JOINT

A joined-up Union, a stronger Europe

JOINT
Research Papers No. 4

November 2021

Not Yet Fit for the World: Piecemeal Buildup of EU Military, Cyber and Intelligence Assets

Kristi Raik

Contributing authors:
Kristine Berzina, Ivo Juurvee,
Tony Lawrence and Maurice Turner

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 959143.
This publication reflects only the view of the author(s) and the European Commission is not responsible for any use that may be made of the information it contains.

Not Yet Fit for the World: Piecemeal Buildup of EU Military, Cyber and Intelligence Assets

Lead author: Kristi Raik

Contributing authors: Kristine Berzina, Ivo Juurvee, Tony Lawrence and Maurice Turner*

Abstract

In the past decades, the EU has developed an increasingly broad, multi-sectoral set of foreign and security policy instruments. All of these can be relevant in sustaining the EU's crisis and conflict management efforts. While trying to create a more effective and integrated toolbox, the Union has faced a number of challenges. First, as the EU's scope of activity and level of ambition have increased, the need to strengthen the "harder end" of instruments – including military, cyber and intelligence tools – has been widely acknowledged, but these remain weak. Second, with EU policies extending to areas where the Union's resources and competencies are weak, the need to mobilise member states' resources has become more important, but ensuring meaningful contributions from member states has proven difficult. Third, it has become an ever more complex task to connect the multiple sectors to each other to build a comprehensive policy.

* Kristi Raik is Director of the Estonian Foreign Policy Institute at the International Centre for Defence and Security (ICDS). Kristine Berzina is Senior Fellow and Head of the Geopolitics Team at the Alliance for Securing Democracy in the German Marshall Fund of the United States (GMF). Ivo Juurvee is Head of Security & Resilience Programme at the ICDS. Tony Lawrence is Head of Defence Policy and Strategy Programme at the ICDS. Maurice Turner is Cybersecurity Fellow at the Alliance for Securing Democracy in the GMF. The authors are grateful to Steven Blockmans, Zach Paikin and Dylan Macchiarini Crosson from CEPS and Pol Bargués from CIDOB for their thorough and insightful comments on earlier versions of the paper.

Introduction

The first foreign policy tools of the European Union date back to the creation of the European Economic Community in 1957, which established common external economic policies with a strong supranational competence. This was traditionally seen as the technical, "low politics" area of external relations, as opposed to the "high politics" of sensitive foreign and security policy matters where member states were keen to maintain an intergovernmental approach.[1] Foreign policy coordination among member states increased from the 1970s, but a leap to a more institutionalised – yet still intergovernmental – Common Foreign and Security Policy (CFSP) was only made with the Maastricht Treaty signed in 1992. The new momentum was initiated by dramatic changes in the international environment that created both new space and a need for a stronger European approach to regional security matters, which was most painfully underscored by the wars in former Yugoslavia.

Since the 1990s, the Union has been gradually strengthening the "higher" and "harder" end of EU foreign and security policy instruments, thereby becoming an increasingly multi-sectoral foreign policy actor. During the past decade, the changing international environment has yet again created new demands, as the world has become more multi-polar, uncertainty about the United States' commitment to European security has grown, instability in the EU's immediate neighbourhood has increased, and security risks and threats have become more complex and manifold. In the words of High Representative of the EU for Foreign Affairs and Security Policy Josep Borrell, this has created the need for the EU to "learn to use the language of power"[2] – which implies the necessity to develop its foreign policy tools accordingly. The EU has made efforts to strengthen its military capabilities in the framework of the Common Security and Defence Policy (CSDP) launched in 1999, while additional tools have been created to address new threats in areas such as cybersecurity and disinformation. The EU has thus constructed an

[1] Stanley Hoffmann, "The European Process at Atlantic Crosspurposes", in *Journal of Common Market Studies*, Vol. 3, No. 1 (1964), p. 85-101.

[2] Josep Borrell Fontelles, *Opening statement, Hearing at the Committee on Foreign Affairs of the European Parliament*, Brussels, 7 October 2019, https://multimedia.europarl.europa.eu/en/hearing-of-josep-borrell-fontelles-high-representative-vice-president-designate-of-the-european-commission-opening-statement_I178140-V_v.

increasingly complex toolbox composed of numerous compartments governed by different institutional arrangements and decision-making procedures, whereby the EU foreign and security policy (EUFSP) has expanded beyond the relatively limited diplomatic-military remit of the CFSP/CSDP. How to mobilise the different instruments and apply them in a concerted manner has become an increasingly pressing and complicated question to answer.

This report aims to unpack this complexity by exploring how and why EUFSP has become more multi-sectoral over the past decades. It focuses on policy tools that sustain EU crisis and conflict management efforts. Following the introduction, the second part of the report analyses the internal and external factors that have shaped the development of a more multi-sectoral EUFSP and then provides an overview and assessment of two key areas: diplomacy and crisis management. The third part will take a closer look at a selection of more recent and dynamic instruments in three fields: military, cybersecurity and intelligence capabilities, which are all vital for the EU's ability to manage contemporary conflicts and crises. Finally, the report draws conclusions on the successes and failures of a multi-sectoral approach, highlighting three challenges identified while analysing the evolution of the instruments. First, as the EU's scope of activity and level of ambition have increased, the need to *strengthen the "harder end" of instruments* has been widely acknowledged, but these remain weak compared to the EU's soft, civilian/non-coercive tools. Second, due to growing "multi-sectorness" extending to areas where the EU's resources and competencies are weak, the need to *mobilise member states' resources and cooperate and coordinate with other actors* has become more important but ensuring meaningful contributions from member states in particular has proven difficult. Third, it has become an ever more complex task to *connect the multiple sectors to each other to build a comprehensive policy*.

1. Conceptualisation, overview and assessment of the increasingly multi-sectoral EUFSP

1.1 Internal and external pressure towards growing multi-sectorness

The growing multi-sectorness of EUFSP during the past decades can be explained by an interplay of internal and external factors. Internally, deepening integration

has brought new policy areas to the EU's agenda and gradually extended EU competencies in areas traditionally belonging to the realm of national sovereignty. Since the 1950s, this process has at times accelerated, and at times stood still, but overall, one can argue that there has been a functionalist logic of integration extending from one sector to another, with spill-over effects triggering further cooperation. For example, economic and trade integration had implications for member states' relations with third countries, contributing to closer coordination of their foreign and security policies. It has also been argued that foreign policy integration has followed the logic of internal functionality in the sense of being a vehicle for further evolution of the European project.[3]

While the internal logic of functionality has pushed integration forward, the principles of intergovernmentalism and national sovereignty have remained strong in the realm of foreign and security policy, which is visible in the development of EUFSP instruments. Even in the most integrated aspect of the EU's external relations, trade, the growing complexity and stronger political aspects of trade agreements have made it more difficult to gain the approval of all member states for new deals. In the field of diplomacy, foreign policy integration has not reduced member states' investment in their own diplomatic tools (e.g. diplomatic staff and networks of embassies) which in the case of larger member states is far larger than the European External Action Service (EEAS) that comprises the diplomatic arm of the EU.[4] EU foreign policy can be seen to entail both the policies institutionalised at the EU level and national foreign policies, although in practice member states' actions are not always aligned with what has been commonly agreed at the EU level. National instruments can be applied to the benefit of the EU as a whole, for example, with member states allocating part of their development cooperation funds through the EU. Furthermore, on some occasions, national foreign ministers have conducted negotiations with third countries on behalf of the Union. However, there is a vast unused potential in actually making member states' foreign policy instruments available to the EU and using them to implement jointly agreed EU policies.

---

3 Christopher J. Bickerton, *European Union Foreign Policy: From Effectiveness to Functionality*, Basingstoke, Palgrave Macmillan, 2011.

4 Rosa Balfour, Caterina Carta and Kristi Raik, "Conclusions: Adaptation to the EU or to the Changing Global Context?", in Rosa Balfour, Caterina Carta and Kristi Raik (eds), *The European External Action Service and National Foreign Ministries. Convergence or Divergence?*, Farnham, Ashgate, 2015, p. 197.

The tension between supranational and intergovernmental elements of EUFSP, and possible ways to move beyond the dichotomy, has been extensively covered in earlier studies.[5] However, the dichotomy remains visible in the different institutional structures and policy-making procedures in different areas of EUFSP. The institutional and procedural complexity is an important feature of the multi-sectorness of EUFSP that reduces its consistency and effectiveness. New measures to improve consistency and coordination have been introduced with treaty changes since Maastricht, especially with the Lisbon Treaty that created the European External Action Service.[6] Yet coordination among institutions, notably the EEAS and the Commission, and between the EU and national institutions remained a major challenge.[7]

Externally, the changing international environment has created new demands and opportunities for a stronger EU foreign and security policy. In the 1970s, European foreign policy coordination was enhanced in the shadow of bipolar competition between the two superpowers of the time, the United States and the Soviet Union. Quite like today, Europeans – especially the French – were motivated to pursue a more independent foreign policy that was not always in agreement with the United States (with visible tensions in the transatlantic relationship over issues such as the Middle East, Afghanistan and Poland).[8]

The collapse of the Eastern bloc and the end of the Cold War created an entirely new external environment where the EU and the United States agreed on the strategic goals to reunify Europe and extend liberal democracy and market economy to the former Eastern bloc, while the EU had an indispensable role to play

---

5 E.g., ibid.; Josep Bátora, "The 'Mitrailleuse Effect': The EEAS as an Interstitial Organization and the Dynamics of Innovation in Diplomacy", in *Journal of Common Market Studies*, Vol. 51, No. 4 (July 2013), p. 598-613; Jolyon Howorth, "Decision-Making in Security and Defense Policy: Towards Supranational Inter-Governmentalism?", in *Cooperation and Conflict*, Vol. 47, No. 4 (December 2012), p. 433-453.

6 Jean-Claude Piris, *The Lisbon Treaty: A Legal and Political Analysis*, Cambridge, Cambridge University Press, 2010.

7 Christophe Hillion and Steven Blockmans, *From Self-Doubt to Self-Assurance. The European External Action Service as the Indispensable Support for a Geopolitical EU*, Brussels, CEPS/SIEPS/FES, January 2021, https://www.sieps.se/en/publications/2021/from-self-doubt-to-self-assurance.

8 Hazel Smith, *European Union Foreign Policy. What It Is and What It Does*, London/Sterling, Pluto Press, 2002, p. 127-135.

in pursuing these goals. At the same time, the wars in former Yugoslavia and the fragile security situation in many other parts of the former Eastern bloc called for a stronger EU contribution to European security beyond the Union's borders. This new context contributed to the establishment of the CFSP and the emergence of enlargement as a major, as well as distinctly multi-sectoral, foreign policy tool focused on securing democracy, stability and economic development in Europe.

The new post-Cold War environment also explains the rise of crisis management as a major priority of CSDP, with the first missions located in the Western Balkans. Furthermore, the specific shape of EU crisis management, with a focus on civilian tools and long-term involvement in post-conflict reconstruction, reflects both the internal nature of the EU and the broader international trends at the time. The EU's internal historical experience of securing peace through integration has been reflected in the emphasis put on the institution-building and integration of the Western Balkan countries into the Union. Externally, the end of Cold War confrontations reduced the relevance of military power, in spite of the Yugoslav wars happening right next door and underscoring the EU's inability to prevent the fighting or to intervene. Although war was still a reality in one corner of Europe, in a longer-term perspective the future of European security depended to a large extent on the success of political and economic transformation in post-Communist countries and beyond, which highlighted the need for a broader set of tools. Internally, the EU built its foreign policy identity strongly on the notions of civilian and normative power (the latter not excluding the use of military instruments, but nonetheless stressing a non-military approach). In an attempt to turn the lack of military capabilities into a virtue – or reflecting a conviction that a civilian approach was indeed the EU's particular strength and advantage – the EU (and a host of EUFSP research) emphasised the unique nature of its international actorness.[9]

Since the mid-2000s, the European and international security environment has become more conflictual, complex and unpredictable. This is evident in the contrast between the European Security Strategy of 2003 and the EU Global Strategy of

[9] E.g., François Duchêne, "The European Community and the Uncertainties of Interdependence", in Max Kohnstamm and Wolfgang Hager (eds), *A Nation Writ Large? Foreign-Policy Problems before the European Community*, London/Basingstoke, Palgrave Macmillan, 1973, p. 1-21; Ian Manners, "Normative Power Europe: A Contradiction in Terms?", in *Journal of Common Market Studies*, Vol. 40, No. 2 (June 2002), p. 235-258.

2016. While the priorities of EUFSP remained largely the same, the latter points to a host of new challenges, highlighting the need to "enhance our efforts on defence, cyber, counterterrorism, energy and strategic communications".[10] The strategy also calls for stronger intelligence capabilities to achieve "better and shared assessments of internal and external threats and challenges".[11] These instruments are part of an "integrated approach" to conflicts and crises – a concept introduced by the Global Strategy, building on earlier efforts to develop a "comprehensive approach".[12] The need to strengthen the harder end of EUFSP instruments has been dictated by external factors, while the EU's readiness to move ahead has been weakened by internal political factors such as lack of a common strategic culture and shared threat perceptions. Arguably today, while the regional and global security environment makes strengthening EUFSP more necessary than ever, stronger internal cohesion is more difficult to achieve.

1.2 Assessing the evolution of EU diplomacy and crisis management

As noted above, the EU's diplomatic tools made a leap forward with the Maastricht Treaty that established the CFSP. The creation of the institutions of the High Representative (HR) for CFSP (1999), a post later merged with that of the External Action Commissioner into an empowered High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission (HRVP) (2009), and the EEAS (also in 2009) strengthened the EU's diplomatic capacity. Yet the Union's achievements in managing conflicts and crises have been modest. Weak political unity, institutional cohesion and policy instruments, including hard power to back up soft tools, are frequently cited reasons for the limited success. A brief look at four different cases – the wars in ex-Yugoslavia in the 1990s, in Georgia in 2008 and in Libya in 2011, and the talks over Iran's nuclear programme – illustrates the limits of EU diplomacy.

---

10 European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, June 2016, p. 9, https://europa.eu/!Tr66qx.

11 Ibid., p. 45.

12 European Commission and High Representative of the Union, *The EU's Comprehensive Approach to External Conflict and Crises* (JOIN/2013/30), 11 December 2013, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52013JC0030. For a brief analysis and comparison of the concepts, see Thierry Tardy, "The EU: From Comprehensive Vision To Integrated Action", in *EUISS Briefs*, No. 5 (February 2017), https://www.iss.europa.eu/node/1297.

The newly created CFSP experienced a "baptism of fire" in the 1990s conflicts related to the breakup of Yugoslavia.[13] Diplomacy was the EU's main tool to address the conflicts, complemented by economic benefits, sanctions and humanitarian aid. The United States initially chose to stay in the background, pushing the EU to lead, for the first time ever, mediation between warring parties in the bloodiest conflict in Europe since WWII. The EU's failures led to the United States (and NATO) taking action to end the war. Many observers were highly critical of the EU's contribution,[14] although its impact and growth in maturity during the process was also acknowledged.[15] One of the conclusions drawn was that the EU needed to improve the functioning of its CFSP and create an operational defence capability, to be better prepared to deal with other conflicts in its neighbourhood.[16]

The six-day war in Georgia in August 2008 was another occasion where the United States pushed Europeans to take the initiative. France, who held the presidency of the Council at the time, took the lead in brokering a ceasefire between Tbilisi and Moscow on behalf of the EU. It achieved the goal of ending the war and stopping Russia from entering deeper into Georgia's territory. However, since then the EU has failed to push back Russia's military presence in Abkhazia and South Ossetia and ensure respect for Georgia's territorial integrity, which it highlights in principle. The EU declined to use other instruments, such as sanctions, to push Russia to fully implement the ceasefire agreement and withdraw its military to the line where it had been before the war.[17] Instead, it quickly restored normal diplomatic ties and cooperation with Russia. Arguably, the Russian side took this as a signal that it could get away with military aggression and use force to regain influence in the post-Soviet space. Therefore, the EU's partial diplomatic success can be characterised as a failure of multi-sectorness.

---

13 Roy H. Ginsberg, *The European Union in International Politics. Baptism by Fire*, Lanham, Rowman and Littlefield, 2001.

14 E.g. Richard Holbrooke, To End a War, New York, Random House, 1998; Philip H. Gordon, "Europe's Uncommon Foreign Policy", in *International Security*, Vol. 22, No. 3 (Winter 1997/1998), p. 74-100.

15 Roy H. Ginsberg, The European Union in International Politics, cit.; John Peterson, "US and EU in the Balkans: 'America Fights the Wars, Europe Does the Dishes'?", in *EUI Working Papers RSC*, No. 2001/49 (2001), http://hdl.handle.net/1814/1758.

16 Roy H. Ginsberg, *The European Union in International Politics*, cit.

17 Ronald D. Asmus, *A Little War that Shook the World. Georgia, Russia, and the Future of the West*, New York, Palgrave Macmillan, 2010, p. 189-214.

The EU was again expected by the United States to take the lead in responding to the civil war in Libya in 2011, given how strongly France and the United Kingdom pushed for a military intervention. However, the EU failed to take up a prominent role apart from providing humanitarian aid, while the international response became focused on military intervention. In a rare show of diplomatic disunity, EU countries failed to reach a common position in the United Nations Security Conflict (UNSC), with Germany, an elected UNSC member at the time, abstaining in a vote on the authorisation of a military intervention, along with Brazil, China, India and Russia. France and the United Kingdom took the lead in imposing a no-fly zone, authorised by UNSC Resolution 1973 and relying on a NATO framework to enforce. US military involvement turned out to be critical, exposing the weakness of European forces. The conflict highlighted the lack of a common strategic culture of EU member states.

The EU's diplomatic engagement emerged as a more appropriate instrument in addressing Iran's nuclear programme. In 2003–5, the E3 and the HR (E3/EU) tried to obtain from the Iranians objective guarantees that their nuclear programme only had peaceful aims. When the talks failed in early 2006, the EU HR played a leading role in a renewed and expanded diplomatic process that eventually led to the conclusion of the Joint Comprehensive Plan of Action (JCPOA) in 2015. The agreement involving the "E3/EU+3" – China, France, Germany, Russia, the United Kingdom and the United States – and Iran was celebrated as a major achievement of EU diplomacy. The JCPOA seeks to ensure Iran's nuclear programme will be exclusively peaceful. Implementation of the programme was the condition for the EU to lift its nuclear-related economic and financial sanctions against Iran, which it did in 2016. However, the unilateral withdrawal of the United States from the JCPOA in 2018 dealt an almost fatal blow to the programme, yet again highlighting the EU's lack of capacity for autonomous action.[18]

To complement the evolution of EU diplomacy, CSDP was launched in 1999 with the primary task of planning and conducting crisis management operations.[19] Since

[18] Riccardo Alcaro, "Europe's Defence of the Iran Nuclear Deal: Less than a Success, More than a Failure", in *The International Spectator*, Vol. 56, No. 1 (March 2021), p. 55-72, https://doi.org/10.1080/03932729.2021.1876861; Riccardo Alcaro, *Europe and Iran's Nuclear Crisis. Lead Groups and EU Foreign Policy-Making*, Basingstoke/New York, Palgrave Macmillan, 2018.

[19] Giovanni Grevi, "ESDP institutions", in Giovanni Grevi, Damien Helly and Daniel Keohane (eds),

then the EU has launched 35 missions and operations, covering a wide spectrum of civilian and military tasks and all stages of conflict from prevention to intervention and peacebuilding. The first operations were introduced in the favourable political and security environment of the early 2000s, when the EU's own security was assessed to be stronger than ever, the Union was widening and deepening, and domestic and external expectations for the EU to become a stronger international actor were high.[20] In subsequent years, CSDP missions and operations became an important part of the EU's response to conflicts in the neighbourhood and beyond, including the Western Balkans, Georgia, Ukraine, Libya, the Democratic Republic of Congo (DRC) and Somalia.

The CSDP missions and operations have had mixed results.[21] They have had some success in reaching the mandated goals, but these have often been rather limited, reflecting the EU's low level of ambition as a crisis manager. The EU has generally not been good at conflict prevention and rapid response, which would usually be the most cost-effective approach. Sometimes it has failed to establish a mission in situations where there was an obvious need and a high expectation for it to do so, most notably in Libya in 2011, characterised as the "archetypical scenario for which the CSDP had been preparing to assume leadership".[22] Political disagreements and limited readiness of member states to contribute intelligence and other capabilities have been major obstacles. Institutional coherence has also been a challenge, although the institutional set-up has gradually improved. Over time, CSDP missions have become more embedded in the EU's broader foreign policy goals.[23]

The EU has highlighted the need for a comprehensive, or more recently "integrated", approach bringing together civilian and military assets. Yet the relationship and

European Security and Defence Policy: The First Ten Years (1999-2009), Paris, EUISS, 2009, p. 19, https://www.iss.europa.eu/node/611.

20 Christoph O. Meyer, "CSDP Missions and Operations", in *European Parliament In-Depth Analysis*, January 2020, p. 4, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_IDA(2020)603481.

21 Ibid.

22 Jolyon Howorth, "The Lisbon Treaty, CSDP and the EU as a Security Actor", in Mario Telò and Frederik Ponjaert (eds), *The EU's Foreign Policy. What Kind of Power and Diplomatic Action?*, Farnham, Ashgate, 2013, p. 72. (The EU did launch a border assistance mission to Libya in 2013.)

23 Christoph O. Meyer, "CSDP Missions and Operations", cit.

finding the right balance between civilian and military activities has remained a contentious issue. There has been a growing political emphasis on the need for more substantial military capabilities, but modest progress, as described below. At the same time, the civilian dimension has been arguably overshadowed by the political focus on military capabilities.[24] This stands in contrast to the EU's actual activities and relative strengths as an international security actor. A majority of CSDP operations (22 out of 35) have been categorised as purely or predominantly civilian in nature.[25] Indicating shifting political priorities, member states' contribution of personnel to civilian missions dropped from almost 2,000 in 2010 to around 700 in 2019.[26]

By 2020, the focus of CSDP had moved towards protection of the EU and its citizens, as highlighted in the Global Strategy. This led analysts to ask "whether CSDP has outgrown the 'crisis management' paradigm"[27] and to call for the definition of a "narrower set of key priorities".[28] According to some critics, "heavy politicization of CSDP since the adoption of EUGS" narrowed and hampered the work of CSDP missions.[29] Both external and domestic demands on EU crisis management have changed, necessitating a review of the appropriate goals and instruments which is ongoing as the Union is preparing a "strategic compass".[30]

---

24 Ana E. Juncos, "Beyond Civilian Power? Civilian CSDP Two Decades On", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 74-85, https://www.iss.europa.eu/node/2423.

25 Christoph O. Meyer, "CSDP Missions and Operations", cit., p. 5.

26 Timo Smit, "Towards a More Capable European Union Civilian CSDP", in *SIPRI Policy Briefs*, November 2019, https://www.sipri.org/node/4947.

27 Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 4, https://www.iss.europa.eu/node/2423.

28 Nicole Koenig, "Crisis Management", in Christian Mölling and Torben Schütz (eds), "The EU's Strategic Compass and Its Four Baskets. Recommendations to Make the Most of It", in *DGAP Reports*, No. 13 (November 2020), p. 6, https://dgap.org/en/node/34620.

29 Tobias Pietz, "EU Crisis Management: Back to the Future", in *Internationale Politik Quarterly*, No. 4/2021 (October 2021), https://ip-quarterly.com/en/node/35349; Nicoletta Pirozzi, "The Civilian CSDP Compact. A Success Story for the EU's Crisis Management Cinderella?" in *EUISS Briefs*, No. 9 (October 2018), https://www.iss.europa.eu/node/2270.

30 Christian Mölling and Torben Schütz (eds), "The EU's Strategic Compass and Its Four Baskets. Recommendations to Make the Most of It", in *DGAP Reports*, No. 13 (November 2020), https://dgap.org/en/node/34620.

2. Case studies on some relatively new and dynamic policy tools

2.1 Military tools

The EU itself has few military tools. Most elements of its military power – personnel, units and assets – are retained by the member states and made available to the Union for specific time-limited purposes. Nonetheless, over the course of more than thirty years, the EU has developed a small set of military tools that may broadly be divided into two categories: tools for the planning and conduct of military operations (e.g. military staff within the EU's External Action Service, the EU Battlegroups); and tools to encourage the cooperative development of military capability, namely the European Defence Fund (EDF) and the Permanent Structured Cooperation (PESCO). However, member states have continued to insist on sovereignty in defence, and practical cooperation and integration have remained below the levels necessary to deliver the high common level of ambition they have agreed to politically.[31] Presently, the EU is able to operate militarily only at the lower end of the aspirations it has articulated.[32]

Planning and conduct of operations: The MPCC

In the past twenty years, the EU has developed a limited capacity for planning and conducting operations at the military-strategic level by creating staff elements such as the EU Operations Centre (2012–2016), and the Military Planning and Conduct Capability (MPCC) established in 2017. Several member states – notably, before Brexit, the United Kingdom – have strongly opposed the creation of larger, permanent military command structures.[33]

---

31 Claudia Major and Christian Mölling, "The EU's Military Legacy", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 39, https://www.iss.europa.eu/node/2423; Council of the EU, *Council Conclusions on Implementing the EU Global Strategy in the Area of Security and Defence* (14149/16), 14 November 2016, p. 15, https://data.consilium.europa.eu/doc/document/ST-14149-2016-INIT/en/pdf.

32 Douglas Barrie et al., *Protecting Europe: Meeting the EU's Military Level of Ambition in the Context of Brexit*, London, International Institute for Strategic Studies (IISS), November 2018, p. 3, https://dgap.org/system/files/article_pdfs/protecting_europe.pdf.

33 Sarah Lain and Veerle Nouwens, "The Consequences of Brexit for European Defence and Security", in *RUSI Occasional Papers*, April 2017 (updated August 2017), p. 11, https://rusi.org/explore-our-research/publications/occasional-papers/consequences-brexit-european-defence-and-

A military-strategic headquarters in the command chain between the political-strategic level and the force/theatre headquarters, known in the EU as an Operation Headquarters (OHQ), provides for improved common strategic culture, situational awareness and contingency planning, rapid response, demarcation of operational responsibilities, and coordination of a comprehensive approach to crisis management.[34] It is thus a vital instrument for the effective and efficient conduct of crisis management operations. But in the early 2000s, concerns about unnecessarily duplicating NATO structures meant that an OHQ was not among the newly created EU military structures, and the EU Military Staff (EUMS) was specifically prohibited from taking on this role.[35] Instead, the EU was to make use of either national OHQs or NATO's Supreme Headquarters Allied Powers in Europe (SHAPE), made available to it under the 2002 Berlin Plus agreement.

Around 2016, a combination of factors, including a changing threat environment, Brexit, and the uncertainties of the presidency of Donald Trump in the United States, persuaded many policymakers that Europe should become more self-reliant in defence and develop more tools at the EU level to underpin the ambition of a "stronger Europe".[36] This included creating a Military Planning and Conduct Capability (MPCC) in the EUMS, which both reflects common practice for conducting national and multinational military operations and aims to address the weaknesses of the alternatives. Berlin Plus is politically difficult, not least for an EU that strives for greater autonomy, and seems, in one of the only two cases it has

security.

34 Nik Hynek, "EU Crisis Management After the Lisbon Treaty: Civil-Military Coordination and the Future of the EU OHQ", in *European Security*, Vol. 20, No. 1 (2011), p. 95-97; Maurice de Langlois and Andreas Capstack, "The Role of the Military in the EU's External Action: Implementing the Comprehensive Approach", in *Laboratoires de l'IRSEM*, No. 23 (2014), p. 33, https://www.defense.gouv.fr/content/download/327813/4516088/file/Laboratoire%20n%C2%B023%20(En).pdf; Luis Simon, "The Spanish Presidency and CSDP: Time to Get Serious about the Union's Military Planning and Conduct Capability", in *Analyses of the Elcano Royal Institute (ARI)*, No. 33/2010 (February 2010), p. 7-8, http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari33-2010.

35 See "Military Bodies in the European Union and the Planning and Conduct of EU-led Military Operations" (the so-called "Toolbox Paper" presented to the meeting of EU Defence Ministers in Sintra, Portugal, 28 February 2000), in Maartje Rutten (ed.), "From St-Malo to Nice. European Defence: Core Documents", in *Chaillot Papers*, No. 47 (May 2001), p. 96, https://www.iss.europa.eu/node/172.

36 Pauli Järvenpää, Claudia Major and Sven Sakkov, *European Strategic Autonomy. Operationalising a Buzzword*, Tallinn, International Centre for Defence and Security (ICDS), October 2019, p. 3-6, https://icds.ee/en/?p=46602; EEAS, *Shared Vision, Common Action: A Stronger Europe*, cit., p. 7.

been applied (Operation Althea in Bosnia), to have been a source of coordination problems between the strategic and operational levels.[37] The use of national HQs, meanwhile, has led to problems such as planning delays, bureaucratic conflict and friction related to the creation of a multinational HQ around a national core.[38]

The MPCC currently acts as the OHQ for all EU non-executive military missions, i.e., the training missions in Somalia, Mali, and the Central African Republic, and is to be scaled up to a permanent strength of sixty seconded military and civilian officers. In crisis, it can be augmented by a further 94 staff, allowing it to command up to 2,500 troops – an EU Battlegroup – although no such opportunity has so far arisen.[39] It reports to and receives direction from the member states through the Political and Security Committee and the EU Military Committee.

The MPCC is thus another piece in the jigsaw of the command and control arrangements the EU will most likely require if it is to become a serious actor in defence. It has the potential to overcome the shortcomings of previous arrangements but has so far remained largely untested.

Capability development: PESCO

The EU has developed several tools intended to encourage the cooperative development of military capability. While not crisis management instruments per se, these inward-facing instruments are needed to stimulate the development of the military capability widely acknowledged to be lacking in the member states. The rationale for EU-level involvement includes a number of ideas. While capability development remains in the hands of the member states, some degree of (supranational) coordination is necessary if their efforts are to be brought

---

37 Ivana Boštjančič Pulko, Meliha Muherina and Nina Pejič, "Analysing the Effectiveness of EUFOR Althea Operation in Bosnia and Herzegovina", in *European Perspectives*, Vol. 8, No. 2 (October 2016), p. 98, https://www.cep.si/wp-content/uploads/2017/07/2016-8-2.pdf.

38 For example: Bjoern H. Seibert, *Operation EUFOR TCHAD/RCA and the European Union's Common Security and Defense Policy*, Carlisle, US Army War College Strategic Studies Institute, October 2010, p. 50-52, https://press.armywarcollege.edu/monographs/592; Helmut Fritsch, "EUFOR RD Congo: A Misunderstood Operation?", in *Martello Papers*, No. 33 (2008), p. 71-72, https://www.queensu.ca/cidp/sites/webpublish.queensu.ca.cidpwww/files/files/publications/Martellos/Martello33.pdf.

39 EEAS, *Factsheet: The Military Planning and Conduct Capability (MPCC)*, November 2018, p. 2, https://europa.eu/!fm43Fj.

together into a coherent whole. The member states also need to be encouraged to put aside national sentiments and pursue the common development of capability that will ensure economies of scale and enhance interoperability. Peer pressure amongst partners will encourage them to do more than they might otherwise do on a national basis. These tools have included prominent initiatives such as the Headline Goal, the European Capabilities Action Plan, the Headline Goal 2010, and Pooling and Sharing, as well as more routine processes such as the Capability Development Plan and the European Defence Agency's research and development programmes. The present weak state of European defence, however, offers little evidence that either they or similar initiatives and processes in NATO have succeeded in encouraging the member states to invest more, and more cooperatively, to address longstanding capability shortfalls.[40]

Three further EU-level programmes were introduced in 2016. The Coordinated Annual Review on Defence (CARD), while important, is essentially a beefed-up planning and assessment tool. The other two programmes contain novel elements suggesting they might be more effective than their predecessors: the Permanent Structured Cooperation requires participating Member States (pMS) to make legally binding commitments to each other, while the European Defence Fund provides, for the first time, EU-level financial incentives for collaborative defence research and development.

PESCO was implemented by activating dormant articles of the Lisbon Treaty[41] and its contribution to EU crisis management efforts is twofold. First it requires pMS to broadly step up their defence efforts by making a range of commitments to each other, the legal standing of which is intended to encourage a higher level of compliance than earlier, more voluntary agreements.[42] The pMS thus agreed to fulfil twenty "more binding commitments" and to submit to an annual assessment of their performance by the Council on the basis of a report by the

[40] European Defence Agency, *2020 CARD Report: Executive Summary*, November 2020, https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf.

[41] European Union, *Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union*, OJ C 202, 7 June 2016, articles 42(6) and 46, and additional protocol 10 of the Treaty of Lisbon, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG.

[42] Sven Biscop, "European Defence: Give PESCO a Chance", in *Survival*, Vol. 60, No. 3 (2018), p. 162-163.

High Representative.[43] Among these are commitments to make available military formations for the realisation of the EU level of ambition, to provide substantial support for EU missions and operations and to substantially contribute to the EU battlegroups.[44] Other commitments aimed at improving military capability are intended to ensure that the member states have the means to support these crisis management commitments.

Analysts have observed, however, that most of the commitments are vaguely worded, making it hard to assess whether they have been achieved, and that they do not conform to a clear strategic outlook.[45] The EU's own first strategic review of PESCO in 2020 agreed that "the more binding commitments [...] have proven to present a solid guideline in ensuring consistent implementation of PESCO and must therefore not be changed". However, it also suggested that performance shortfalls in operational commitments and in the implementation of a European collaborative approach meant that the "establishment of indicative measurable objectives with related progress indicators" would need to be discussed.[46]

The pMS also committed to "take part in at least one project under the PESCO which develops or provides capabilities identified as strategically relevant by Member States".[47] The cooperative military capability development projects are PESCO's second, better-known contribution to EU crisis management. They are implemented by smaller groups of pMS, with existing EU structures and a PESCO secretariat providing governance and coordination.[48] So far, 46 projects have been

---

43 Council of the EU, *Council Decision (CFSP) 2017/2315 of 11 December 2017 Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States*, 11 December 2017, articles 3 and 6, https://eur-lex.europa.eu/eli/dec/2017/2315/oj.

44 Ibid., Annex, para 12.

45 For example: Niklas Nováky, "The EU's Permanent Structured Cooperation in Defence: Keeping Sleeping Beauty from Snoozing", in *European View*, Vol. 17, No. 1 (April 2018), p. 101, https://doi.org/10.1177/1781685818764813; Sven Biscop, "European Defence and PESCO: Don't Waste the Chance", in *EU IDEA Policy Papers*, No. 1 (May 2020), p. 7, https://euidea.eu/?p=1018; Justyna Gotkowska, "The Trouble with PESCO. The Mirages of European Defence", in *OSW Point of View*, No. 69 (February 2018), p. 20, https://www.osw.waw.pl/en/publikacje/point-view/2018-03-01/trouble-pesco.

46 Council of the EU, *Council Conclusions on the PESCO Strategic Review 2020* (13188/20), 20 November 2020, p. 12, https://data.consilium.europa.eu/doc/document/ST-13188-2020-INIT/en/pdf.

47 Council of the EU, *Council Decision (CFSP) 2017/2315*, cit., Annex, para 17.

48 Ibid., Article 4, 7.

initiated.[49] The Council has welcomed the fact that 26 of these are expected to deliver concrete results or reach full operational capability by the end of the current PESCO phase (2025).[50]

Analysts, though, have noted that while PESCO projects are a step in the right direction, they tend to be at the low end of the capability spectrum and will not address shortfalls in the EU level of ambition. Some have not (and may never) advance beyond a conceptual stage. They include many projects that would have gone ahead, PESCO or not. Besides, they are fragmented, rather than aimed towards the EU's goal of arriving at a "coherent full spectrum force package".[51] The Council, too, appears to have recognised the need for a more interventionist approach to managing the PESCO project portfolio if this otherwise "Member States-driven" process is to reach its full potential, and has floated the need for the PESCO secretariat to take a "stronger advisory role".[52]

Capability development through PESCO is further complicated by the fact that most pMS are also NATO allies, creating a tension between the EU's agenda and the NATO Defence Planning Process. While PESCO projects could, in theory, be used to satisfy both EU and NATO capability targets, in practice national defence planners are torn between national, NATO and EU requirements and many pMS privilege the first two of these over the third.[53] While both organisations recognise the problem, they have only been able to agree on weak solutions such as staff-to-staff contacts and attendance at each other's meetings.[54]

---

49 See PESCO official website: https://pesco.europa.eu.

50 Council of the EU, *Council Conclusions on the PESCO Strategic Review 2020*, cit., Appendix 2.

51 For example: Alice Billon-Galland and Yvonni-Stefania Efstathiou, "Are PESCO Projects Fit for Purpose?", in *ELN/ISS Defence Policy Briefs*, 20 February 2019, p. 12, https://www.europeanleadershipnetwork.org/?p=8542; Sven Biscop, "Strategic Choices for the 2020s", in *Security Policy Briefs*, No. 122 (February 2020), p. 3, https://www.egmontinstitute.be/?p=35796; Council of the EU, *Council Decision (CFSP) 2017/2315*, cit., Annex I.

52 Steven Blockmans and Dylan Macchiarini Crosson, "PESCO: A Force for Positive Integration in EU Defence", in *European Foreign Affairs Review*, Vol. 26, Special Issue (2021), p. 105, https://www.ceps.eu/?p=34001.

53 Daniel Fiott, "Capability Development", in Christian Mölling and Torben Schütz (eds), "The EU's Strategic Compass and Its Four Baskets. Recommendations to Make the Most of It", in *DGAP Reports*, No. 13 (November 2020), p. 11, https://dgap.org/en/node/34620; Sven Biscop, "EU and NATO Strategy: A Compass, a Concept, and a Concordat", in *Security Policy Briefs*, No. 141 (March 2021), p. 5, https://www.egmontinstitute.be/?p=38842.

54 North Atlantic Treaty Organization (NATO), *Common Set of New Proposals on the*

2.2 Cyber tools

The issue of cybersecurity and defence rose to the top of the EU security agenda in 2007, after Russia committed cyberattacks on public and private institutions in Estonia. Since then, the cyber field has grown in importance for the EU, and unlike traditional foreign policy questions, it bridges the internal-external policy and civil-military divides.

There are two dimensions to EU activities in the cyber realm: first, creating EU policies, standards and institutions that protect member states and EU institutions against cyberthreats; and second, conducting cyber diplomacy to promote norms and standards with partners around the world and cooperating with international security bodies like NATO to counter cyber and hybrid threats and conduct cyberdefence. Unlike in the purely military realm, there is greater complementarity between the EU and NATO on cyber and other hybrid threat areas.

Despite the significant number of activities in the cyber field and recent strategic frameworks, the EU needs to develop further measures to be a successful cybersecurity actor both internally and externally. Cybersecurity and cyberdefence are an important aspect of the EU's foreign and security policy, but they need to be further integrated into, and used in coordination with, traditional foreign policy instruments.

Development of EU cybersecurity instruments

The EU's cybersecurity tools have the primary task of improving cybersecurity for member states. The institutions and policies the EU has set up to protect its digital systems serve as a basis for the EU's external cyber activities, especially cyber diplomacy and creating cyber norms. The EU's policy trajectory has moved toward ever-increasing integration and Europeanisation of the cyber realm. The most comprehensive EU policy addressing both internal and external cyber

Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, 5 December 2017, https://www.nato.int/cps/en/natohq/official_texts_149522.htm.

dimensions is the new EU Cybersecurity Strategy for the Digital Decade which the Council adopted in March 2021.[55] This strategy seeks to strengthen collective European resilience against cyberthreats and improve the EU's external efforts to set norms in cyberspace. Plans include security operations centres to create a "cybersecurity shield" for the EU, Digital Innovation Hubs and the development of further European cyber defence capabilities in cooperation with the European Defence Agency, the European Defence Fund and PESCO.[56]

Some elements of the strategy intentions are becoming reality. The Commission took steps to set up the Joint Cyber Unit which seeks to respond to large-scale incidents and will change information sharing practices from a "need to know" to a "need to share" approach, in June 2021.[57] Similarly, the Commission set up a Cybersecurity Competence Centre in Bucharest in July 2021.[58]

The EU has achieved significant steps in bringing about a more European approach to cybersecurity, especially through the 2021 digital strategy, and has done well in connecting intra-EU success in this realm to a more global agenda. Certain factors could explain this success. First, the cyber policy space is new and competencies in cybersecurity can be shared between member states and EU institutions from the beginning. EU policies towards member states seek to improve both national and EU level institutions and capabilities, leading to less competition between member states and the EU. Second, because cyberthreats are inherently transnational, and attacks frequently occur in many countries at once, responding to cyberthreats can require a multi-national approach. This lends itself to greater collaboration.

---

55 European Commission, *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN/2020/18), 16 December 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52020JC0018.

56 European Commission, *New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient*, 16 December 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.

57 European Commission, *EU Cybersecurity: Commission Proposes a Joint Cyber Unit to Step Up Response to Large-Scale Security Incidents*, 23 June 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088.

58 European Commission, *The European Cybersecurity Competence Centre and Network is Now Ready to Take Off*, 28 June 2021, https://europa.eu/!MCyuXn.

Cyber diplomacy: Norm-setting and capacity development

The EU seeks to set international norms on behaviour in cyberspace. In 2015, European Council Conclusions on Cyber Diplomacy demanded that the EU conduct cyber diplomacy around the world that "promotes and protects human rights and is grounded on the fundamental EU values of democracy, human rights and the rule of law, including the right to freedom of expression; access to information and [the] right to privacy".[59] The importance of EU cyber diplomacy is also set out in the 2016 EU Global Strategy.[60]

Concrete policy tools provide the basis for EU cyber diplomacy. In 2017, a Joint EU Diplomatic Response to Malicious Cyber Activities, or the Cyber Diplomacy Toolbox, set forth a common approach to respond to malicious activities. Rooted in a conflict prevention and cyberthreat reduction framework, the toolbox encourages the EU to "intensify cyber dialogues" and recognises the importance of diplomacy. The toolbox, for the first time, allows the EU to use restrictive measures under the CFSP against malicious cyber activities.[61]

These policy guidelines have real-world applications. The EEAS has engaged in bilateral diplomacy with various countries around the world to promote greater cooperation and cohesion between cybersecurity approaches. This activity includes bilateral "Cyber Dialogues" with government and civil society in the United States, India, Brazil, China, South Korea and Japan.[62] Other examples of cyber diplomacy and capacity-building activities include joint EU, US, and Japan-run cybersecurity training for Indo-Pacific partners.[63] Regular communication on cyber issues is not reserved for like-minded states. The EU conducts a Sino-European Task Force on Cyber Issues, under HRVP Borrell's guidance, and an EU-China ICT Dialogue under

---

59 Council of the EU, *Council Conclusions on Cyber Diplomacy* (6122/15), 11 February 2015, p. 4, https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

60 EEAS, *Shared Vision, Common Action: A Stronger Europe*, cit., p. 42.

61 Council of the EU, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities* ("Cyber Diplomacy Toolbox") (9916/17), 7 June 2017, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf.

62 European Union Institute for Security Studies (EUISS) website: *EU Cyber Direct*, https://www.iss.europa.eu/node/2220.

63 European Commission, *International Cooperation: EU, Japan and the US in Joint Cybersecurity Training*, 15 March 2021, https://europa.eu/!hnCfwB.

Commissioner Thierry Breton. No such dialogue exists with Russia.[64]

In regard to the transatlantic relationship, in addition to the Cyber Dialogue, the EU has engaged the United States in an EU-US Working Group on Cybersecurity and Cybercrime since 2010,[65] which continued throughout the Trump Administration. Most recently, the EU and United States agreed to form a bilateral Trade and Technology Council (TTC) to facilitate high level political coordination on technology and digital issues including ICTS security.[66]

Cooperation through the TTC is a core element of EU efforts to rebuild relations with the United States under the Joe Biden presidency. Rather than being peripheral to a bigger strategic and foreign policy dialogue, the TTC's efforts to establish compatible approaches on cyber and other technological issues are core to big-picture foreign policy and efforts to counter digital authoritarianism.

Cyber tools also contribute to the EU's development and global agenda. Under the EU's new Cybersecurity Strategy, more resources will be given to cyber diplomacy and capacity-building efforts. Assistance to third countries will be provided through an EU External Cyber Capacity Building Agenda. Furthermore, the EU will increase cyber dialogues with third countries, regional and international organisations and civil society, and the EU will also create an EU Cyber Diplomacy Network.[67]

Cyber defence: Deterring and responding to cyber incidents

The EU's leadership role on cyber issues also extends to its growing appetite for setting consequences for malicious cyber activity and the inclusion of cyber tools in defence policy. The adoption of the EU Cyber Diplomacy Toolbox in 2017 opened the door to using restrictive measures against malicious cyber acts. The EU

64 Patryk Pawlak, "Navigating the EU's Cyber Diplomacy", in *Directions Blog*, 25 September 2020, https://directionsblog.eu/?p=1172.

65 Dimitrios Anagnostakis, "The European Union-United States Cybersecurity Relationship: A Transatlantic Functional Cooperation", in *Journal of Cyber Policy*, Vol. 6, No. 2 (2021), p. 243-261, https://doi.org/10.1080/23738871.2021.1916975.

66 European Commission, *Factsheet: EU-US Trade and Technology Council*, October 2021, https://trade.ec.europa.eu/doclib/html/159642.htm.

67 European Commission, *New EU Cybersecurity Strategy and New Rules*..., cit.

Council adopted a framework in 2019 to permit the use of sanctions in response to malicious cyber activities,[68] and the EU used those powers to sanction eight persons and four entities (from Russia, China and North Korea)[69] over the course of 2020.[70]

Cyber defence is also an important part of the EU's Common Security and Defence Policy. The EU's first Cyber Defence Policy Framework (CDPF) was published in 2014, and cyberspace was made a domain of operations for the EU in 2018.[71] A Military Vision and Strategy on Cyberspace as a Domain of Operations will soon be released by the EU Military Committee, explaining how cyberspace works as a domain in EU CSDP missions and operations. In the future, CSDP missions in support of electoral processes may need to address the effects of cyberattacks on critical infrastructure,[72] given that the United Nations Development Programme and other bodies are already needing to address the effect of disinformation on their missions.[73] In addition, a Military CERT-Network is being developed by the European Defence Agency. The Cyber Security Strategy calls on member states to use PESCO and EDF resources for cyber defence research, innovation and capability development.[74]

Cooperation with NATO is a major element of the EU's cyber defence portfolio. A joint declaration by EU and NATO leaders at the NATO Warsaw Summit in 2016 called for greater EU-NATO cooperation,[75] and further statements defined cybersecurity and cyber defence cooperation as central to the relationship. Information sharing,

---

68 Council of the EU, *Cyber-Attacks: Council Is Now Able to Impose Sanctions*, 17 May 2019, https://europa.eu/!yp76kW.

69 Laurens Cerulus, "EU Countries Extend Sanctions Against Russian, Chinese Hackers", in *Politico*, 17 May 2021, https://www.politico.eu/?p=1709184.

70 Council of the EU, *Cyber-Attacks: Council Prolongs Framework for Sanctions for Another Year*, 17 May 2021, https://europa.eu/!CK67uW.

71 Council of the EU, *EU Cyber Defence Policy Framework (2018 Update)* (14413/18), 19 November 2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf.

72 Gustav Lindstrom, "Emerging Security Challenges", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 93, https://www.iss.europa.eu/node/2423.

73 Daniel Fiott, "As You Were?", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 114-115, https://www.iss.europa.eu/node/2423.

74 European Commission, *The EU's Cybersecurity Strategy for the Digital Decade*, cit.

75 NATO, *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133163.htm.

common training and exercises, including through the NATO Cooperative Cyber Defence Centre of Excellence, and cooperation on cyber defence innovation is a particular focus.[76] Over the past five years, significant progress has been made on common cyber staff and political consultations, exercises and concept and doctrine exchanges and consultations.[77]

Cyber cooperation with NATO entails cooperation with the US, building on the other cyber dialogues taking place across the Atlantic. Communication between the transatlantic partners is crucial because of the inherently global nature of many cyberattacks. For example, although the SolarWinds breach by Russia's cyber agents largely harmed the United States, the attack also encroached on six EU agencies.[78] Solidarity is also a prominent principle in US-EU cyber defence cooperation. Hence, the EU issued a statement in solidarity with the United States on the same day the US government imposed sanctions on Russia for the SolarWinds hack, and a few weeks later the EU further extended cyber sanctions that had already been in place.[79]

Challenges

The EU's actions in anticipating, preventing and defending member states from cyber-based security threats, while moving forward, continue to lag behind the pace of the rapid evolution of the threat itself. A growing field of malicious actors are evolving their tools and methods to extract ransoms, disrupt operations and subvert democratic institutions with growing efficiency. This reality will remain the status quo until resilient strategies are proven to interrupt profitable criminal

---

[76] NATO, *Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 6 December 2016, https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

[77] EU and NATO, *Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*, 3 June 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf.

[78] European Parliament, *Answer Given by Mr Hahn on Behalf of the European Commission* (Question P-001112/2021), 13 April 2021, https://www.europarl.europa.eu/doceo/document/P-9-2021-001112-ASW_EN.html.

[79] Julia Schuetze and Arthur de Liedekerke, "The EU's Response to SolarWinds", in *Net Politics Blog*, 26 May 2021, https://www.cfr.org/blog/eus-response-solarwinds.

business models and effectively deter nation-state operations.

The reliance on digital technologies for convenience and critical operations continues to accelerate. In 2020, this became more apparent as millions of people in the EU adapted to conducting many more aspects of their daily lives remotely because of the covid-19 pandemic. The traditional boundaries of organisations extended into the homes of their staff members, effectively linking the risks of home networks and devices to the organisation.

The EU's updated cybersecurity strategy[80] is putting cybersecurity certification schemes,[81] systems security directives,[82] and capacity-building initiatives[83] on track to become realities in the near future.

There are, however, practical limits to the efficacy of certification schemes, directives and initiatives when they are not grounded on a foundation of national deterrence. Recent cyberattacks have targeted several institutions across critical infrastructure sectors: health services in Ireland, water treatment in Norway and government in Belgium.[84] The motivations for the attacks vary but are not necessarily as important as the reason behind the growing number of successful hacks. Adversaries[85] are now operating in an environment where less-sophisticated actors can enlist the services of more technically capable actors to provide hacking tools as a service. This investment in malicious services returns a substantial profit for both criminal parties at the expense of victims who are unlikely to have any ransom returned or damages fully repaired. National investigative bodies are challenged to trace through the criminal networks to effectively attribute the source of the

80 European Commission, *Cybersecurity: Council Adopts Conclusions on the EU's Cybersecurity Strategy*, 22 March 2021, https://europa.eu/!xk33vJ.

81 European Commission, *The EU Cybersecurity Certification Framework*, last update 1 July 2021, https://digital-strategy.ec.europa.eu/en/node/9656.

82 European Commission, *Revised Directive on Security and Network Information Systems (NIS2)*, last update 8 March 2021, https://digital-strategy.ec.europa.eu/en/node/337.

83 Council of the EU, *Bucharest-based Cybersecurity Competence Centre Gets Green Light from Council*, 20 April 2021, https://europa.eu/!vk66Ur.

84 Center for Strategic and International Studies (CSIS) website: *Significant Cyber Incidents*, accessed 3 October 2021, https://www.csis.org/taxonomy/term/723.

85 Verizon, *2021 Data Breach Investigations Report*, July 2021, https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.

attacks to specific individuals. Even if identification is possible, the individuals may be harboured in a jurisdiction that is uncooperative with EU member state investigations or unwilling to prosecute extra territorial cybercriminal activities.

Evolving an effective EU strategy to mitigate cyber-based threats in an online environment that struggles to sufficiently prioritise security will always result in an asymmetric advantage to adversaries. Simply put: the EU needs to reduce the overall risk in the network environment to allow organisations, and individuals the opportunity to build resilience. This is a collective action problem, the solutions to which lies in foreign policy. Member states have not effectively engaged jurisdictions that benefit from being safe havens for cybercriminal activity in order to prevent those malicious activities from infiltrating EU borders. More traditional foreign policy, rather than cyber tools as such, would improve the overall landscape. The EU should better integrate the understanding of cyberthreats, cyber diplomacy and cyberdefence tools into its broader foreign policy outlook. That means addressing cyberthreats through traditional means (extending the approach already started with cyber sanctions) and using cyber tools in traditional foreign policy settings.

2.3 Intelligence

The need for stronger intelligence capabilities has been highlighted in the EU Global Strategy and is an important element of enhancing the EU's conflict resolution capabilities. As a union of democratic countries, the EU cannot use intelligence as a tool to interfere in decision-making processes in third countries. However, intelligence plays an important role in supporting the decision-making processes of the EU and its member states, providing early warning of harm on its way and operating as a "force multiplier" or enabler to make other EU foreign policy instruments more efficient. Support of EU missions and operations has formed the focal point of EU intelligence efforts.

The toolkit of intelligence is wide with usually five main collection disciplines: open-source intelligence (OSINT); human intelligence or espionage (HUMINT); signals intelligence (SIGINT, lately, this may also include cyber intelligence or CYBINT); imagery intelligence (IMINT); and finally, the highly technical field of measurement and signature intelligence (MASINT). EU member states possess impressive assets in all of these fields, although they largely differ country by country depending

on the resources available, the geographical location etc. However, Brexit has weakened the overall assets available for EU nations given the UK's outstanding resources in this policy areas.

In the field of intelligence, there are particularly strong constraints on making national foreign policy instruments of the member states available to collective EU policymaking. Intelligence cooperation differs from other fields of cooperation in one fundamental aspect: the sharing of information is seriously curtailed by the need to protect the collection assets (both human and technical) and the level of knowledge the services possess at a given moment. Therefore, intelligence cooperation tends to be bilateral, not multilateral.

Thus far the most successful intelligence cooperation is the Five Eyes – mainly a signals intelligence alliance between the United States, the United Kingdom, Canada, Australia and New Zealand. Even inside NATO the flow of intelligence information remains restricted. There are some publicly known cases where third country intelligence services have penetrated intelligence or counterintelligence services of NATO and EU countries; therefore, the concerns over sharing are well founded. Additionally, intelligence estimates based on the consensus of a large number of parties may become vague and lose their utility.

Hence, the nature of the EU as a multinational organisation (although with supranational elements) implies that its possibilities in bolstering intelligence capabilities are limited. However, they do exist. An important preliminary step on the way to building trust was the informal forum called the Club of Bern (Club de Berne), the roots of which go back well into the Cold War era, but which has proved useful in the counterterrorism efforts of the last decades.[86] Until recently, counterterrorism has been the central stimulus backing intelligence exchange among EU member states. Currently, the main EU body in the field of intelligence is the EU Intelligence and Situation Centre (EU INTCEN),[87] a part of the EEAS since 2011. While the terrorist threat has somewhat decreased recently, the "hybrid

[86] Gianluca Sgueo, "Counter-Terrorism Funding in the EU Budget", in *EPRS Briefings*, April 2016, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)580904.

[87] This body has grown out of the EU Joint Situation Centre which was reformed to the EU Situation Centre in 2005 (SITCEN). It became the EU Intelligence Analysis Centre (EU INTCEN) in 2012 and gained its current name in 2015, while maintaining the previous acronym.

threats" are on the rise and intelligence has a great role in facing them, both to assist in decision-making and to provide early warning. Therefore, EU INTCEN contains an EU Hybrid Fusion Cell that together with its focal points in member states is tasked to provide situational awareness for developing threats.

Obviously, the intelligence component inside the EEAS does not deal with the collection of other than open-source intelligence and it concentrates on analytical work. Together with the Intelligence Directorate of the EU Military Staff (EUMS INT), the EU INTCEN runs the EU's Single Intelligence Analysis Capacity (SIAC), but staff numbers remain limited.[88] Comprised of intelligence experts contributed by member states, SIAC analyses finished intelligence products of member states, but also open source intelligence and imagery intelligence on their own.[89] The efficiency of SIAC is bolstered by coordination with NATO, and some elements are already co-located with NATO structures.[90]

While the EU as a multinational organisation has restrictions in regard to sharing human intelligence or signals intelligence, it also has some strengths. First, it can use its advantages in regional knowledge and linguistic skills for more effective employment of open-source intelligence. Second, the EU has been successful in the field of imagery intelligence, and the EEAS – including EU INTCEN – is a consumer of the EU Satellite Centre (EU SATCEN). Its mission is to support EU decision-making in crisis management missions and operations "by providing products and services resulting from the exploitation of relevant space assets and collateral data, including satellite imagery and aerial imagery, and related services".[91] In addition to support of EU missions and operations, intelligence could be used as a force multiplier of EU aid programs and sanction regimes, providing an opportunity to assess and increase their efficiency. Probably the best example of EU gaining and collating operationally useful intelligence so far would be the

88 Raphael Bossong, "Intelligence Support for EU Security Policy Options for Enhancing the Flow of Information and Political Oversight", in *SWP Comments*, No. 51 (December 2018), https://www.swp-berlin.org/en/publication/intelligence-support-for-eu-security-policy.

89 Christophe Hillion and Steven Blockmans, *From Self-Doubt to Self-Assurance*, cit.

90 Interview with a retired intelligence officer of an EU member state with a background in international cooperation, 3 September 2021.

91 SATCEN website: *Mission, Users and Partners*, https://www.satcen.europa.eu/who-we-are/our-mission.

anti-piracy Operation Atalanta off the Horn of Africa (European Union Naval Force Somalia) that has been ongoing since 2008.[92] Furthermore, agencies like Europol and Frontex have their needs in the field of criminal intelligence where the practice of information exchange will be easier to establish than in the highly sensitive field of foreign relations.

In the framework of defence cooperation, there is a current PESCO project of the Joint EU Intelligence School (JEIS), coordinated by Greece with Cyprus presently the only other participant.[93] Two member states are obviously too few to found a really "joint" school and that may hinder the future of the project. However, there are other PESCO projects which aim to provide technological input to situational awareness. The European High Atmosphere Airship Platform – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability,[94] the European Military Space Surveillance Awareness Network[95] and the Electronic Warfare Capability and Interoperability Programme for Future Joint Intelligence, Surveillance and Reconnaissance (JISR)[96] can be mentioned in this context. The limited scope of ongoing projects leads to the conclusion that, even if their goals are fully met, they would not be sufficient to turn intelligence into an efficient EU foreign policy tool.

Conclusions

Since the 1990s, the EU has substantially increased the range of foreign policy instruments it can deploy, and thus has inevitably become more multi-sectoral. The traditional instruments of trade and aid have been accompanied by stronger diplomatic and crisis management capabilities. In recent years, the EU has paid much attention to the three new instruments explored above in more detail –

92 Interview with a retired intelligence officer of an EU member state with background in international cooperation, 3 September 2021.

93 PESCO website: *Joint EU Intelligence School (JEIS)*, https://pesco.europa.eu/?p=784.

94 PESCO website: *European High Atmosphere Airship Platform (EHAAP) – Persistent Intelligence, Surveillance and Reconnaissance (ISR) Capability (EHAAP)*, https://pesco.europa.eu/?p=802.

95 PESCO website: *European Military Space Surveillance Awareness Network (EU-SSA-N)*, https://pesco.europa.eu/?p=816.

96 PESCO website: *Electronic Warfare Capability And Interoperability Programme For Future Joint Intelligence, Surveillance and Reconnaissance (JISR)*, https://pesco.europa.eu/?p=808.

military, cybersecurity and intelligence capabilities – as indispensable, yet thus far underdeveloped, parts of its conflict management toolkit. Altogether, this has been a piecemeal development lacking any grand design, with new tools and initiatives added in reaction to both external events and internal demands, as the EU has tried to address various crises and challenges.

The report has shed light on three challenges in particular. First, the weakness of its hard power has constrained if not paralysed the EU's actions in the context of several external conflicts that have endangered European security in the past decades. The structural and political limitations run deep into the very nature of the EU and efforts to fix the problem have created new challenges. In the field of crisis management, there has been growing political attention directed at the need to strengthen military instruments. However, actual progress has been very limited. The EU's real contribution has been predominantly civilian, in line with its long-time emphasis on civilian power. Yet this contribution has weakened over the past decade, and it has been argued that the EU's civilian nature has been overshadowed by the political focus on defence. Furthermore, according to some experts, the contribution of CSDP missions and operations to international security has been negatively affected by an increased focus on member states' narrow security interests. So, one important conclusion to be drawn is that some of the EU instruments that used to be relatively strong have weakened – or at least been less frequently used – but this has not been accompanied by a significant strengthening of the harder instruments that are required for the EU to be a credible geopolitical player, or of the determination to use them.

Second, the difficulty to mobilise member states' resources is a challenge across EUFSP but is particularly pertinent in the areas of military and intelligence capabilities where the EU's ability to act depends on national contributions. The EU's reliance on the resources and actions of member states is also strong in the field of cybersecurity, including domestic, foreign and defence policy aspects. When it comes to hard security, it is an enduring political reality that the EU is not the primary framework of cooperation for many member states. The instruments that have been created at the EU level have often not been utilised or developed to their full potential.

Third, the difficulty in applying different instruments in a coordinated way is ingrained in the nature of EUFSP with its supranational and intergovernmental elements, complex inter-institutional relations and, underneath it all, limited political unity. The problem is well acknowledged and the EU has made efforts to develop a more comprehensive or integrated approach through several treaty changes, strategy documents and new initiatives – with limited success. In particular, it has tried to enhance its ability to promote the EU's overall goals and strategic interests in a consistent manner. The question of what these strategic interests are goes beyond this report; suffice it to say that there is obviously no easy answer and the difficulty in defining them is a core challenge of a multi-sectoral EUFSP.

As the international environment has grown more unstable and new threats have emerged, the EU's focus has shifted from an idealistic aim to advance global security towards a more self-centric focus on protecting the Union and its citizens. This may indeed be what the citizens and political leaders expect. However, it raises troubling questions about the EU's foreign policy identity and global influence, as well as its capacity to deliver in really protecting Europeans. Looking ahead, the EU needs continuous political work and the engagement of member states to strengthen the common understanding of the EU's strategic goals and the most appropriate means to reach them. Secondly, on a more technical level and looking at conflict management in particular, it is important to regularly exercise the multi-sectoral toolbox the EU has at its disposal. Thirdly, more efforts are required to integrate new elements such as cyber diplomacy and new defence tools into a broader foreign policy approach and enhance the actual use of the different elements of the EU's multi-sectoral toolbox.

References

Riccardo Alcaro, *Europe and Iran's Nuclear Crisis. Lead Groups and EU Foreign Policy-Making*, Basingstoke/New York, Palgrave Macmillan, 2018

Riccardo Alcaro, "Europe's Defence of the Iran Nuclear Deal: Less than a Success, More than a Failure", in *The International Spectator*, Vol. 56, No. 1 (March 2021), p. 55-72, https://doi.org/10.1080/03932729.2021.1876861

Dimitrios Anagnostakis, "The European Union-United States Cybersecurity Relationship: A Transatlantic Functional Cooperation", in *Journal of Cyber Policy*, Vol. 6, No. 2 (2021), p. 243-261, https://doi.org/10.1080/23738871.2021.1916975

Ronald D. Asmus, *A Little War that Shook the World. Georgia, Russia, and the Future of the West*, New York, Palgrave Macmillan, 2010

Rosa Balfour, Caterina Carta and Kristi Raik, "Conclusions: Adaptation to the EU or to the Changing Global Context?", in Rosa Balfour, Caterina Carta and Kristi Raik (eds), *The European External Action Service and National Foreign Ministries: Convergence or Divergence?*, Farnham, Ashgate, 2015, p. 195-208

Douglas Barrie et al., *Protecting Europe: Meeting the EU's Military Level of Ambition in the Context of Brexit*, London, International Institute for Strategic Studies (IISS), November 2018, https://dgap.org/system/files/article_pdfs/protecting_europe.pdf

Josep Bátora, "The 'Mitrailleuse Effect': The EEAS as an Interstitial Organization and the Dynamics of Innovation in Diplomacy", in *Journal of Common Market Studies*, Vol. 51, No. 4 (July 2013), p. 598-613

Christopher J. Bickerton, *European Union Foreign Policy: From Effectiveness to Functionality*, Basingstoke, Palgrave Macmillan, 2011

Alice Billon-Galland and Yvonni-Stefania Efstathiou, "Are PESCO Projects Fit for Purpose?", in *ELN/ISS Defence Policy Briefs*, 20 February 2019, https://www.europeanleadershipnetwork.org/?p=8542

Sven Biscop, “EU and NATO Strategy: A Compass, a Concept, and a Concordat”, in *Security Policy Briefs*, No. 141 (March 2021), https://www.egmontinstitute.be/?p=38842

Sven Biscop, “European Defence and PESCO: Don’t Waste the Chance”, in *EU IDEA Policy Papers*, No. 1 (May 2020), https://euidea.eu/?p=1018

Sven Biscop, “European Defence: Give PESCO a Chance”, in *Survival*, Vol. 60, No. 3 (2018), p. 161-180

Sven Biscop, “Strategic Choices for the 2020s”, in *Security Policy Briefs*, No. 122 (February 2020), https://www.egmontinstitute.be/?p=35796

Steven Blockmans and Dylan Macchiarini Crosson, “PESCO: A Force for Positive Integration in EU Defence”, in *European Foreign Affairs Review*, Vol. 26, Special Issue (2021), p. 87-110, https://www.ceps.eu/?p=34001

Josep Borrell Fontelles, *Opening statement, Hearing at the Committee on Foreign Affairs of the European Parliament*, Brussels, 7 October 2019, https://multimedia.europarl.europa.eu/en/hearing-of-josep-borrell-fontelles-high-representative-vice-president-designate-of-the-european-commission-opening-statement_I178140-V_v

Raphael Bossong, “Intelligence Support for EU Security Policy Options for Enhancing the Flow of Information and Political Oversight”, in *SWP Comments*, No. 51 (December 2018), https://www.swp-berlin.org/en/publication/intelligence-support-for-eu-security-policy

Ivana Boštjančič Pulko, Meliha Muherina and Nina Pejič, “Analysing the Effectiveness of EUFOR Althea Operation in Bosnia and Herzegovina”, in *European Perspectives*, Vol. 8, No. 2 (October 2016), p. 87-116, https://www.cep.si/wp-content/uploads/2017/07/2016-8-2.pdf

Laurens Cerulus, “EU Countries Extend Sanctions Against Russian, Chinese Hackers”, in *Politico*, 17 May 2021, https://www.politico.eu/?p=1709184

Council of the EU, *Bucharest-based Cybersecurity Competence Centre Gets Green Light from Council*, 20 April 2021, https://europa.eu/!vk66Ur

Council of the EU, *Council Conclusions on Cyber Diplomacy* (6122/15), 11 February 2015, https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Council of the EU, *Council Conclusions on Implementing the EU Global Strategy in the Area of Security and Defence* (14149/16), 14 November 2016, https://data.consilium.europa.eu/doc/document/ST-14149-2016-INIT/en/pdf

Council of the EU, *Council Conclusions on the PESCO Strategic Review 2020* (13188/20), 20 November 2020, https://data.consilium.europa.eu/doc/document/ST-13188-2020-INIT/en/pdf

Council of the EU, *Council Decision (CFSP) 2017/2315 of 11 December 2017 Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States*, 11 December 2017, https://eur-lex.europa.eu/eli/dec/2017/2315/oj

Council of the EU, *Cyber-Attacks: Council Is Now Able to Impose Sanctions*, 17 May 2019, https://europa.eu/!yp76kW

Council of the EU, *Cyber-Attacks: Council Prolongs Framework for Sanctions for Another Year*, 17 May 2021, https://europa.eu/!CK67uW

Council of the EU, *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* (9916/17), 7 June 2017, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Council of the EU, *EU Cyber Defence Policy Framework (2018 Update)* (14413/18), 19 November 2018, https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

François Duchêne, "The European Community and the Uncertainties of Interdependence", in Max Kohnstamm and Wolfgang Hager (eds), *A Nation Writ Large? Foreign-Policy Problems before the European Community*, London/Basingstoke, Palgrave Macmillan, 1973, p. 1-21

European Commission, *Cybersecurity: Council Adopts Conclusions on the EU's Cybersecurity Strategy*, 22 March 2021, https://europa.eu/!xk33vJ

European Commission, *The EU Cybersecurity Certification Framework*, last update 1 July 2021, https://digital-strategy.ec.europa.eu/en/node/9656

European Commission, *EU Cybersecurity: Commission Proposes a Joint Cyber Unit to Step Up Response to Large-Scale Security Incidents*, 23 June 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088

European Commission, *The European Cybersecurity Competence Centre and Network is Now Ready to Take Off*, 28 June 2021, https://europa.eu/!MCyuXn

European Commission, *The EU's Cybersecurity Strategy for the Digital Decade* (JOIN/2020/18), 16 December 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52020JC0018

European Commission, *Factsheet: EU-US Trade and Technology Council*, October 2021, https://trade.ec.europa.eu/doclib/html/159642.htm

European Commission, *International Cooperation: EU, Japan and the US in Joint Cybersecurity Training*, 15 March 2021, https://europa.eu/!hnCfwB

European Commission, *New EU Cybersecurity Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient*, 16 December 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

European Commission, *Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive Directive (EU) 2016/1148* (COM/2020/823), 16 December 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52020PC0823

European Commission, *Revised Directive on Security and Network Information Systems (NIS2)*, last update 8 March 2021, https://digital-strategy.ec.europa.eu/en/node/337

European Commission and High Representative of the Union, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber Space* (JOIN/2013/1), 7 February 2013, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52013JC0001

European Commission and High Representative of the Union, *The EU's Comprehensive Approach to External Conflict and Crises* (JOIN/2013/30), 11 December 2013, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52013JC0030

European Defence Agency, *2020 CARD Report: Executive Summary*, November 2020, https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf

European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, June 2016, https://europa.eu/!Tr66qx

European Parliament, *Answer Given by Mr Hahn on Behalf of the European Commission* (Question P-001112/2021), 13 April 2021, https://www.europarl.europa.eu/doceo/document/P-9-2021-001112-ASW_EN.html

European Union, *Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union*, OJ C 202, 7 June 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG

European Union and NATO, *Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017*, 3 June 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

Daniel Fiott, "As You Were?", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 110-123, https://www.iss.europa.eu/node/2423

Daniel Fiott, "Capability Development", in Christian Mölling and Torben Schütz (eds), "The EU's Strategic Compass and Its Four Baskets. Recommendations to Make the Most of It", in *DGAP Reports*, No. 13 (November 2020), p. 10-11, https://dgap.org/en/node/34620

Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, https://www.iss.europa.eu/node/2423

Helmut Fritsch, "EUFOR RD Congo: A Misunderstood Operation?", in *Martello Papers*, No. 33 (2008), https://www.queensu.ca/cidp/sites/webpublish.queensu.ca.cidpwww/files/files/publications/Martellos/Martello33.pdf

Roy H. Ginsberg, *The European Union in International Politics. Baptism by Fire*, Lanham, Rowman and Littlefield, 2001

Philip H. Gordon, "Europe's Uncommon Foreign Policy", in *International Security*, Vol. 22, No. 3 (Winter 1997/1998), p. 74-100

Justyna Gotkowska, "The Trouble with PESCO. The Mirages of European Defence", in *OSW Point of View*, No. 69 (February 2018), https://www.osw.waw.pl/en/publikacje/point-view/2018-03-01/trouble-pesco

Giovanni Grevi, "ESDP institutions", in Giovanni Grevi, Damien Helly and Daniel Keohane (eds), *European Security and Defence Policy: The First Ten Years (1999-2009)*, Paris, EUISS, 2009, p. 19-67, https://www.iss.europa.eu/node/611

Christophe Hillion and Steven Blockmans, *From Self-Doubt to Self-Assurance. The European External Action Service as the Indispensable Support for a Geopolitical EU*, Brussels, CEPS/SIEPS/FES, January 2021, https://www.sieps.se/en/publications/2021/from-self-doubt-to-self-assurance

Stanley Hoffmann, "The European Process at Atlantic Crosspurposes", in *Journal of Common Market Studies*, Vol. 3, No. 1 (1964), p. 85-101

Richard Holbrooke, *To End a War*, New York, Random House, 1998

Jolyon Howorth, "Decision-Making in Security and Defense Policy: Towards Supranational Inter-Governmentalism?", in *Cooperation and Conflict*, Vol. 47, No. 4 (December 2012), p. 433-453

Jolyon Howorth, "The Lisbon Treaty, CSDP and the EU as a Security Actor", in Mario Telò and Frederik Ponjaert (eds), *The EU's Foreign Policy. What Kind of Power and Diplomatic Action?*, Farnham, Ashgate, 2013, p. 65-76

Nik Hynek, "EU Crisis Management After the Lisbon Treaty: Civil-Military Coordination and the Future of the EU OHQ", in *European Security*, Vol. 20, No. 1 (2011), p. 81-102

Pauli Järvenpää, Claudia Major and Sven Sakkov, *European Strategic Autonomy. Operationalising a Buzzword*, Tallinn, International Centre for Defence and Security (ICDS), October 2019, https://icds.ee/en/?p=46602

Ana E. Juncos, "Beyond Civilian Power? Civilian CSDP Two Decades On", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 74-85, https://www.iss.europa.eu/node/2423

Nicole Koenig, "Crisis Management", in Christian Mölling and Torben Schütz (eds), "The EU's Strategic Compass and Its Four Baskets. Recommendations to Make the Most of It", in *DGAP Reports*, No. 13 (November 2020), p. 6-7, https://dgap.org/en/node/34620

Sarah Lain and Veerle Nouwens, "The Consequences of Brexit for European Defence and Security", in *RUSI Occasional Papers*, April 2017 (updated August 2017), https://rusi.org/explore-our-research/publications/occasional-papers/consequences-brexit-european-defence-and-security

Maurice de Langlois and Andreas Capstack, "The Role of the Military in the EU's External Action: Implementing the Comprehensive Approach", in *Laboratoires de l'IRSEM*, No. 23 (2014), https://www.defense.gouv.fr/content/download/327813/4516088/file/Laboratoire%20n%C2%B023%20(En).pdf

Gustav Lindstrom, "Emerging Security Challenges", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 88-96, https://www.iss.europa.eu/node/2423

Claudia Major and Christian Mölling, "The EU's Military Legacy", in Daniel Fiott (ed.), *The CSDP in 2020. The EU's Legacy in Security and Defence*, Paris, EUISS, 2020, p. 38-49, https://www.iss.europa.eu/node/2423

Ian Manners, "Normative Power Europe: A Contradiction in Terms?", in *Journal of Common Market Studies*, Vol. 40, No. 2 (June 2002), p. 235-258

Christoph O. Meyer, "CSDP Missions and Operations", in *European Parliament In-Depth Analysis*, January 2020, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_IDA(2020)603481

Christian Mölling and Torben Schütz (eds), "The EU's Strategic Compass and Its Four Baskets. Recommendations to Make the Most of It", in *DGAP Reports*, No. 13 (November 2020), https://dgap.org/en/node/34620

North Atlantic Treaty Organization (NATO), *Common Set of New Proposals on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization*, 5 December 2017, https://www.nato.int/cps/en/natohq/official_texts_149522.htm

NATO, *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133163.htm

NATO, *Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, 6 December 2016, https://www.nato.int/cps/en/natohq/official_texts_138829.htm

Niklas Nováky, "The EU's Permanent Structured Cooperation in Defence: Keeping Sleeping Beauty from Snoozing", in *European View*, Vol. 17, No. 1 (April 2018), p. 97-104, https://doi.org/10.1177/1781685818764813

Patryk Pawlak, "Navigating the EU's Cyber Diplomacy", in *Directions Blog*, 25 September 2020, https://directionsblog.eu/?p=1172

John Peterson, "US and EU in the Balkans: 'America Fights the Wars, Europe Does the Dishes'?", in *EUI Working Papers RSC*, No. 2001/49 (2001), http://hdl.handle.net/1814/1758

Tobias Pietz, "EU Crisis Management: Back to the Future", in *Internationale Politik Quarterly*, No. 4/2021 (October 2021), https://ip-quarterly.com/en/node/35349

Jean-Claude Piris, *The Lisbon Treaty: A Legal and Political Analysis*, Cambridge, Cambridge University Press, 2010

Nicoletta Pirozzi, "The Civilian CSDP Compact. A Success Story for the EU's Crisis Management Cinderella?" in *EUISS Briefs*, No. 9 (October 2018), https://www.iss.europa.eu/node/2270

Maartje Rutten (ed.), "From St-Malo to Nice. European Defence: Core Documents", in *Chaillot Papers*, No. 47 (May 2001), https://www.iss.europa.eu/node/172

Julia Schuetze and Arthur de Liedekerke, "The EU's Response to SolarWinds", in *Net Politics Blog*, 26 May 2021, https://www.cfr.org/blog/eus-response-solarwinds

Bjoern H. Seibert, *Operation EUFOR TCHAD/RCA and the European Union's Common Security and Defense Policy*, Carlisle, US Army War College Strategic Studies Institute, October 2010, https://press.armywarcollege.edu/monographs/592

Gianluca Sgueo, "Counter-Terrorism Funding in the EU Budget", in *EPRS Briefings*, April 2016, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)580904

Luis Simon, "The Spanish Presidency and CSDP: Time to Get Serious about the Union's Military Planning and Conduct Capability", in *Analyses of the Elcano Royal Institute (ARI)*, No. 33/2010 (February 2010), http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari33-2010

Ido Sivan-Sevilla, "Europeanisation on Demand: The EU Cybersecurity Certification Regime Between Market Integration and Core State Powers (1997–2019)", in *Journal of Public Policy*, Vol. 41, No. 3 (September 2021), p. 600-631

Timo Smit, "Towards a More Capable European Union Civilian CSDP", in *SIPRI Policy Briefs*, November 2019, https://www.sipri.org/node/4947

Hazel Smith, *European Union Foreign Policy. What It Is and What It Does*, London/Sterling, Pluto Press, 2002, p. 127-135

Thierry Tardy, "The EU: From Comprehensive Vision To Integrated Action", in *EUISS Briefs*, No. 5 (February 2017), https://www.iss.europa.eu/node/1297

Verizon, *2021 Data Breach Investigations Report*, July 2021, https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

JOINT

A joined-up Union, a stronger Europe

www.jointproject.eu

info@jointproject.eu

facebook.com/JOINTprojectonline

@joint_project

linkedin.com/company/joint-project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N. 959143.
This publication reflects only the view of the author(s) and the European Commission is not responsible for any use that may be made of the information it contains.