**A European Political Community for a Geopolitical Era**

*Proposals to make the EPC deliver for shared European stability, security and prosperity*
*Paris 24 May 2023*

The inaugural meeting of the European Political Community (EPC) took place on 6 October 2022 in Prague gathering 44 leaders from across the continent together with the President of the European Commission and of the European Council. Against the backdrop of Russia's war in Ukraine, the gathering sought to strengthen their cooperation on issues of common interest, revolving around peace and security, the economic situation, energy and climate, and migration and mobility.

A second summit of the EPC will be held on 1 June 2023 in Chisinau, Moldavia. One gathering is an event; two is an established feature. It shows that participants value the format and want to build around the EPC to help Europe navigate these geopolitical times.

A gathering of all European leaders in Moldova, a country neighbouring the war, threatened by Russia and candidate to join the EU will send a strong political signal in itself. The photograph will be the message.

The meeting in Moldova will also help anchor the EPC as a forum where leaders can discuss issues that impact the security and prosperity of the continent without prepared speeches or pre-cooked communiques. Where they can have candid exchanges and build a collective understanding of each other's necessities. The informality will allow for valuable exchanges.

With the next two summits already scheduled, in Spain in the fall followed by the UK during the first semester of 2024, the EPC can become a regular, continental-wide leaders meeting giving political impetus to a European agenda. Beyond the circumstances of the war now prevailing, its format, both informal and intergovernmental, may prove to have an added-value in three ways:

- *Discussion forum for strategic matters*

  The EPC provides the needed informal setting to foster discussion at the highest political level. All leaders attending the Prague summit appreciated this unique opportunity to exchange directly on an equal footing, with no expected immediate result, on the continent's security and other common matters of strategic interest, such as migration. Favouring personal contacts among leaders in a club-like atmosphere, helps develop a sense of belonging to the same continent, beyond the EU. With the key participation of the UK and of Turkey, it provides the channels of dialogue, outside existing institutional formats, that are necessary for Europe to build its assertiveness and visibility.

- *Diplomatic hub for regional disputes*

  EPC summits offer new opportunities for dialogue for leaders of countries under long and on-going disputes. For instance, the Prague summit allowed for bilateral discussions to develop between Armenian and Azerbaidjan leaders and between Serb and Kosovar leaders with the participation

of other peers helping facilitate. Once again, informality provides flexibility, but also peer-pressure to advance solutions.

- *Political booster for concrete cooperation*

A regular gathering of leaders can also be used to give new impetus to pan-European cooperation initiatives improving the lives of millions of Europeans. The Prague summit has identified seven areas of concrete cooperation in line with the strategic interests of the continent that the EPC is meant to pursue: energy, critical infrastructures, cybersecurity, youth, migration, regional cooperation in the Black Sea and Caucasus.

This note provides suggestions about concrete initiatives that the EPC could articulate on three areas: **cybersecurity, youth education and migration.** Following the inter-governmental nature of the EPC, the proposed initiatives are conceived as forms of reinforced cooperation among members of the EPC rather than as necessitating specific new organizational structures. Given the numerous initiatives already in existence within and among members of the EPC, the choice of proposed initiatives has been guided by added value. Ultimately these proposals would strengthen the geopolitical visibility of European both for its citizens, as well as for third countries.

This brief has been produced through a dialogue among academics from leading European Universities and Think Tanks from across Europe led by Sciences Po and the Jacques Delors Institute.

Arancha González, Dean, Paris School of International Affairs at Sciences Po

Sébastien Maillard, Director, Jacques Delors Institute

**Participants from the following institutions:** Civica Alliance of European Universities; CIDOB (Spain); CIRD (Serbia); Cligendael Institute (The Netherlands); Egmont – Royal Institute for International Relations (Belgium); ELIAMEP-Hellenic Foundation for European and Foreign Policy (Greece); EDAM-Centre for Economics and Foreign Policy Studies (Turkey); EU ISS (EU Institute for Security Studies); Global Relations Forum (Turkey); Instituto Elcano (Spain); Istituto Affari Internazionali (Italy); IWM Vienna (Austria); Polish Institute of International Affairs (Poland); SWP-German Institute for International and Security Affairs (Germany).

**Cybersecurity**

Arnault Barichella
Researcher Sciences Po, Paris

**Context**

Cybersecurity has been a topic of increasing concern over the last few years, as Europe has been exposed to a rising number of cyberattacks that have grown in sophistication, causing widespread damage. Moreover, cyberattacks targeting particular countries can spread across the continent due to the level of economic and digital interconnection amongst European nations. For instance, the Wannacry virus in 2017 (with North Korea as a prime suspect) was a global cyberattack impacting over 150 countries - including most of Europe, which resulted in several billion euros in damage due to the diversity of sectors impacted, ranging from the UK's NHS, French carmaker Renault, German federal railway system, Italian universities, along with energy and telecom companies in Portugal and Spain. Governmental entities, private companies and civil society organizations across Europe are now being targeted by cyberattacks on a daily basis, with tens of thousands of reported attacks each year.

While independent hacking groups are sometimes responsible, an increasing number of cyberattacks are receiving support from governmental entities, often in relation to geopolitical tensions. Nations such as Iran, China and North Korea are suspected to provide at least covert backing in a number of cases. After the annexation of Crimea and the beginning of military clashes in the Donbas region in 2014, a decade-long cyber confrontation has been unfolding between Russia, Ukraine and Europe (or NATO more generally). Hackers possessing ties to the Kremlin have launched several of the most devastating cyberattacks in history. For example, the NotPetya virus targeting Ukraine in 2017 shut down up to 30% of computer systems in the country, before propagating to many European countries and resulting in 10€ billion worth of damage due to supply disruption and equipment damage.

The war in Ukraine constitutes the first important factor in analysing how the EPC can contribute to cybersecurity in Europe. Russia launched several waves of cyberattacks to destabilize the country in preparation for the full invasion in February 2022, which targeted critical infrastructure (energy, banking, communications, etc.) as well as government and military sites. Throughout the war, Moscow has intensified cyberattacks, whilst engaging in a form of 'hybrid warfare' blending cyberattacks with kinetic military strikes on the ground.

Ukraine has demonstrated impressive cyber resilience by learning from past mistakes; likewise, Europe and NATO have provided Ukraine with essential support, including real-time intervention from cyber agencies, helping to contain the worst effects from Russian hacking. Yet, this is no reason for complacency, since the pace and sophistication of cyberattacks have been accelerating recently due to stalemate on the battlefield. Moreover, many similar issues have been impacting other neighboring countries, especially Moldova. Indeed, Russia has been amplifying cyberattacks against Moldova over the last couple of months, seeking to destabilize the country. Since Ukraine and Moldova are participants in the EPC, the Community could become an essential platform to enhance and reinforce the provision of cyber assistance:

- This would involve the transfer of additional, more sophisticated IT equipment and software, along with greater institutionalized training on cybersecurity both for Ukraine's so-called 'IT Army', as well as for Moldova. Decisions made through the EPC on this matter could thus complement those made via other organizations such as NATO.

- The EPC could also provide a key channel for discussing and organizing how to expand the mandate of the EU's current advisory mission to Ukraine in order to tackle cybersecurity risks, covering strategic communications and digital technologies. A similar advisory mission could also be sent to Moldova.
- The EPC could also operate as a bridge linking associated 'Eastern Partnership' countries like Ukraine, Moldova and Georgia with the EU's framework for 'permanent structured cooperation' projects involving cybersecurity and hybrid risks. The latter might even result in the launching of civilian cyber operations in these countries, for example.

A second critical factor in evaluating the potential of the EPC to address cybersecurity is the challenge of 'weak links'. Cybersecurity threats stemming from the war in Ukraine also involve the risk of potential spill-over into Europe. One notable example was the hacking by a Russian-backed group of the Viasat satellite company on the first day of the invasion, which led to the disabling of connected modems. This seriously disrupted communications not only in Ukraine but spilled into Europe and affected tens of thousands of people from Poland to Germany and France, with disconnection problems lasting over several months. For the time being, propagation into Europe from Russian cyberattacks targeting Ukraine has mostly been contained, partly due to enhanced cyber defenses enacted by European nations following the start of the invasion. Nevertheless, the risk of escalation is real and should not be under-estimated, especially since Moscow has recently increased the pace and sophistication of its cyberattacks on Ukraine and Moldova. Moreover, Russia appears to be increasingly targeting NATO members as well, especially those countries serving as transit routes to deliver weapons to Ukraine, such as Poland and Romania, which have faced successive waves of Russian hacking over the last few months.

The EPC could provide a key channel for reinforcing cybersecurity collaboration across the continent to prevent either spill-overs from Ukraine, or direct Russian cyberattacks on European countries that spread to neighboring states. In particular, the EPC has the potential to play an essential role in terms of tackling the problem of weak links, which facilitates the propagation of cyber viruses. A multispeed framework is at work, whereby a small group of countries such as France, the UK or Germany lead the way as they have enacted some of the most extensive cybersecurity frameworks in the world, supported by far-reaching national legislation. Yet, a number of other European countries, partly due to a lack of resources or adequate infrastructure, have yet to enact sufficiently robust policies on cybersecurity, leading to the emergence of 'weak links' across the continent.

This is highly problematic, since countries with less developed cybersecurity norms become vulnerable and constitute potential openings for inserting cyber viruses, which may then spread to the entire European network. Such a situation is exacerbated by the close interconnection between European countries due to the rules of the Single Market and the EU integration process, which also extends to affiliated countries of the European Free Trade Area and associated Eastern Partnership countries to a certain extent. In this regard, energy infrastructure crossing Ukraine has been an ongoing issue of concern for Europe due to its vulnerability to hacking. Even within the EU itself, norms and regulations on cybersecurity for critical infrastructure, such as the NIS Directive, tend to establish mostly general rules and guidelines, providing Member States with broad autonomy in the implementation process. Although there has been some improvement with the recent NIS2 proposal, the latter does not do enough to tackle the issue of weak links.

**A Forum for fostering a common cybersecurity floor across Europe**

There is clear potential for the EPC to play a role by:

- Providing a **forum for European countries to share best practices and information**, which could help pave the way for greater convergence of cybersecurity norms across the continent. As an intergovernmental set up, the EPC does not possess any binding authority but it could prove a useful platform for high-level political dialogue. This could also apply to the disclosure of classified information, which countries are often reluctant to share.

- Thanks to its broad membership, the EPC could also help to ensure that EU cyber norms are taken into account by non-EU countries, especially those in Eastern Europe that are most vulnerable to Russian cyberattacks. This includes not only Ukraine and Moldova, but also Georgia, Armenia and Azerbaijan. While not completely resolving the problem of weak links, the EPC could help to mitigate some of its consequences by aiming to develop a "floor" involving common minimum cybersecurity standards across Europe.

- The EPC could act as an essential bridge or conduit between member states and countries outside the EU. In fact, it might even be possible for those countries which are most advanced in the field of cybersecurity, like France or Germany, to take the lead, including via the creation of ad-hoc groups for example.

A third factor is that the EPC includes countries such as the United Kingdom and Turkey, both of which have had difficult relations with the EU over the last years. In the case of the UK, Brexit has led to concerns about the risk of gradual estrangement on defense matters, including in terms of cybersecurity, with respect to EU initiatives in this field (revolving around the 'Common Security and Defence Policy' – CSDP), as well as with Europe's continental military powers. The UK and France enjoy a long historical tradition of military cooperation which has been partly slowed down following Britain's departure from the EU. The EPC could become an essential platform for Britain to actively collaborate with continental Europe on defense issues, including on strategic matters like cybersecurity which involve mutual vulnerabilities due to the risk of spill-over.

The EPC's potential to act as a bridge between NATO and the EU's CSDP is a final, critical factor in assessing the Community's prospects for addressing cybersecurity issues. The objective would be to foster dialogue and communication by ensuring that new initiatives launched by the CSDP on cybersecurity, do not overlap and duplicate those of NATO. NATO has been organizing a large-scale cybersecurity exercise every year since 2010 known as 'Locked Shields', which simulates a massive cyberattack on computer systems. This exercise provides valuable real-time training for NATO members to upgrade their cyber defenses based on the latest threat appraisals and technologies. Similarly under the CSDP, the EU has announced an enhanced Cyber Defence Policy in November 2022, along with the EU's 'Strategic Compass' for Security and Defence announced in June 2022, where cybersecurity features prominently.

In conclusion, the EPC can provide a foum to enhance and accelerate the provision of additional IT equipment and training to Ukraine and Moldova, helping to reinforce resilience against Russian cyberattacks. It could also act as a key conduit for information-sharing and best practice exchanges on cybersecurity between EU and non-EU countries. This would help to tackle the issue of 'weak links' by creating a level-playing field through the establishment of minimum common cybersecurity norms across the continent, thus reducing the risk of spill- over. The EPC also shows potential for maintaining collaboration on cybersecurity between the EU and countries like the UK or Turkey. Finally, it can contribute to mitigating overlaps or duplication between NATO and the EU's CSDP, by serving as a bridge between the two organizations.

**Youth Education**

Xavier Prats, Jacque Delors Institute

This note explores the opportunities for EPC cooperation on education and youth, while taking into account that infrastructure and capacity-building are beyond the remit of EPC, and that cooperation in the field of education should be respectful of each country's unique context and governance. The note proposes actions on mobility and digital education.

**Key trends and challenges in education**

In human capital, strategy, infrastructure and technology, few education systems and institutions were prepared for the impact of the Covid-19 pandemic. In the short term, the temporary cessation of face-to-face activities reduced the global demand for education and increased inequalities with often dramatic consequences. In the medium term, two main trends are shapingthe future of education, globally as well as across Europe:

- Demand for relevant education and skills will increase irrespectively of demographic change, especially university, vocational, hybrid and online education. Traditional institutions on their own will not be able to satisfy the demand for new skills, internationalization, and physical and virtual mobility.
- Digitalisation is reshaping education. Education systems had been mostly insulated from the disruption created by technology and digitalization in all aspects of society. With the pandemic and the exponential development of artificial intelligence, there is a significant shift towards online and blended learning, as digitalization creates new services and a demand for new skills. While each country has its own unique context, policies and resources, across the EPC there are similar education challenge, albeit with different degrees of intensity: equity and access, particularly for vulnerable groups including migrants; the quality and relevance of education, particularly in areas that are critical for economic growth and competitiveness such as STEM, soft skills and digitalization; teacher training and professional development; and intercultural education, including critical thinking and education for sustainable development.

**Opportunities for EPC cooperation**

Education is at the same time a significant challenge and an exceptional opportunity for the EPC community, as human capital development is a key instrument for productivity and inclusion. There are approximately 80 million young people aged 15-24 in the EPC, 60 of whom in the EU. On average, the higher education attainment rate (the percentage of population aged 25-64 years who have obtained a university degree) in the EPC as a whole is 34%, but it varies enormously between countries, from under 20% to almost 50%.

The EU has a long experience of support for education and youth, with programmes and platforms ranging from student mobility to university cooperation and civic engagement. Most of these initiatives are part of the Erasmus+ programme; while their main remit is within the EU, most non-EU EPC countries are (partly) eligible also (for ex. on university mobility). Within the EPC's

budgetary and human resources constraints, there are two potential areas of EPC cooperation at a relatively low cost in both financial and human resources, which could be implemented either through the extension and adaptation of existing EU instruments, or as separate initiatives: mobility and digital education.

**1. Mobility and exchange**

Mobility and exchange initiatives, though small in absolute numbers, can help support youth participation and young entrepreneurs, and promote greater social and environmental awareness and engagement among young people. Taking the EU experience and its existing instruments as a reference or model, five types of initiatives could be explored:

- An EPC Youth Forum for civic engagement and capacity building, including through youth councils, online platforms, and social media channels to promote digital citizenship, including topics such as online safety, digital media literacy, other mechanisms that give young people a voice in local and national policies.

- Student and schoolteacher exchanges, including vocational training institutions, to promote intercultural understanding, employability, language learning and professional development across EPC member countries.

- Teacher academies, offering the opportunity to teachers from EPC countries to exchange best practices, develop their skills and teaching and learning strategies to address the needs of the global economy (e.g. new STEM programmes and fields with high demand for skilled workers).

- An EPC Solidarity Corp: It could offer young people the opportunity to volunteer and work on projects that benefit communities and promote social cohesion across the EPC. The Corp could support mentoring or organizing youth activities, to build social and civic skills, promote intercultural learning, and encourage active citizenship.

**2. Digital education**

Cooperation on digital education can help bridge the digital divide and promote more equitable access to high-quality digital education resources, while also providing an incentive for collaboration between the EU and non-EU education institutions. The European Digital Education Hub created in 2022 and its resource centre can play a supportive role:

- A virtual community for schools: an online platform for school education, modelled on the EU School Education Gateway. offering teacher training and a forum for online school cooperation, sharing expertise and resources on pedagogy, curriculum development, and assessment.

- Virtual student mobility through digital learning, allowing students to take courses from other countries without the need to physically travel.

### 3. Outline of a flagship initiative - the EPC Digital University alliance

The EPC might wish to signal a higher level of ambition in addressing the systemic challenges of education in the European continent, particularly inequalities, human capital development and the growing impact of technology and digitalization. For that purpose, a cost-effective and impactful way could be to create an EPC Digital University Alliance (DUA). Its main features would be the following:

- Model: The EPC's DUA would be inspired by the European University Initiative (EUI) originally proposed by President Macron, which was endorsed at the 2017 Gothenburg Summit and now involves already 300+ EU universities cooperating in 44 alliances. More specifically, The DUA would draw from the model of OpenEU, the only candidate for EUI Alliance that gathers the main open universities of the EU with 400,000 students overall.

- Structure and organisation; In practice, like the 44 EUI Alliances, the DUA alliance would take the form of a long-term partnership between several existing universities from EPC countries, including mainly but not only online universities. It would be supported by a secretariat located in one of its member universities (as the EUI Alliances). Operating costs are difficult to estimate, but by analogy to EUI Alliances they would not exceed 5 MEURO p.a.

- Mission: DUA's mission would be twofold: a) to establish an inclusive EPC digital university, widening access to quality higher education and lifelong learning to all EPC citizens, any time, from anywhere, regardless of their personal or professional circumstances, their age, gender, nationality, time constraints or place of residence. And b) to contribute to the digital transformation and modernisation of higher education Institutions across the EPC, supporting them in the integration of digital technologies for education.

- Policy rationale and added value: The DUA would address three key challenges common to all European higher education institutions: digitalisation, inclusion, and life-long learning. Human capital development and education have been identified as a key challenge for the Balkans and other non-EU EPC members; current academic cooperation between higher education institutions of the EPC beyond the European Economic Areas is mostly bilateral and does not focus on digitalisation.

- Deliverables: The DUA alliance objectives could be similar but initially less stringent than those of an EU alliance. They would include sharing best practices, developing common standards and curricula, providing technical assistance and resources for online and blended learning, joint degrees, etc.

If the idea of an EPC Digital University alliance is considered as worth exploring, further work should be done on key factors such as membership requirements, organisation, budget.

## Migration and Mobility

Jérôme Vignon
Jacques Delors Institute

### Context

It seems à priori of little relevance to think on migration as a potential common issue for EPC. Let us think of striking contrasts among members: some of them are sources of irregular migration which is not really welcomed in other members territory. Some are subject to transit mobility which ends up in non-regular migration; The recent surge in irregular migration - 330 000 were recorded in 2022, a 60% increase compared with 2021 – saw half of them following the western Balkan route, a route which leads mainly towards the EU but also to a large extent to the UK , since many irregular movements recorded in 2022 had a link with English speaking countries of origin.

However, there are opportunities to set up a forum, non-binding in nature, to explore cooperative spaces around two areas: building a common culture of border protection; and developing a common approach around the external dimension of migratory policies.

### Building a common border protection and monitoring culture

At first look, considering the various EPC members, it is striking to see the important "pull factor" of the Schengen area. Free movement remains a strong magnet which might underpin some cooperation:

- There are 27 Members of the Schengen area, 4 of them are non-EU (Norway, Switzerland, Liechtenstein, Iceland)
- There are 3 EU members which are not member of Schengen, but have applied to become one (Bulgaria, Romania, Cyprus).
- There are 8 countries officially recognised as candidate countries Albania, Bosnia, Montenegro, North Macedonia, Moldova, Serbia, Turkey and Ukraine.
- At least two others still not recognised would like to join in (Georgia and Kosovo).

So around 36 members of EPC are more or less concerned by the perspective of the free movement of workers, which entails some form of common migration and even asylum policy.

If free movement is still a shared, even a long-term perspective for most EPC members, then it would be desirable to build a common culture about border protection.

Even if a large part of inflows might be migrants on transit to a final destination, no EPC country is comfortable with irregular migration. In addition, all EPC members have undertaken to respect human rights and a shared border control culture could also embed a human rights culture.

As the EU now relies upon two fully-fledged agencies – Frontex and the European Asylum agency – it would be derisible to develop information and training on the twin issues of border protection and human right implementation while organising voluntary missions of those two Agencies in all EPC members. In addition, Frontex could be mandated to extend access to the ETIAS and ESE databases to all non-Schengen EPC members to register incoming and outgoing passengers into their territories.

An ad hoc EPC migration and mobility forum could be set up to address these issues as well as other potential areas of cross border cooperation.

**Broadening the scope of the external dimension of EU migration and mobility policy.**

In the EU, when it comes to building a common migration policy, member states tend to agree with its so-called “external dimension”: cooperation with third countries of origin to strength their ability to control migration, to become a “ safe country of origin” , to monitor migration routes including the fight against smugglers, to implement readmission of irregular migrants and more generally to use the various external policy instruments - including trade and development – to reduce irregular migratory flows .

However, until now, the external dimension has proven of limited effectiveness and at times inconsistent with other foreign policy objectives. Take for example the latest conclusions of the European Council under the Swedish presidency early February 2023. Those conclusions took a strong stance against southern countries of origin, aiming at putting pressure on them by all possible EU foreign policy instruments (including for example migration related conditionality to access GSP trade preferences). At the same time, the EU is working to attract more countries in the South to support its stance concerning Russia’s aggression against the Ukraine. Members of the EPC other than the EU also face similar difficulties.

Another consideration has to do with the changing nature of external migration flows. Figures show that migration inflows into the EU are mainly driven by labour considerations and that a large proportion of migrants - including irregular migrants - tend to display a high proportion of medium or high qualification. Therefore, managing labour migration, including temporary migrants, could also offer new avenues for external cooperation with third countries of origin or transit.

This is why the United Nations Global compact on labour migration and mobility, adopted in 2018, was intended as a framework for multilateral and bilateral negotiations between origin and destination countries.

Given the above, the EPC Forum on migration and mobility could also help its members develop common approaches to engage with non-EPC countries of origin. The Forum could also serve as a testing ground for the UN Global Compact for labour mobility and /or migration.