategy, the implementation of Military Airworthiness arrangements, Remotely Piloted Aircraft Systems Air Traffic Integration, Aviation security including cyber, as well as civil initiatives, such as SES/SESAR.	Considering Ukraine's participation in SALIS and intensive use of UAV, Ukraine may be included in the ad hoc consultations.
36	Enhance interoperability through increased interaction on standardisation.	EU and NATO should develop a single list of standardisations available for Ukraine that can be integrated into the accession process and updated ANP.

37	Establish cooperation and consultation at staff level, through regular meetings, in military mobility in all domains (land, maritime, air) to ensure a coherent approach and synergies between the EU and NATO.	The issue of military mobility intensified since 2022 due to the necessity to deliver military aid for Ukraine as well as enhance Eastern flank defence, so the trilateral consultations may be regularly held on lessons learnt and experience sharing.
38	Ensure coherence of output between the Coordinated Annual Review of Defence (CARD) and respective NATO processes (such as the NATO Defence Planning Process) ….	n/a
	5. Defence industry and research	
39	Further develop a dialogue between EU and NATO staff on industrial aspects using existing fora.	Considering that the first EU and NATO member states companies have opened their offices or manufacturing in Ukraine, Kyiv should be included in such a trialogue.
40	Enhance cooperation at staff level on defence-related R&T in common areas of interest.	
	6. Exercises	
41	NATO or EU staff experts of the non-leading organisation for the respective years to be invited to contribute to the planning and conduct of the leading organisation's exercise, in a spirit of reciprocity.	n/a
42	Lessons and recommendations to be shared to the extent possible.	As Ukraine has participated in numerous NATO-led exercises, continued to be trained by NATO and EU representatives, as well as has a unique combat experience, it can be invited in different formats to both joint trilateral exercises or lessons and recommendations sharing formats.
43	Complement training and education inter alia through invitations to each other's staff to appropriate events (e.g. workshops, presentations, exercises).	See above.
44	NATO will, as of 2017, continue to invite the EU (EEAS and European Commission) to participate in observing its military exercises. The EU will reciprocate accordingly.	n/a

45	Based on the experience of the respective EU and NATO exercises in hybrid and cyber contexts, develop and roll-out, starting in 2018, a set of common training and exercise modules, be it stand alone or integrated in the scenarios of wider exercises and training formats, to provide coherent training to respective personnel.	See above.
46	Enhance staff-to-staff interaction, as appropriate, in the framework of relevant NATO and EU disaster response exercises.	n/a
47	Establish a staff-to-staff dialogue to explore the possibility to conduct detailed scenario-based discussions on fighting terrorism for staff training purposes.	See above.
	7. Defence and security capacity-building	
48	NATO and EU staffs will foster cooperation, including on the ground, on building partners' capacity and resilience, in particular in the Western Balkans, the Eastern and Southern Neighbourhoods, including Georgia, Republic of Moldova, Ukraine, Jordan, Morocco and Tunisia.	A direct reference to Ukraine.
49	Encourage cooperation and exchange of expertise through respective Centres of Excellence and other relevant training activities and programmes in support of partners.	Ukraine already participates in several CoEs and is in the process of negotiations regarding joining others.
50	Identify possibilities for EU and NATO to participate in their respective projects and practical partnership programmes.	NATO-EU consultation format can take place in Ukraine regarding PDP and EUMAM priorities
51	Ensure complementarity of maritime capacity building efforts..	This should involve more active participation and planning in the Black Sea.
52	Exchange information about the security situation in Eastern and Southern partner countries, as well as Iraq and Libya and the Western Balkans, as well as on how to support those countries and relevant international organisations.	This process regarding Ukraine intensified since 2022.
53	Coordinate the support to building the capacities of partners to counter CBRN, cyber and terrorist threats.	This is already happening due to the Russian aggression in Ukraine.

54	Foster cooperation on gender and WPS related aspects in building partners' capacity in areas as appropriate in support of UNSCR 1325 (2000).	Ukraine should intensify the implementation of 1325 and coordinate its national implementation plans according to the goals of the EU and NATO membership.

Ukraine faces a difficult choice. Should it differentiate two organisations, cooperation with them and commitments, thus utilising those spheres which will be the best to develop with each, or aim to establish triangle relations, using complementarily and uniting efforts of both organisations towards Ukraine? The second approach will need a clear set of spheres where both organisations' activities overlap, requirements for membership coincide, but also where establishing the Trilateral coordination mechanismis possible. The last doesn't mean rejection from the Association Council or NATO-Ukraine Council. It means a separate coordination body allowing regular and focused dialogue. Such spheres as resilience building, maritime security, climate influence on security, innovations, disinformation and cyber security, military mobility, Women, peace and security agenda can be a priority for the trilateral dialogue.

In preparation for the new Adapted Annual National Programme, Ukraine should consider the spheres already stressed in candidate negotiations with the EU and emphasise the necessity of coordination regarding good governance, anti-corruption work, and other spheres present in both organisations' requirements for membership. Ukraine should avoid two parallel reporting and implementation mechanisms in the framework of the integration process requirements in the spheres of NATO and EU priority. Within the adapted ANP, Ukraine should concentrate on reforms in defence and security sectors that are important for reaching interoperability with Alliances forces and will facilitate the integration process, thus avoiding duplication with the EU integration agenda.

Also, it should be considered Ukraine joining the NATO Innovation Fund and later a newly established Defence Innovation Accelerator that will allow for the bringing together of governments, the private sector, and academia to bolster the technological edge, as well as other projects aimed for increased security and innovation readiness. Within the established NATO-Ukraine Council, Ukraine needs to build a system of cooperation on cyber security that will not be limited only to the training and exchange of experience but will also include the discussion on the specific instruments of cooperation – like the exchange of the operative information, financial assistance, and the help with the further modernisation of the regulatory setting in Ukraine.

The cyber domain has long since become the priority for the EU and NATO. The risks posed by the cyber-attacks and the new risks coming from the development and application of technologies, especially in the military, dictate a necessity for capabilities and partnership development. Ukraine, being in the cyber war with Russia, is a constant target of cyber-attacks and attacks on critical infrastructure. Along with developing its own capabilities in cyber defence and cyber offence, cooperation with the EU and NATO has been crucial since 2014 for the general protection and modernisation of the cyber security ecosystem along with the ongoing digitalisation resulting in the existing resilience. In the context of European and Euro-Atlantic integration, Ukraine needs to continue with the partners' support to harmonise its own legislation with the EU files and NATO standards. In this regard, Ukraine needs to clearly identify the needs and requests to be sent to the partners after conducting the cyber audits of the governmental institutions.

The EU-NATO Structured Dialogue on Resilience is an opportunity for the engagement of Ukraine. As the Assessment report stated, "Ukraine's example has both proven that it is possible to withstand even large-scale attacks and underscored how important resilient critical infrastructure and the continued

provision of essential services are to a country's ability and determination to defend itself".[65] The second sphere where Ukraine can engage as a partner for both organisations is the area of emerging technologies. While the EU and NATO step by step roll out their programs, including the discussion on the support of military innovations and deep tech standards, Ukraine, since the start of the full-scale invasion, actively worked on this dimension that proves at the battlefield.

Considering the growing need and initiatives for cooperation between the EU and NATO, Ukraine is to find its place in such a triangle, complementing its experience in addition to regular training and exercise. In the digital and cyber domain, Ukraine has become not only a "rule-taker" but can share the unique practical experience and the knowledge of working in the emergency setting that is of interest to the EU and NATO, especially in the case of the protection of critical infrastructure. With the view to the existing nexus and win-win cooperation, Ukraine needs to have a regular platform for discussions with both the EU and NATO on cyber security that can be embodied in the EU-NATO-Ukraine Cyber Dialogues.

NATO Washington summit in 2024 opens an opportunity for the Trilateral declaration development that may encompass 1) joint efforts on Ukrainian integration, where the shared priorities for reforms or harmonisation of legislation and processes can be identified; 2) perspective spheres of cooperation that can be enhanced independently from the integration dialogue and already included in practical trilateral cooperation.

[65] EU-NATO Task Force on The Resilience of Critical Infrastructure. Final Assessment Report, June 2023, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

POLICY PAPER

EU, NATO AND UKRAINE

DREAM TEAM OR A TRIANGLE?

UKRAINIAN PRISM
www.prismua.org
info@prismua.org
+38093 57 88 405