January 2023

How Sweden Can Use its EU Presidency to Build the Civilian Security Dimension of the Eastern Partnership

Michal Baranowski, Mikołaj Bronert, Maximilian Kaminski, and Elene Kintsurashvili

The EU's Eastern Partnership (EaP) lacks a security dimension and this is an urgent reform need. In particular, the EU should become the leading provider of civilian security support in the EaP countries, particularly Ukraine. But significant weaknesses in this policy field inhibit its capability to do so.

Sweden's long-term focus on the EaP, its experience in augmenting domestic cyber and hybrid resilience as well as in placing the civilian aspect at the heart of its national security, and it its leading contribution to the EU's Common Security and Defense Policy (CSDP) missions put it in a unique position to be a champion of the security dimension of the EaP during its presidency of the Council of the EU.

Sweden can do so by pushing for: a EU-NATO memorandum of understanding on the EaP; the provision of a rapid financing mechanism to assist EaP countries in nonmilitary defense; a more coordinated training, planning, and implementing process for CSDP missions between EU actors and the EaP countries; a more targeted approach towards EaP countries; and prioritization of deepening of cooperation with EaP countries in the domain of hybrid threats.

GMF
Ideas.
Leadership.
Hope.

75 The Marshall Plan 1947–1951
GMF 50

Introduction

Since its establishment over a decade ago, the European Union's Eastern Partnership (EaP) evolved dynamically, resulting in mismatched outcomes given that one size did not fit all of the six partner countries. Progress has been clearest with the "Associated Trio" of Georgia, Moldova, and Ukraine, which have signed Association Agreements, including Deep and Comprehensive Free Trade Areas, with the EU. After Russia's full invasion of Ukraine in February 2022, Kyiv applied for a fast-track EU membership, followed by Chisinau and Tbilisi. As a result, the EU granted Moldova and Ukraine candidate status and stated that Georgia had a "European perspective."

There has been no similar progress in EU integration for the three other EaP countries. A combination of close ties with and constant pressure from Russia have prevented Armenia from moving forward successfully with its European agenda. There is no interest from Azerbaijan in advancing the negotiations on a new framework agreement with the EU. The dictatorial regime in Minsk suspended Belarus's participation in the EaP in 2021.

Despite the achievements of the Associated Trio, the EaP lacks a security dimension.

Despite the achievements of the Associated Trio, the EaP lacks a security dimension. Given the war in Ukraine, developing this must now be the most important topic when it comes to reforming the EaP. And strong security as well as humanitarian and civilian support will be instrumental to Ukraine's reconstruction and European integration once it has repelled Russia's invasion.

Sweden was one of the early champions of the EaP and it is a trusted partner of countries in Eastern and Western Europe alike. This puts it in a unique position to push this part of the EaP agenda forward during its presidency of the Council of the EU in the first half of 2023. It is one of the largest bilateral donors to Eastern Europe, and it has shifted a large portion of its funds to become one of the largest donors of humanitarian and development aid to Ukraine. In December 2021, the Swedish government approved a strategy for reform cooperation with Eastern Europe for 2021–2027 with a budget of approximately €600 million. Since February 2022, Sweden has more than doubled its support to Ukraine in the military, humanitarian, and reconstruction fields, for reforms, and through financial guarantees and civilian operations.

Sweden's experience of being highly integrated in Western political and defense structures while not being a NATO member offers a potential model that EaP countries could emulate in the long run in a best-case scenario. The country has been very active in EU missions and operations, including every military and civilian mission under the Common Security and Defense Policy (CSDP). Sweden was also instrumental in establishing the civilian component of the CSDP. Its security objectives at home have also been centered around civilian defense and preparedness, making an ideal actor to advance the discussion on this dimension of the EaP.

The EaP and the CSDP

The European Council declared in 2015 that the political, economic, and security stabilization of the EU's eastern neighbors would be a priority, given that an unsecured neighborhood poses a threat to its security. It was thus decided to strengthen the security dimension of the EaP, linking it with the CSDP civilian tools.[1] The EU has worked within the scope of the CSDP and bilaterally to provide the six EaP countries support regarding hybrid threats and strengthening civil society, but the war in Ukraine has made clear that it needs to step up its security support. In June 2022, the European Parliament adopted a resolution on security in the EaP calling on the EU "to expand support mechanisms for the further participation of the EaP countries in CSDP civilian and military missions and operations."[2]

The EU's engagement in civilian crisis management and security beyond its borders is addressed predominantly through CSDP missions. Their goals are usually limited to reinforcing the police, the rule of law, and the civil adminis-

1 Council of the European Union, Joint Declaration of the Eastern Partnership Summit, December 15, 2021, p. 15

2 European Parliament, Security in the Eastern Partnership area and the role of the common security and defence policy, June 8, 2022, p. 24

tration in fragile and conflict settings.[3] However, the interest of member states in these endeavors has been declining. Between 2010 and 2018, the number of EU staff deployed to CSDP missions nearly halved.[4] Applied command structures also differ across CSDP operations.

The CSDP's institutional framework and capabilities are attempting to respond to the growing saliency of cyber and hybrid threats. In 2018, the member states signed the Civilian CSDP Compact, urging the EU to take actions in the hybrid and cyber spheres.[5] There are also ten Permanent Structured Cooperation (PESCO) projects focused on increasing the capacity of member states to combat cyber threats.[6] Since 2020, third countries, including Ukraine, can take part in PESCO projects.[7] There is now a Hybrid Fusion Cell operating within the EU Intelligence and Situation Centre, under the European External Action Service (EEAS).[8] In approving the EU's Strategic Compass in 2022, the member states endorsed the development of a Hybrid Toolbox, a Cyber Diplomacy Toolbox, and a Foreign Information Manipulation and Interference Toolbox.[9]

The CSDP is only one of three pillars of the EU civilian security system.[10] The European Commission is another, most notably through the European Union Agency for Network and Information Security (ENISA). The agency's salience has grown since the adoption of the Cybersecurity Act in 2019, which strengthened its mandate, staff, and financial capabilities. However, ENISA does not conduct activities beyond the EU's borders.[11] The third pillar consists of the agencies of the Justice and Home Affairs Council (JHA)—which brings together the justice and home affairs ministers of all member states—that deal with hybrid interference externally. Among these, the European Border and Coast Guard Agency (Frontex) plays a growing role. Thus, the EU's reaction to civilian, hybrid, and cyber threats is fragmented, and its institutional setting does not respond well to the growing domestic/external threat nexus.

Supporting Resilience in Ukraine

To enhance Ukraine's resilience, as outlined in their 23rd summit joint statement in 2021, the EU committed to contributing to "countering cyber and hybrid threats in addition to tackling disinformation campaigns."[12] The country has been a target of Russian information warfare "from the onset of the 'Euromaidan' demonstrations" in 2013.[13] It has experienced an increase in cyberattacks causing power cuts, damaging the internal networks of state institutions, and undermining crucial infrastructure. Given that electronic warfare has become the "backbone" of Russian military strategy,[14] the EU has done a great deal to make Ukraine cyber-resilient. As a member of the EaP, Ukraine is a part of the Cybersecurity East Project, which aims at strengthening cybersecurity governance.[15] In 2021, the EU established a Cyber Dialogue with Ukraine "to bolster cyber resilience and advance responsible state behaviour in cyberspace."[16] Under this project, an EaP delegation held a meeting with the European Union Agency for Cybersecurity in October 2022 to

3 Thierry Tardy, Quo Vadis Civilian CSDP?, Center for International Peace Operations, February 2018.

4 Timo Smit, Increasing Member States Contributions to EU Civilian CSDP Missions, Stockholm International Peace Research Institute, November 2020.

5 Council of the European Union, Civilian Common Security and Defence Policy: EU strengthens its capacities to act, November 19, 2018.

6 PESCO, Projects, 2022.

7 Council of the European Union, Council Decision establishing the general conditions under which third States could exceptionally be invited to participate in individual PESCO projects, October 27, 2020, p. 3.

8 NATO Cooperative Cyber Defence Centre of Excellence, EU Policy on Fighting Hybrid Threats, 2022.

9 Council of the European Union, A Strategic Compass for a stronger EU security and defence in the next decade, March 21, 2022.

10 Tardy, Quo Vadis Civilian CSDP?

11 European Commission, Cybersecurity Policies.

12 Jakub Przetacznik with Linda Tothova, EU-Ukraine relations and the security situation in the country, European Parliament, February 2022.

13 Margarita Jaitner, "Russian Information Warfare: Lessons from Ukraine," in Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO Cooperative Cyber Defence Centre of Excellence, 2015

14 Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable, Eurasia Daily Monitor, May 24, 2017.

15 EU4Digital, EU4Digital: Cybersecurity East

16 European External Action Service, Cyberspace: EU and Ukraine launch dialogue on cyber security, June 3, 2021.

assess the country's current cyber threat landscape.[17] Since February 2022, the EU has contributed to Ukraine's cyber resilience with €10 million for equipment, software, and other related support and €15 million to support resilient digital transformation.[18] However, the majority of EU countries have not established bilateral relations with Ukraine's military intelligence services, making the country's fight against cyberattacks and hybrid threats less effective.[19]

The EU is also contributing to Ukraine's civilian security sector through its advisory mission (EUAM) established in 2014 after the Revolution of Dignity "to expedite [the country's] sustainable reform."[20] As a civilian CSDP mission, EUAM's mandate includes de-oligarchization, good governance, the rule of law, and the fight against corruption.[21] The border assistance mission to Moldova and Ukraine (EUBAM) aims at promoting economic development and enhancing regional security.[22]

The EU perceives both missions as successful but there are gaps in their mandates. There is a mismatch between Ukraine's expectations and the mandates of the missions. This is clear in the case of the EUAM. First, Ukraine had repeatedly asked for a monitoring mission but instead received an advisory one. Second, as one study found, the country's "institutions were excluded from the formulation of the mission's mandate and only got to know that the mandate concerned them once the EUAM was already in place."[23] Third, Ukraine and the EU have had different views of which agencies belong to the security sector and thus that have to be reformed, which has created friction between the EUAM team and Ukrainian officials.[24] When it comes to support for civilian security, the EUAM faces fundamental operational challenges. The sector is bureaucratic, affected by the strong presence of oligarchs, and characterized by an unclear division between the military and civilian sectors. Despite these challenges, however, it seems that with time the EUAM has been able to adjust to the different needs and difficulties, and helped Ukrainian people regain trust in the state.

Hybrid and Cyber Threats

The launch of the European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine) in October 2022[25] addressed the needs the country has been articulating since 2014, but its mandate lacks a clear hybrid and cyber dimension. The salience of hybrid and cyber threats has been underlined in numerous EU papers and communications, yet there are still no specific roadmaps or "mini-concepts" for solutions within CSDP missions and operations planning.[26] Moreover, the EU Military Staff cannot provide or deploy any operational cyber capabilities, as these must be requested from the member states. Therefore, planning and operationalizing measures against hybrid and cyber threats is insufficient.[27] Even at the training level, the courses provided by the European Security and Defense College, which teach strategic planning processes for civilian missions, do not focus much on cyber elements.[28]

In fact, the EU's institutional framework related to these matters is highly fragmented between the CSDP, the JHA, the European Council, and the European Commission. For example, there is no institutionalized process of JHA actors

17 European Union Agency for Cybersecurity, International Cooperation: ENISA Welcomes EU Eastern Partnership Delegation for a Study Visit to its Headquarters, October 4, 2022.

18 European Commission, EU assistance to Ukraine.

19 Gustav Gressel, In Europe's Defence: Why the EU needs a security compact with Ukraine, European Council on Foreign Relations, September 20, 2022.

20 EUAM Ukraine, About us, 2022.

21 EUAM Ukraine, Our Priorities, 2022.

22 EUBAM Moldova and Ukraine, Who we are, 2022.

23 Kateryna Zarembo, Perceptions of CSDP effectiveness in Ukraine: a host state perspective, European Security, February 20, 2017.

24 Tracey German and Andriy Tyushka, Security challenges at the EU's eastern border: which role for CSDP?, Directorate General for External Policies of the European Union, January 2022, p. 25.

25 Council of the European Union, Ukraine: EU sets up a military assistance mission to further support the Ukrainian Armed Forces, October 17, 2022.

26 Stefanie Mavrakou, The Internal - External Security Nexus: A contribution to a better understanding and operationalisation of cooperation between civilian CSDP and JHA, European Centre of Excellence for Civilian Crisis Management, November, 2021, p. 21.

27 Federal Ministry of Defence of the Republic of Austria, Handbook on CSDP, 2021, p. 129.

28 European Security and Defence College, Strategic Planning Processes for Civilian Missions Course, July 11-15, 2022, Brussels, July 18, 2022.

being involved in the planning of CSDP actions, missions, and operations. JHA staff are not integrated into mission personnel. CSDP staff have little knowledge of JHA activities and vice versa as there is a scarcity of crosscutting training for both sides, which results in them operating in silos.[29] This concern is also shared by the European Council conclusions from December 2022, calling for "a renewed impetus towards the civilian Common Security and Defence Policy". In this, the council said it will aim to strengthen the "internal-external security nexus through increased cooperation between civilian CSDP and Justice and Home Affairs." The conclusions also call for strengthening resilience to hybrid and cyber threats.[30]

These issues were noted in the November 2022 Joint Communication of the European Commission and the High Representative for Foreign Affairs and Security Policy on an EU Cyber Defense policy and an Action Plan on Military Mobility 2.0. The declaration states that "The EU will reinforce its coordination mechanisms among national and EU cyber defense players, to increase information exchange and cooperation between military and civilian cybersecurity communities, and further support military CSDP missions and operations."[31]

Hybrid threats and cyber resilience are central when it comes to the security of the EaP countries, which have been targets of Russian cyber warfare for some time.[32] For example, Ukraine has long been the object of regular large-scale Russian cyberattacks threatening the stable operation of government information resources and critical infrastructure.[33] According to the Security Service of Ukraine, between the beginning of the invasion in February 2022 and the first half of November, the Cybersecurity Department repelled over 3,500 cyberattacks on state agencies and critical infrastructure.[34]

The EU has responded with financial support for the EaP countries to improve their cyber resilience, including through the Instrument contributing to Stability and Peace and the European Neighbourhood Instrument. With the EU's assistance, all the EaP countries set up cybercrime units and increased their cooperation with Europol, which can be regarded as one of the achievements of civilian CSDP.[35]

Despite the EU's increased engagement, the capacity of the EaP states to successfully counter hybrid attacks on their own is limited.

Nevertheless, if the EU wants to play a greater role in combatting hybrid threats in the EaP countries, more institutionalized security cooperation should be established. For example, officials from Ukraine's State Service of Special Communications and Information Protection's cyber agency have stressed the importance of the country being given the status of ENISA Special Partner, which would make it easier for the country as candidate countries to bring domestic legislation in line with EU standards (the same would apply for Moldova).[36] This would be beneficial to the EU as well, given that there is a lot it can learn from the experience of EaP countries when it comes to facing cyberattacks.[37]

Despite the EU's increased engagement, the capacity of the EaP states to successfully counter hybrid attacks on their own is limited. The reasons for this include a low level of awareness among the public, the use of outdated or non-licensed software, a lack of qualified staff in the national

29 Mavrakou, The Internal - External Security Nexus: A contribution to a better understanding and operationalisation of cooperation between civilian CSDP and JHA, p. 11-14.

30 European Council, Council approves conclusions calling for a renewed impetus towards the civilian Common Security and Defence Policy, December 12, 2022.

31 European Commission, Cyber Defence: EU boosts action against cyber threats, November 10, 2022.

32 Johann Wolfschwenger, The EU's Eastern Partnership between a rock and a hard place, AIES Fokus, September 2020.

33 The Razumkov Centre, The EU-Ukraine Security Partnership: Status and Prospects, Kyiv 2021.

34 Security Service of Ukraine, Russia carries out over 10 cyberattacks on Ukraine's strategic facilities daily – Chief of SSU Cyber Security Department, November 9, 2022.

35 Eastern Partnership Civil Society Forum, EaP Panel on CSDP, Security and Civil Protection, October 2020, November 6, 2020.

36 State Service of Special Communications and Information Protection of Ukraine, Ukraine enhances cooperation with the EU Network and Information Security Agency, October 10, 2022.

37 Elżbieta Kaca, Boosting Cybersecurity Resilience in the Eastern Partnership Region: Options for the EU, Polish Institute of International Affairs, February 25, 2022.

authorities, and weak cooperation between the state and the private sector.[38] As a consequence of their exposure to cyber threats, the private sector and local authorities play a crucial role in this domain, and the EU must include these different stakeholders to build resilience more effectively at all levels in the EaP countries.

The EU and NATO in Ukraine

Russia's war on Ukraine, not least when seen alongside the EU's ambitious goals in the region, shows that EU cannot be the only foreign security actor to support the country. The EU and NATO have been deepening their respective institutional ties with Ukraine. For example, in 2015, the European Defense Agency and the country's Ministry of Defense signed an administrative arrangement for cooperation.[39] In 2020, NATO offered Ukraine the status of Enhanced Opportunity Partner, which provides the country with preferential access to the alliance's interoperability toolbox, including exercises, training, exchange of information, and situational awareness.[40]

The EU and NATO were equally involved in Ukraine before the February 2022 invasion, coming to an informal division of labor. Before the invasion, it was predominantly NATO members—Canada, the United Kingdom, and the United States—that provided training to Ukrainian soldiers in local training centers.[41] This training based on NATO's best standards and practice proved crucial in enabling the Ukrainian army to face down its larger Russian adversary. As soon as the invasion started, EUAM Ukraine shifted all of its funds (about €1.6 million) to provide an emergency support package to its Ukrainian partners, including the police, the security services, war-crimes investigators, border guards, and refugees and the civilian population.[42]

Increased cooperation between EU and NATO in Eastern Europe and their growing commitment to its security environment is a positive development, but this can also cause problems of duplication and lack of synergy. For example, both are committed to improving Ukraine's technical capabilities for resilience against hybrid and cyber threats. NATO does this through its Information and Communication Agency, the NATO Industry Cyber Partnership, and the NATO-Ukraine Trust Fund on Consolidation, Command, Control and Communication.[43] The EU does it through the EU4Digital program[44] or PESCO projects related to cyber and hybrid threats that are now also open to EaP countries. Both institutions target similar goals but they have not yet come to an agreement that would allow them to take full advantage of their respective capabilities and experience while avoiding duplication and ensuring the most effective division of work.

The recently concluded EU Integrated Resolve 2022 exercise and NATO's parallel PACE 2022 Exercise intended to strengthen synergy between both entities. More importantly, Ukrainian troops took part in the latter, making it possible to properly assess needs and capabilities on both sides, based on real-life scenarios.[45]

Sweden's Potential Role

After Brexit, Sweden had to rethink its security and defense policy, which had for long been more closely aligned to that of the United Kingdom rather than to that of the EU institutions. Sweden recognized that there is insufficient political will among the EU member states for deepening joint military capabilities,[46] and that this ambition has to be achieved through NATO. Its application for NATO membership was the final step in cementing Sweden's commitment to the transatlantic alliance and the military obligations that come with it. Sweden has also reiterated that its military spending

38 Ibid.

39 Mission of Ukraine to the European Union, Ukraine-EU cooperation in the military-political, military and military-technical spheres, April 15, 2021.

40 NATO, NATO-Ukraine Relations, February 2022.

41 Gressel, In Europe's defence.

42 EUAM Ukraine, #EUAM4Ukraine: "Now wholly redeployed, EUAM experts continue building resilience with their Ukrainian counterparts", October 7, 2022.

43 Vira Ratsyborinska, EU-NATO and the Eastern Partnership Countries Against Hybrid Threats (2016-2021), National Security and Future, 2022, p.21.

44 EU4Digital, EU4Digital: Cybersecurity East, 2022.

45 European Commission, Hybrid threats: EU concludes EU INTEGRATED RESOLVE 2022 exercise, November 18, 2022.

46 Government Offices of Sweden, Deterioration of the security environment – implications for Sweden, May 13, 2022.

would reach the NATO target of 2 percent of GDP by 2026, two years sooner than previously expected.[47]

For Sweden, however, cooperation in civilian defense and combating hybrid threats, which are crucial pillars in its approach to defense policy, can and should be pursued through existing EU frameworks. In 2021, the previous government underlined that "through the EU, Sweden can make a stronger contribution to peace and security in our neighborhood."[48] As the third-largest contributor of personnel to CSDP civilian missions,[49] it has shaped the CSDP by promoting initiatives such as the Civilian CSDP Compact in 2018 and logistically by building a warehouse in central Sweden that provides the EU with the capacity to deploy all the necessary equipment to start a new 200-strong mission within 30 days.[50]

Sweden is leading light in Europe when it comes to civilian defense and preparedness against hybrid threats.

Sweden is leading light in Europe when it comes to civilian defense and preparedness against hybrid threats. The new government that took office in 2022 made its ambitions in civilian defense clear by shifting responsibility for it from the Ministry of Justice to the Ministry of Defense, and by appointing a special minister for civilian defense.[51] It also wants to increase the country's resilience to hybrid threats and improve its cybersecurity competencies. Both are core areas in building up resilience and crisis management, which has been advocated by Sweden in the development of the EU's Strategic Compass. Furthermore, Sweden has been steadily increasing its investments in civilian and military defense capabilities to match its ambitions.

Because of Russia's aggression in Eastern Europe and the rise of hybrid threats, Sweden has since 2015 worked to increase the resilience of its society and infrastructure. The main institution guiding the efforts in civilian defense is the Civil Contingencies Agency (MSB).[52] Its responsibilities range from civil protection and infrastructure resilience to crisis management and cybersecurity. The MSB's works abroad too, usually under the umbrella of rescEU, a program created by the European Commission for civil protection and disaster management. Sweden's cybersecurity efforts are coordinated through the EU Cybersecurity Competence Center and the National Coordination Centers in every EU member state.[53] Sweden established a cybersecurity center in 2020 to improve coordination between its security agencies such as MSB, the armed forces, and other institutions.[54]

In 2018, Sweden appointed an ambassador and special Envoy for countering hybrid threats in the Ministry for Foreign Affairs.[55] The minister's main tasks include coordinating efforts at the national and international levels to counter them. To aid with this task, the Swedish research community has been providing policy advice on topics linked to hybrid threats, and it also plays an important role in raising awareness and supporting decision-making on these issues.[56]

All these efforts in civilian defense and countering hybrid threats are developed in line with Sweden's "total defense" approach. This tries to involve the whole of society to strengthen resilience against major crises or to take measures to prevent them. In the past years, the government has taken steps to increase civilian defense and preparedness by developing security concepts in areas such as defense

47 Reuters, "Sweden's supreme commander says defence spending to reach 2% of GDP by 2026," November 1, 2022.

48 Government of Sweden, Statement of Government EU Policy 2021, January 20, 2021.

49 Timo Smit, Increasing Member State contributions to EU civilian CSDP missions, Stockholm International Peace Research Institute, November 2020.

50 European External Action Service, Equipping our civilian CSDP Missions: the strategic warehouse in Central Sweden ensures streamlined logistics, December 18, 2020.

51 Government of Sweden, Statement of Government Policy, October 18, 2022.

52 Swedish Civil Contingency Agency, Our mission, June 4, 2019.

53 European Cybersecurity Competence Centre and Network, About us.

54 Gerard O'Dwyer, "Sweden to establish national cyber security centre," Computerweekly.com, February 8, 2021.

55 Mikael Wigell, Harri Mikkola, and Tapio Juntunen, Best Practices in the whole-of-society approach in countering hybrid threats, European Parliament, May 2021.

56 Wigell, Mikkola, and Juntunen, Best Practices in the whole-of-society approach in countering hybrid threats.

organization, cybersecurity, maintaining critical supply lines, and improving cooperation between the public and private sphere.[57] By pooling resources from the public and private spheres, the strengths and weaknesses of Sweden's security system can be identified and addressed. However, in this "whole of society" approach, uncertainty about the responsibility of different security aspects can arise in the public and private sector alike due to the great number of national authorities involved. This can slow down the initial response to a crisis.[58]

To sum up, since adopting its approach of total defense, Sweden has developed a successful framework that increases the resilience of its society and critical infrastructure. It is therefore well qualified to share valuable experience with the EaP countries and assistance for incorporating some elements of its total defense system to increase their civilian defense capabilities.

Recommendations

Despite the fact there is a significant need for building up the security dimension of the EaP, especially with regard to supporting Ukraine today, the potential for the EaP's evolution through the CSDP and wider civilian security is underused in the EU's policies in the region. The recommendations below suggest ways forward, bearing in mind Sweden's assets and advantages in the context of its presidency of the Council of the EU.

The EU and NATO should develop a memorandum of understanding on the EaP, and most importantly with regard to Ukraine.

The war in Ukraine is yet another display of Russia's destabilizing role in the region, after its war with Georgia, its annexation of Crimea and military intervention in Donbas, and its role in the escalation in Nagorno-Karabakh. The invasion has clarified more than ever the nature of challenges shared by NATO and the EU. As these two institutions are heavily invested in the region, and especially in Ukraine, a clear division of labor between them is crucial to effectively ensure security in Eastern Europe and the South Caucasus. NATO's undisputed military role, sharing of best practices, and support for Ukraine and the EaP countries can be complemented by the EU's established civilian force on the ground. New challenges in the hybrid and cyber fields can be better dealt with by a clear demarcation of tasks between the two institutions. Sweden is in a privileged position to serve as the moderator of a discussion that can lead to a clearer and more coherent EU-NATO collaboration in the EaP countries.

The EU should provide a mechanism for EaP countries to quickly access funds to assist them in nonmilitary defense.

The EaP countries need funds to strengthen their civilian defense, to increase the resilience of their critical infrastructure, and to improve their crisis management. They need to be able to access these funds fast and without too many bureaucratic hurdles. The European Peace Facility provides swift support in military and defense situations, and it covers costs for military CSDP missions. By extending this support to civilian missions, the EU can help the EaP countries significantly improve their defense capabilities from the ground up. Access to these funds could be tied to them reaching milestones in rule-of-law, anti-corruption, or judiciary reforms that also tie the EaP countries closer to the EU.

There should be a more coordinated training, planning, and implementing process for CSDP missions between the EEAS, the JHA, EU member states, and EaP countries.

Pre-seconded CSPD mission personnel should spend some time within EU agencies, primarily those related to the JHA. For instance, in the case of the EUAM Ukraine or the EUBAM, this could include Frontex and Europol, given that policing and border control are at the core of these missions' activities. These practices would allow new members of mission staff to understand the nuances of the relationship between the CSDP and the JHA, and it would also enhance dissem-

57 Ibid.

58 Jacek Raubo, "Total Defence for the New Era. Swedish Expert: Increase of the Armed Forces Size is a Challenge," Defence 24 August 25, 2022.

inating best practices. As the member state that sends the largest numbers of seconded personnel to CSDP missions, Sweden is in a unique position to initiate the development of a CSDP-JHA cooperation handbook, drawing on their feedback. Such an initiative can easily be launched during Sweden's EU Presidency.

The EU should establish a more targeted approach toward the EaP countries.

Since its establishment, the EaP has evolved dynamically, which has resulted in uneven outcomes given that one approach did not fit all six countries. Progress in matters of EU integration has been clearest with Georgia, Moldova, and Ukraine, while there has been little success with Armenia, Azerbaijan, and Belarus. Sweden pushed for the creation of the EaP as a policy tool to support regional cooperation and to deepen relations between the EU and its eastern neighbors, and it has since supported efforts to ensure that the EaP is successful in achieving its goals. The EU should adopt a new approach to the EaP based on differentiation. Sweden can contribute to a more targeted approach to each EaP country by promoting in-depth consultations with each one, involving their governments and other stakeholders.

The EU should prioritize deepening cooperation with the EaP countries in the domain of hybrid threats.

The EU should further strengthen its strategic dialogue on cybersecurity with the EaP countries. To do this, it should initiate intelligence sharing on cyber threats by offering to Georgia and Moldova cybersecurity dialogues like the ones it has with Ukraine and by organizing joint cyber exercises. The EU should support committed EaP countries financially in developing effective national early-warning and early-response mechanisms to counter hybrid threats. Moreover, the EU should provide the necessary assistance to selected EaP countries to secure their critical infrastructure from hybrid threats. This is best done by strengthening the public and private spheres simultaneously. Sweden has been enhancing cooperation between its public and private sectors for some time now and can provide guidance the EaP countries for successfully doing so. Ukraine's participation in the EU's Integrated Resolve exercise was an important step forward, yet it is important to engage not only the country's military but also its security services and agencies. Georgia and Moldova should also be invited to participate in the next EU's hybrid and cyber security exercises.

Strengthening cooperation on hybrid threats between the EU and the EaP countries will be mutually beneficial. By gaining firsthand experience from these partners in countering hybrid threats, the EU can improve its crisis-response system.

As a non-partisan and independent research institution, The German Marshall Fund of the United States is committed to research integrity and transparency. This work represents solely the opinion of the author(s) and any opinion expressed herein should not be taken to represent an official position of the institution to which the author is affiliated.

About the Author(s)

Michal Baranowski is Managing Director, GMF East.
Mikołaj Bronert is a program assistant in GMF's Warsaw office.
Maximilian Kaminski was a trainee in GMF's Warsaw office.
Elene Kintsurashvili is a program assistant in GMF's Warsaw office.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of the Second World War, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

75 The Marshall Plan 1947–1951
GMF 50

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

www.gmfus.org