

# **STRENGTH IN MEMBERS: HOW TO RALLY EU ENLARGEMENT FOR DEFENCE**

**Gustav Gressel, Nicu Popescu**

April 2025

---

## **SUMMARY**

- The EU's enlargement process has traditionally focused on economic and democratic reforms, leaving defence integration largely to NATO. This approach is no longer sufficient. Not all EU members or candidates are NATO members.
- This paper outlines how to enhance defence cooperation by expanding the EU's enlargement methodology or by creating tailored roadmaps. These initiatives would help candidate countries align with EU security standards and contribute to collective defence efforts.
- The first option is to include classified defence-focused questions in the enlargement questionnaire. This would allow the EU to evaluate the candidates' readiness for a geopolitically stronger Europe and align their defence sectors. However, both EU and non-EU countries alike may resist greater EU oversight.
- The second option, defence cooperation roadmaps, may be more palatable. They provide an alternative pathway for security integration and interoperability, especially for countries not on a NATO membership track.
- Linking EU enlargement to defence policies—through closer cooperation with candidate countries and expanded defence integration—offers a path to greater security and autonomy.

# Convergence in an age of unpeace

As the biggest war since 1945 ravages European soil, European countries face a new set of unavoidable security challenges. The new US administration resents shouldering defence responsibilities for Europe. European countries must learn how to cope alone in a Trumpian world.

Deeper and faster defence integration with EU accession countries would help project European power and protect them against aggression. Russia's full-scale invasion of Ukraine has already spurred a significant shift towards greater cohesion among NATO and EU member states: Sweden joined NATO in 2023 and Finland in 2024; Denmark abolished its opt-out from the European Union's Common Security and Defence Policy (CSDP) in 2022; and the EU established a defence-industrial strategy for the first time in March 2024.

But more needs to be done. European countries must ramp up their defence, secure and develop new critical infrastructure, and stay competitive in the artificial intelligence (AI) race. Now, more than ever, there is a clear need for stronger and faster convergence of candidate countries with the EU, not just on technical standards but also on security and defence policy. Achieving this convergence will require policy upgrades in multiple domains, not least in the way the EU pursues its own enlargement.

This paper proposes two concrete options to accelerate defence alignment for EU accession countries with the rest of the EU. The first way is to expand the enlargement methodology. The second—and the core of this ECFR paper—is to embrace a more intergovernmental approach in creating defence cooperation roadmaps with EU accession countries.

## The defence gap in EU enlargement

The EU's enlargement policy has been guided by Jean Monnet's vision of gradual integration through practical steps, such as merging the steel and coal industries of former enemies France and Germany. This approach has succeeded in creating a cohesive economic bloc but has left gaps in defence and security. Historically, NATO has shouldered the primary responsibility for European defence, with the EU playing a complementary role. However, this division of labour is increasingly inadequate in the face of hybrid threats, cyberattacks and energy security challenges.

The EU has a mutual defence clause, Article 42.7 of the Treaty on the European Union. It requires member states to help each other if one is attacked. However, the EU relies on NATO to enforce Article 42.7, and not all current or future EU members are also NATO members.

What's worse, even NATO's own Article 5 defence clause seems more vulnerable than ever, as the Trump administration has hinted it may ignore its obligation to come to the aid of European allies. This could also render Article 42.7 meaningless. More dangerously, the EU's potential inability to enforce its own mutual defence in case of military threats against an EU member state could lead to the political destruction of the entire EU. Member states facing military attacks will have no reason to respect any article of the EU Treaty if the EU cannot act upon its mutual defence clause.

The bloc has previously adjusted its membership criteria to adapt to contemporary concerns. In 1995 and 2004, the EU expanded by 13 countries, but some new member states failed to comply fully with its criteria on the rule of law. The bloc adapted by strengthening its enlargement methodology to monitor more closely democratic "fundamentals", such as the rule of law, democratic consolidation and justice sector reform. These fundamentals have become central to the EU's membership process. The same can be done on defence policy.

## Enlargement without defence integration

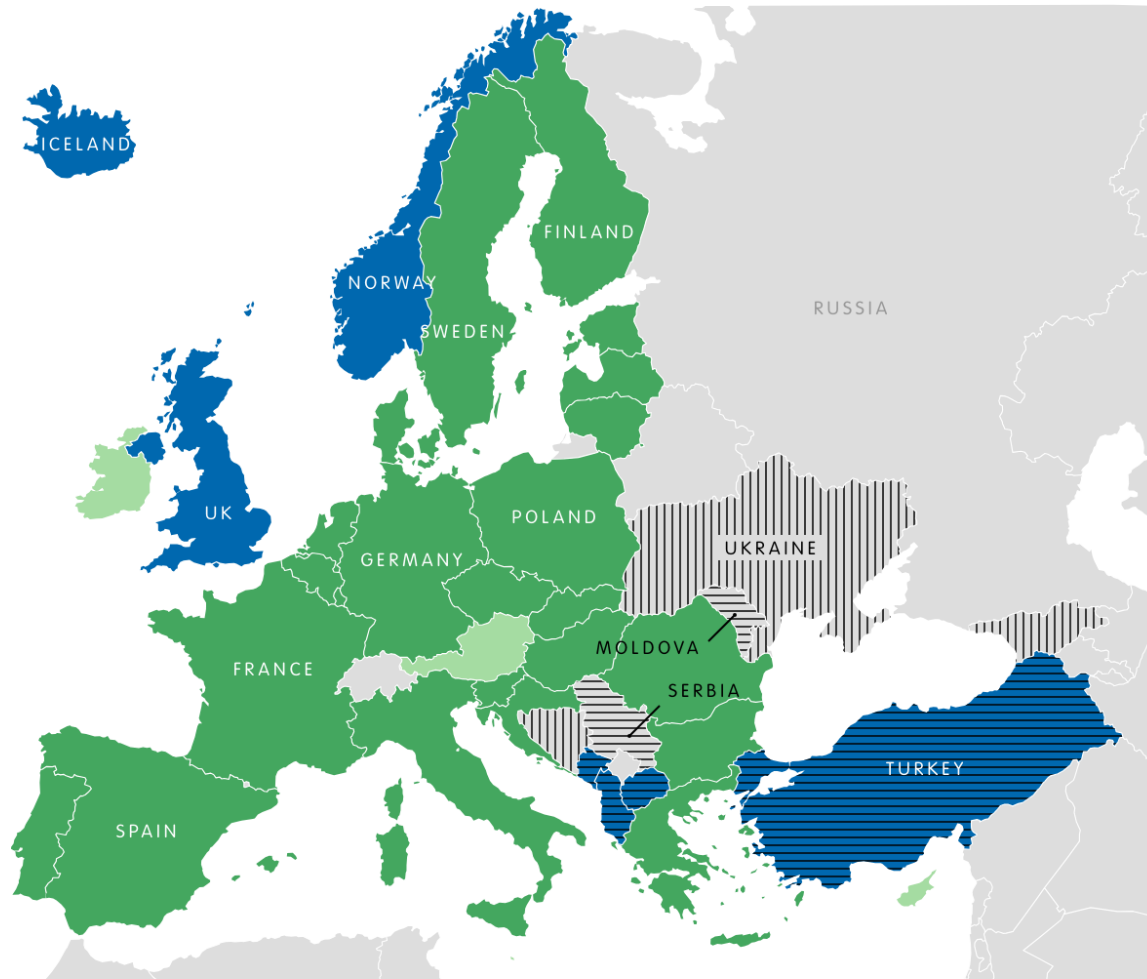
The EU enlargement processes have so far been, first and foremost, about the economy. In previous EU enlargements, security and defence integration was effectively managed through NATO. This had worked well. Of the 12 countries that joined the EU in 2004 and 2007, only Malta and Cyprus did not join NATO too.

However, the EU can no longer outsource all security and defence aspects of its enlargement to NATO because some of its new candidates for accession are not on track to join NATO. Currently, there are ten prospective new members. Moldova and Serbia do not seek NATO membership, making the NATO solution inapplicable to them. The rest are either NATO members already (Albania, Montenegro, North Macedonia and Turkey) or aspire to join NATO (Bosnia and Herzegovina, Georgia and Ukraine). Georgia and Ukraine have Individual Partnership Action plans with NATO, which are useful for cooperation but fall short of full membership. Bosnia and Herzegovina's dialogue with NATO is facing constraints because of the country's complex political structure and divisions. Yet, when they all join the EU, it is important for them to contribute to EU security, including through the EU mutual defence clause, even without NATO membership.

## Prospective EU and NATO members. March 2025

■ NATO and EU member ■ EU member only ■ NATO member only

|||| NATO+ and EU candidate ≡ EU candidate only



+ Partner countries that have declared their aspirations to NATO membership

Source: European Union; NATO.

ECFR · ecf.eu

On defence and security convergence, the EU merely monitors the foreign and security policies of candidate countries. It focuses on issues such as external trade relations, alignment with EU foreign policy statements, compliance with EU sanctions, participation in EU peace support operations, and neighbourly relations and cooperation on issues like chemical, biological, radiological and nuclear training.

Such domains are important, but they only scratch the surface of well-designed and EU-

compatible security and defence policies for candidate countries. In theory, states could comply with all EU requirements and still maintain China or Russia as close defence partners. They may engage in weapons and cybersecurity software purchases, military training, intelligence sharing and hundreds of other activities that are not addressed in the EU enlargement process but constitute the core of a country's defence policy.

Therefore, there is a clear need for the EU to develop stronger mechanisms for defence policy coordination and integration with EU candidate countries. This is, of course, easier said than done. The political and administrative obstacles are many. Defence is a cornerstone of national sovereignty, and member states are deeply protective of their authority in this domain, making them wary of expanding EU powers. Besides, both EU and candidate countries fear that stricter accession conditions or heightened monitoring in security and defence could raise the bar of entry into the EU even higher. This could slow down the already snail-paced speed of enlargement in the Western Balkans.

These are valid concerns, but so is the need to address this policy blind spot to make the EU more coherent, united and forceful.

## Closing the defence gap

There has already been some discussion on why and how to advance deeper defence integration. This paper suggests two possible routes to achieve that.

The first option is to expand the EU enlargement method. In theory, this is easier and neater, as it would be part of the existing process of steering countries into the EU. However, it is politically more complicated because member states are wary of giving more powers to EU institutions. The second option is to create new “defence cooperation roadmaps” for aspiring members. This method is somewhat more complicated but might be more palatable to EU member states. Either way, both routes should lead to the same result: deeper security and defence policy convergence of future EU member states with the rest of the EU in a world that is increasingly insecure for Europe as a whole.

### Option 1: Expand the enlargement methodology

The EU enlargement process is guided by a framework designed to ensure effective integration and cooperation among existing member states and new members: the enlargement methodology. One way to deepen defence integration is to add more ambitious criteria to the EU enlargement methodology.

Every year, in early spring, the European Commission sends accession countries an “enlargement questionnaire.” Throughout spring EU accession countries respond to these questions. The commission then combines these responses with its own independent analysis to produce annual enlargement country reports, typically published in October or November. These reports assess the candidates’ implementation of the rule of law and the *acquis communautaire*, the body of EU law, principles and obligations. The reports also identify stronger-performing domains and recommend areas where countries should accelerate progress, as well as how they might achieve this.

Chapter 31 of the EU *acquis* deals with “Foreign, Security and Defence Policy”. This chapter covers the EU’s Common Foreign and Security Policy (CFSP) and the CSDP. It requires candidate countries to:

1. align with EU declarations, decisions, and positions on foreign policy;
2. apply EU sanctions;
3. participate in EU crisis management operations;
4. end agreements with third countries that contradict EU positions; and
5. strengthen diplomatic capabilities to participate in the CFSP fully.

The enlargement questionnaire for this section focuses on the alignment of accession countries with EU foreign policy statements, sanctions and diplomatic relations with both EU member states and other candidate countries. The questions serve as indicators of the foreign policy of EU accession countries, aiming to encourage them to conform closely with established EU foreign policy positions. However, these assessments only scratch the surface of the foreign and security policy of an accession country. They do not measure crucial aspects of security and defence cooperation with EU member states, such as conducting joint military exercises, sharing intelligence, and cooperating on cybersecurity.

One way to correct this would be to develop 30-40 new questions to better evaluate defence policy alignment and progress. Since this would pertain to defence, both the questions and answers would need to be classified. The questionnaire could be a semi-formal exercise, not subject to regular voting and veto rights by EU member states. That would accommodate member states’ protectiveness of their national security prerogatives and circumvent the EU’s lack of authority in this area.

## Option 2: Create defence cooperation roadmaps

The other option is to create new roadmaps for defence cooperation based on agreements with close security partners that the EU started developing last year. In 2024, the EU designed and signed security and defence partnership agreements with Albania, Japan, Moldova, North Macedonia, Norway and South Korea. Negotiations are underway with several other countries.

Building on this foundation, the EU could create defence cooperation roadmaps tailored to each accession country's specific needs. For EU candidate countries that are not NATO members or on a NATO accession track, these roadmaps would provide an alternative pathway to achieve the security integration and interoperability with the EU that NATO typically provides. The roadmaps would be technically separate from the formal EU enlargement process—they would not be direct preconditions for membership but would provide a structure to anchor these states in EU defence frameworks before and after the date of their formal accession.

Defence cooperation roadmaps could be similar to the visa liberalisation roadmaps that were offered to Georgia, Moldova, Ukraine, and the Western Balkans in the 2000s and 2010s. These listed several dozen measures countries needed to implement to gain visa-free travel to the EU. They were divided into four sections, each outlining 70-100 measures that candidates needed to implement. Likewise, defence cooperation roadmaps could contain sections on hard defence, military mobility, hybrid threats, intelligence, cybersecurity, critical infrastructure, defence industry and government procurement. Some of the EU assistance—whether through the European Peace Facility or bilateral agreements—could also be integrated into these structured security partnerships, ensuring a coordinated and comprehensive approach to defence cooperation. The EU could then assess progress based on these measures, just as it did for the visa liberalisation roadmaps.

The mentoring and monitoring of EU accession states could be led by a core group of willing EU member states and institutions, or even third-party partners such as Britain, Canada, Norway or NATO. That would not be without precedent. The union already relies heavily on external expertise in the current EU enlargement process, such as the Council of Europe's Venice Commission to assess justice sector reforms or the OECD for public administration reforms. Similarly, international development banks—such as the World Bank and the European Bank for Reconstruction and Development—regularly coordinate and support projects that also contribute to the EU accession process. National development agencies, such as the French Development Agency and the German Agency for International Cooperation, also participate. The expertise and contribution of international organisations are therefore already embedded in the EU enlargement process.

## How to structure a defence cooperation roadmap

Many lessons can be drawn from NATO's past engagement processes, which share similarities with those of the EU. As part of its Membership Action Plan, NATO required aspiring members to submit annual progress reports on several issues. In 1999, the EU agreed to base its evaluation of a candidate's military and defence capabilities on NATO standards, ensuring consistency and interoperability.

However, NATO standards are often broad and open to interpretation. They serve as a minimum benchmark rather than a guarantee of quality. NATO does have a dedicated bureaucratic apparatus for defence matters, which drafts annual programmes and reform plans for the new members. By contrast, the EU has only a small military staff and does not conduct joint force or capability planning. It is ill-equipped to draft comprehensive defence reform roadmaps for candidate countries. Even the commission's enlargement teams lack the expertise and technical knowledge to address defence issues or implement NATO standards in military and defence structures. These capacities could be gradually developed. After all, NATO standards already form the foundation of intra-EU defence cooperation.

The defence cooperation roadmaps could help accession countries develop the legal and conceptual architecture that would align closely with the standards of EU member states. Countries could structure their defence policies based on the laws, strategies, or whitepapers that emerge through the roadmaps. This paper proposes the following structure for the EU's defence cooperation roadmaps.

### Section 1: Political affairs and defence policy

The most important issues regarding defence policy and governance are included among the EU's "fundamentals" in the enlargement process: democracy, good governance and human rights. However, the evaluation used for the fundamentals, such as compliance with sanctions or alignment with official statements, is not appropriate for a country's defence policy. For example, the EU accession process focuses solely on the civilian security sector; it does not address whether a country's armed forces are under democratic control. Democratic control of the armed forces is a necessary condition of good governance and should be part of a cooperation roadmap. But, at the same time, the accession process should ensure the armed forces are protected from abuse of power..

This section could also enhance the EU's understanding of the accession countries' foreign



partnerships. The EU would need to know of any defence agreements that could complicate or compromise a candidate's security sector. Bilateral agreements with competing powers, such as Russia or China (say, on training, disaster relief or intelligence cooperation), may grant them access to the personnel and procedures of the potential EU members. They would be a vulnerability in the security apparatus that would need to be addressed before accession. Doing so can take time because ending ratified treaties of foreign partnerships usually requires national parliaments to act (if the treaty cannot be terminated by the executive alone).

## Section 2: Military organisation and interoperability

NATO standards are the basis for military interoperability within the EU. Accession candidates need to apply NATO standards de facto to be able to work with other EU member states, even if they do not become part of NATO. This should be integral to the defence cooperation roadmaps.

The EU's evaluation of military capabilities in the past relied on the partner country's willingness to participate in the union's common security and defence missions. In NATO, the primary means of checking on the implementation of reforms and work on interoperability was conducting joint exercises with the aspirant country. The EU should emulate this practice in its enlargement. However, joint exercises—both in the NATO framework as well as within a coalition of willing states—have become highly bureaucratised and “scripted” in the past two decades. Scripted exercises are tightly choreographed, leaving little room for improvisation or independent decisions by field commanders. This fails to cultivate independent-minded and assertive commanders and makes it difficult to accurately evaluate operational and tactical capabilities. NATO conducted snap exercises during the cold war to check the readiness and dependability of forces then assigned to the Supreme Allied Commander Europe, but this practice went dormant in the 1990s. Europeans can use the enlargement process as an ideal opportunity to resurrect snap exercises and incorporate partner countries into them.

Although organising collective defence remains the realm of NATO, better alignment between the EU and candidate countries would allow them to carry out large defensive operations together. To do that, the EU will need to clarify where alignment is needed with new members by re-evaluating its security policies and programmes so that they contribute to and facilitate collective defence efforts. For example, Permanent Structured Cooperation programmes developed drones for surveillance and reconnaissance primarily to monitor migrants and possible terrorists in the Mediterranean and Sahel, not to stand up against the Russian air force. However, these drones may also be useful for collective defence. The EU should assess

existing practices and see how they can be adapted. The aspirant member country would still need to align its military structures, planning procedures, training and preparedness with NATO standards.

Again, standards can be relatively flexible. Reforms to harmonise structures and planning processes for cooperation with international partners were always designed individually depending on the specific country's needs. The same would apply to military reforms during EU accession. The EU would need to craft individual roadmaps and reform programmes, as EU candidate countries vary significantly in both capability levels and military traditions. There is no one-size-fits-all concept. In NATO, such tailored, individual reform processes were called the Planning and Review Process. The EU would have to invent its own equivalent of this.

### Section 3: Defence-industrial complex

Incorporating new partner countries into the EU's defence industry is another important chapter of any defence cooperation roadmap. National defence is generally exempt from the common market, allowing states to provide subsidies and favour their own industries in tenders. Consequently, the role of the commission has been limited to that of an enabler and financier, incentivising European defence collaboration without the authority to order, prescribe or control it. Of course, fostering secure defence-industrial cooperation with partner countries is in the EU's interest.

The 2024 European Defence Industrial Strategy intends to expand the bloc's defence-industrial readiness, and the commission appointed a new commissioner for defence and space, Andrius Kubilius, in 2024. The EU defence industry and the governing instruments will likely develop reasonably rapidly in response to the ongoing Russian aggression against Ukraine and the uncertainty emanating from US politics. However, the EU's tools are better adapted to incorporate countries that are already members of NATO, so it will need new processes.

The EU has no power to screen existing member states for defence partnerships that may endanger the EU's security as a whole. It can only audit prospective members. This could cause some discord. Candidate countries may balk at being assessed when existing EU countries are exempt. That could look like a double standard. Nonetheless, the EU should possess the authority to audit, for example, the Serbian defence industry to evaluate whether Russian ownership or shares in Serbia's defence sector could hinder its integration into the EU defence industrial space. But it should also do so for existing EU members.

The EU already tries to deepen defence-industrial and technical cooperation with prospective members by ensuring each candidate state aligns with EU sanctions, export controls, capital controls and investment screening. This is the first step and the minimum requirement to prevent hostile states from using future union members to bypass EU sanctions. After 1989, the defence and information technology industries in many post-communist countries struggled economically, so they eagerly sought any available capital for modernisation. This includes investment from EU rivals Russia and China. The EU should, therefore, conduct a screening of existing shareholders and contracts on R&D cooperation and subcontracting work in third countries.

Integrating partner countries into the EU defence industry might mean forcing them to cut export and investment ties to EU adversaries. This could gut the new partner's domestic defence industries and generate a narrative that the EU "de-industrialised" the candidate country. This scenario occurred in Poland, where the arms industry was embedded in the Warsaw Pact defence industrial complex, producing Russian equipment under license. EU and NATO accession more than two decades ago severed Poland's traditional export markets, leading to a prolonged crisis in its defence industry that only resolved with Ukraine's increased demand for military supplies after February 2022. The Law and Justice Party frequently used the narrative of "they de-industrialised us" before it won the 2015 parliamentary elections.

To cushion the shock of this transition for partner countries, the EU should prepare a buy-out fund to acquire shares or take over defence industrial assets that are on the verge of being sold to conglomerates from potential geopolitical rivals. This will have benefits for the EU as well. A significant amount of pre-production for defence goods (particularly the production of explosives for ammunition or propellant) has been outsourced to the EU neighbourhood over the last three decades. Much of the TNT and nitrocellulose used in most European weapons are from Bosnia and Albania. Serbia is also an important producer and exporter. This outsourcing to the Balkans made the EU's own supply chains more vulnerable, but that can be corrected.

In addition to harmonising export control legislation, the EU would need to help candidate countries to increase the effectiveness of their customs services, financial investigators and regulators, as well as the investigative police and intelligence. It is also important to make these changes more substantial than mere "on paper" exercises. Harmonised export control legislation is useless if no one enforces it.

Important changes will also be necessary in intelligence to integrate new countries into

complex and innovative defence-industrial projects. The new partners must implement common standards for information security and data protection. Secrecy is crucial.

For example, numerous allied reconnaissance planes, drones and satellites monitor the war in Ukraine, collecting extensive technical data on Russian air defence systems, fighter planes, missile communications and electronic countermeasures. Armed forces and intelligence services then use this valuable information to develop new weapons systems to counter Russian threats. These systems are designed and developed by private multinational companies such as Diehl, which is based in Germany but has branches in Norway and Italy, and Rheinmetall, also based in Germany but operating in almost every EU country. For companies working within NATO's or the EU's defence industrial space and receiving top-secret technical information for R&D, standardised procedures for receiving, handling and safeguarding this information are essential. NATO has such procedures, but the EU must establish similar standards for new members that cannot join NATO but wish to integrate with its defence industry. Only secure intelligence sharing will foster cooperation between national militaries and defence-industrial complexes.

## Section 4: Intelligence

Exchanging classified information, sharing technological secrets and collaborating on cutting-edge research and development is at the core of defence. Beyond the technical specifications of weapons systems (both domestic and those of the enemy), sensitive data also includes contingency plans for possible wars and intelligence on the adversaries' activities. Effective cooperation requires stringent measures to protect these secrets.

NATO has three agreements to provide standards for the safe exchange of information and classified data.[1] These treaties provide the foundation not only for the exchange of classified military intelligence but also for defence-industrial cooperation. The EU has no direct equivalents.

However, the role of the intelligence sector in many candidate and partner countries is a sensitive topic. On the one hand, intelligence agencies in these countries are the first organisations to respond and counteract various Russian hybrid attacks, from subversion to sabotage. On the other hand, they are also instruments of power, often used by governments to exert power or gain political advantages. Agencies with Soviet or communist legacies are often over-staffed and underpaid, which incentivises corruption. They are overly reliant on human intelligence, inadequately equipped for technical surveillance and cyber tasks, and frequently confined to their institutional silos. The lack of coordination with financial, customs and economic crime agencies, coupled with overlapping competencies, disrupts investigations due to bureaucratic competition.

The EU's intelligence policies focus on cooperation amongst civilian intelligence services, primarily on counter-terrorism and organised crime. The EU Counter-Terrorism Coordinator and the European Union Intelligence and Situation Centre support these efforts, providing general situational awareness for the European External Action Service. Europol coordinates the investigative work. The EU military staff also has a small intelligence unit, roughly 40 employees, dedicated to exchanging military intelligence. Again, this is a small staff, and the main purpose is to share situational awareness in areas where the EU conducts field missions. However, none of these bodies are authorised or equipped to audit other intelligence services, evaluate reforms and capabilities or engage in capacity-building programmes.

As a result, intelligence reform was neglected in past accession rounds. However, the EU has gained valuable experience in assisting Ukraine's civilian intelligence and security sector reform through the EU Advisory Mission since 2014. It should institutionalise these capabilities to make intelligence reform and capacity-building a permanent aspect of the enlargement policy.

## Section 5: Cybersecurity

Russian cyber-espionage and political subversion through cyber operations have surged since the start of the full-scale invasion of Ukraine. EU aspirant countries, in particular, have faced such attacks because Moscow wants to undermine their relationship with the bloc. Artificial intelligence will decrease the costs of cyber-influence operations, making this trend likely to persist.

In recent years, many partner countries have reformed or established cybersecurity institutions, including cyber incident response teams, cyber forensic capabilities and specialised departments within the police and intelligence agencies. They have also established public-private partnerships with digital service and cybersecurity companies. However, these institutions are weak and under-resourced. In the past, America was the prime source of assistance in cybersecurity, even for tasks such as auditing vulnerabilities in critical infrastructure. But the second Trump administration, influenced by the deregulatory zeal of digital oligarchs, may adopt different policies, potentially ending or altering this source of support.

Fortunately, the EU is better prepared to assist in this field. It has an overall framework and standards for cybersecurity agencies, as well as digital products and services in the form of the Cyber-Resilience Act and the Network and Information Security Directives (NIS1 and

NIS2), which provide standards to achieve a common level of cybersecurity across the bloc. During the accession process, candidate countries will have to implement those as well. The European Union Agency for Cybersecurity (ENISA) is the central certification and coordination hub that audits cybersecurity institutions and sits at the top of the EU's certification pyramid. However, it was not created with enlargement in mind; its primary job is only to coordinate EU member states. When it will start working with candidate countries has not yet been established either, but at least an institution exists.

The EU should also address the pressing issue of creating legal frameworks to counter subversion and strategic disinformation. Both EU member states and candidate countries will need to improve interlinking their intelligence agencies, financial investigations and cyber-reconnaissance tools to effectively uncover subversion and destabilisation plots.

## Enlarge and defend

European security is in tatters. NATO's Article 5, the EU's backbone for decades, is more uncertain than ever. The EU's own ability to enforce its mutual defence clause is not yet operational. Its power to dissuade hostile powers from aggression needs strengthening and its strategic autonomy needs fortifying. To make Europe peaceful and strong, EU enlargement and European defence capabilities need to be linked.

Specific guidelines would improve the integration of the EU enlargement process with security and defence policies. As part of those guidelines, the EU should encourage candidate countries to align on EU defence policy priorities and processes. It should deepen cooperation on public procurement in defence markets and accelerate the integration of future members into the European Defence Agency. All in all, it should expect stronger contributions towards a geopolitically stronger Europe from future EU member states.

The biggest war in Europe since 1945 starkly underscores that for the "Monnet method" of technocratic integration to work, the method needs to be protected by strong defence, capable allies, close third-country partnerships and heavy weaponry. Only this will ensure that current and future EU member states have the capacity to defend themselves. It is time to make this understanding part of the EU enlargement process and method as well.

## About the authors

**Nicu Popescu** is a distinguished fellow at ECFR. He served as deputy prime minister of Moldova, as well as minister for foreign affairs and European integration (2021-2024) and foreign minister between June and November 2019.

**Gustav Gressel** is a senior lecturer at the National Defence Academy in Vienna. He spent ten years in Berlin as a senior policy fellow with ECFR's Wider Europe Programme. Before joining ECFR, Gressel worked in the Bureau for Security Policy of the Austrian Ministry of Defence and served in the Austrian armed forces for five years.

## Acknowledgements

We extend our heartfelt gratitude to our editor, Kat Fytatzi, and the wider editorial team for their invaluable guidance and support in shaping this work. Special thanks also go to the several officials and diplomats who generously shared their insights during our discussions but have chosen to remain unnamed.

[1] The Agreement between the Parties to the North Atlantic Treaty for the Security of Information (Brussels, March 6th, 1997); The Agreement for the mutual safeguarding of secrecy of inventions relating to defence (Paris, September 21st, 1960); and the NATO Agreement on the communication of technical information for defence purposes (Brussels, October 19th, 1970).

## ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy. ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Lykke Friis, and Norbert Röttgen.
- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia, Warsaw, and Washington. Our offices are platforms for research, debate, advocacy and communications.
- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and “friends of ECFR” gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions. [ecfr.eu](http://ecfr.eu)

The European Council on Foreign Relations does not take collective positions. This paper, like all publications of the European Council on Foreign Relations, represents only the views of its authors. Copyright of this publication is held by the European Council on Foreign Relations. You may not copy, reproduce, republish or circulate in any way the content from this publication except for your own personal and non-commercial use. Any other use requires the prior written permission of the European Council on Foreign Relations. © ECFR April 2025. ISBN: 978-1-916682-78-8. Published by the European Council on Foreign Relations (ECFR), 4th Floor, Tennyson House, 159-165 Great Portland Street, London W1W 5PA, United Kingdom.