
The European Union's Handling of Hybrid Threats: In Search of the Enlargement Dimension

PROFESSOR DR. YOURI DEVUYST¹

VRIJE UNIVERSITEIT BRUSSEL, BRUSSELS SCHOOL OF GOVERNANCE

Abstract: *At present, the EU's strategic documents on countering hybrid threats contain hardly any links to the accession process. A more robust defence of an enlarging EU requires the effective operationalisation of the principle of enhanced mutual resilience against hybrid threats between the EU and the candidate countries, including in the upcoming European Democracy Shield.*

Keywords: *European Union; hybrid threats; accession; enlargement; mutual resilience.*

INTRODUCTION

Because “the level of hybrid attacks has not been so high for decades”, European Commission President Ursula von der Leyen has pledged that her new 2024-2029 College will put in place a European Democracy Shield to defend democracy from hybrid threats² and “prevent hostile foreign actors from interfering in our democratic processes, undermining them and, ultimately, destroying them”.³ The Shield would include a dedicated structure for countering foreign information manipulation and interference, more powerful cyber-defence tools, transparency on foreign funding of the EU's public life, bolstering intelligence and detection capabilities, and a new horizontal set of restrictive measures against hybrid threats.⁴ This priority was reflected in the mission letters of at least five members of the new European Commission,⁵ but not in the letter to

¹ Prof. Dr. Youri Devuyt (email: Youri.Devuyt@vub.be) has been teaching European Union history, constitutional law and political institutions at the Vrije Universiteit Brussel (VUB) since 1994. He is currently affiliated with VUB's Brussels School of Governance. He studied at VUB (Doctorate in Political Science; LL.M. International & Comparative Law; Advanced Master International & European Law) and at the Johns Hopkins University's School of Advanced International Studies in Bologna and Washington DC (MA International Relations). His research interests focus on EU enlargement, EU institutional evolutions, and EU-US relations.

² In this paper, the concept of hybrid threats is understood as it was defined by the European Commission and the High Representative for Foreign Affairs and Security Policy in their Joint Framework on countering hybrid threats: a European Union response (Brussels, 6 April 2016 JOIN(2016) 18 final), p. 2: “the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats”.

³ Ursula von der Leyen, Statement at the European Parliament plenary as candidate for a second mandate 2024-2029, (Strasbourg, 18 June 2024), Accessed on 30.11.2024 https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_24_3871.

⁴ Ursula von der Leyen, Europe's choice: Political guidelines for the next European Commission 2024-2029 (Strasbourg, 18 June 2024), Accessed on 30.11.2024

https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en, p. 23.

⁵ See the mission letters for the members of the 2024-2029 Commission, Accessed on 30.11.2024 https://commission.europa.eu/about-european-commission/towards-new-commission-2024-2029/commissioners-designate-2024-2029_en. See, in particular, the mission letters to the Executive Vice-President for Tech Sovereignty, Security and Democracy, the Vice-President/High Representative for Foreign Affairs and Security Policy, and the Commissioners for Defence and Space, for Internal Affairs and Migration, and for Democracy, Justice, and the Rule of Law. In addition, the mission letter to the Commissioner for Preparedness and Crisis Management tasks her with the development and implementation of an EU Preparedness Union Strategy, in follow-up of the report by Sauli Niinistö, “Safer Together: Strengthening Europe's

the new Commissioner for Enlargement.⁶ This might seem somewhat astonishing given the frequent reports of hybrid attacks and foreign interference in the democratic processes of candidate countries such as Georgia, Moldova, Serbia and Bosnia and Herzegovina; all countries whose fate will have a major impact on the EU's own future.⁷

Still, the omission is less surprising when considering that the EU has a long practice of insufficiently reflecting the accession perspective in its key policy documents on hybrid risks. This persistent lack of a comprehensive strategic vision on the link between EU enlargement and countering hybrid threats is studied in detail the following two sections of this paper. To overcome the current situation, and ensure that a robust defence of the EU goes hand with a successful EU enlargement path, the final section of the paper outlines that the EU's strategy to counter hybrid threats, including the announced European Democracy Shield, should be based on the principle of enhanced mutual resilience between the EU and the candidate countries, thus ensuring the effective transition of these countries into EU member states in the crucial field of combatting and deterring hybrid attacks.

THE EU'S FOUNDATIONAL AND CONCEPTUAL TEXTS ON COUNTERING HYBRID THREATS: THE ABSENCE OF AN EXPLICIT ENLARGEMENT PERSPECTIVE

This section is based on an in-depth reading of the EU's foundational and conceptual policy documents on countering hybrid threats. These texts systematically put hybrid threats in the context of developments in the EU's neighbourhood and emphasise the need for cooperation with relevant partner countries. However, none of this leads to a strategic reflection on the interaction between the accession process and hybrid threats.

The EU's first foundational text in this field is the 2016 Joint Framework on countering hybrid threats. In the wake of Russia's illegal occupation of the Crimea in 2014, the civil war in Syria, and the Islamic State's conquering of territories in northwestern Iraq and eastern Syria in 2014-2015, the Joint Framework highlighted the EU's dramatically changed security environment and the challenges to peace and stability in the EU's eastern and southern neighbourhood. In that context, the Joint Framework logically underscored the need to further intensify the exchange of operational and strategic information "with *enlargement countries* and within the Eastern Partnership and Southern Neighbourhood" to help combat organised crime, terrorism, irregular migration and trafficking of small arms, and promote partners' resilience to hybrid activities.⁸ Significantly, this is one of the few times the word "enlargement" is mentioned in the EU's foundational texts on hybrid threats. The 2016 Joint Framework had some immediate operational consequences, such as the creation in mid-2016 of the EU Hybrid Fusion Cell inside the EU Intelligence and Situation Centre, with the task to raise situational awareness and to provide strategic analysis to the EU decision-makers.⁹

Civilian and Military Preparedness and Readiness" (Brussels, 30 October 2024), Accessed on 30.11.2024 https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en.

⁶ Marta Kos – Mission letter (Brussels, 17 September 2024), Accessed on 30.11.2024 https://commission.europa.eu/document/1a2d0ad0-270d-441b-98c8-b6be364d8272_en.

⁷ Thomas De Waal, Dimitar Bechev & Maksim Samorukow, *Between Russia and the EU: Europe's Arc of Instability* (Carnegie Europe & Carnegie Russia Eurasia Center, 2024), Accessed on 30.11.2024 <https://carnegieendowment.org/research/2024/05/bosnia-moldova-armenia-between-russia-eu?lang=en¢er=russia- Eurasia>.

⁸ European Commission and High Representative for Foreign Affairs and Security Policy, *Joint Framework on countering hybrid threats: a European Union response* (Brussels, 6 April 2016 JOIN(2016) 18 final), p. 14.

⁹ European Commission and High Representative for Foreign Affairs and Security Policy, *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats* (Brussels, 28 May 2019, SWD(2019) 200 final), p. 2.

The EU's second foundational text in this policy domain – the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats – was adopted following Russia's nerve agent attack in Salisbury (United Kingdom) in March of the same year.¹⁰ It stressed the necessity for building stronger internal-external links in chemical, biological, radiological and nuclear security and for improved coordination and cooperation on strategic communication with key regional and international partners, but without making a link with EU enlargement.

Following the Joint Communication, the years 2018-2020 saw the approval of an abundance of new EU policy documents on the theme of countering hybrid threats and disinformation.¹¹ They often called for a strengthening of the EU's cooperation with the relevant international actors and neighbouring partners, while lacking an explicit link with the accession process. For example, the 2019 Council conclusions on complementary efforts to enhance resilience and counter hybrid threats highlighted the importance of a comprehensive, whole-of-government and whole-of-society approach to security in order to effectively address hybrid threats.¹² However, the Council omitted any mentioning of the accession process and missed the opportunity to clarify how the EU could help prepare the candidate countries for the whole-of government and whole-of-society approach.

The absence of a thorough consideration of the EU enlargement process in the EU's main documents on countering hybrid threats did not change after Russia's full-scale invasion of Ukraine. The EU's 2022 Strategic Compass for Security and Defence devoted a specific chapter to hybrid threats and it vowed to strengthen the EU's response options, resilience capacities and cooperation both within the EU and in support of partner countries, but without mentioning the accession path.¹³ Likewise, the 2022 Council conclusions on a framework for a coordinated EU response to hybrid campaigns¹⁴ as well as the 2022 Council conclusions on Foreign Information Manipulation and Interference (FIMI)¹⁵ reiterated that the EU would step up its efforts to reach out to partner countries in order to counter hybrid threats and the manipulation of information without mentioning the accession process.

Following the intensification of Russia's hybrid campaign throughout Europe in 2023-2024, the European Council of June 2024 again strongly condemned all types of hybrid activities “including intimidation, sabotage, subversion, foreign information manipulation and interference, disinformation, malicious cyber activities and the instrumentalization of migrants by third countries”.¹⁶ The same European Council also adopted the Union's Strategic Agenda 2024-2029, but

¹⁰ European Commission and High Representative for Foreign Affairs and Security Policy, Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (Brussels, 13 June 2018 JOIN(2018) 16 final).

¹¹ See, for example, European Commission, Communication - Tackling online disinformation: a European Approach (Brussels, 26 April 2018, COM(2018) 236 final); European Commission, Communication - Securing free and fair European elections (Brussels, 12 September 2018, COM(2018) 637 final); European Commission & High Representative for Foreign Affairs and Security Policy, Joint Communication - Action Plan against disinformation (Brussels, 5 December 2018 JOIN(2018) 36 final); European Council, Conclusions (Brussels, 22 March 2019, EUCO 1/19), para. 9; European Council, Conclusions (Brussels, 20 June 2019, EUCO 9/19), para. 6-7; European Commission, Communication on the EU Security Union strategy (Brussels, 24 July 2020 COM(2020) 605 final); Council conclusions on safeguarding a free and pluralistic media system (Brussels, 27 November 2020, 13260/20); Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic (Brussels, 15 December 2020, 14064/20).

¹² Council Conclusions on complementary efforts to enhance resilience and counter hybrid threats (Brussels, 10 December 2019, 14972/19).

¹³ Council of the EU, A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security (Brussels, 21 March 2022, 7371/22).

¹⁴ Council conclusions on a framework for a coordinated EU response to hybrid campaigns (Brussels, 21 June 2022, 10016/22), para. 2, 4, 8.

¹⁵ Council conclusions on foreign information manipulation and interference (FIMI) (Brussels, 18 July 2022, 11429/22), para. 2.

¹⁶ European Council Conclusions (Brussels, 27 June 2024, EUCO 15/24), para. 40.

without laying a conceptual bridge between the commitment to “strengthen its resilience, preparedness, crisis prevention and response capacities, in an all-hazards and whole-of-society approach” and the accession process.¹⁷ It is therefore not entirely astonishing that the 2024 Commission Communication on countering hybrid threats from the weaponisation of migration and strengthening security at the EU’s external borders did not contain a single reference to accession, enlargement or the candidate countries.¹⁸

To some limited degree, the Commission’s 2020 European Democracy Action Plan and 2023 Communication on Defence of Democracy can be singled out as exceptions to the absence of an enlargement dimension in the EU’s strategic documents on hybrid threats. Without going into any depth, the European Democracy Action Plan at least acknowledged the importance of raising awareness of European values and building resilience against disinformation “in particular in the European Neighbourhood and *Enlargement region*”. By way of example, it mentioned the Media Freedom Rapid Response pilot project for countering violations of press and media freedom “in Member States and *candidate countries*”.¹⁹ Likewise, the Commission’s Communication on Defence of Democracy recognised that responding to external threats attacking the democratic process constituted “a priority in *EU enlargement policy*” and that the EU’s Western Balkan media programme, support for electoral reform in the Western Balkans, and several TAIEX activities against disinformation had to be seen in “*the context of enlargement*”.²⁰ However, this did not lead to broader strategic considerations encompassing EU enlargement.

The documents cited above make clear that the EU has been actively mobilising against hybrid threats coming from Russia. It did attach major importance to hybrid developments in its neighbourhood and to cooperation with the relevant partner countries. At the same time, EU enlargement has not been given any structural consideration in this context. None of the foundational and overarching texts on the EU’s response to hybrid threats have devoted a full paragraph to the enlargement process. Where the texts did acknowledge the accession dimension, this was done in a very brief manner and without any elaboration of the strategy behind it. While this might be understandable in the pre-2022 era, when accession issues were not in the forefront of EU politics, it is more difficult to comprehend after the 2022 applications by Ukraine, Moldova and Georgia and the EU’s renewed enlargement drive.

COUNTERING HYBRID THREATS IN PRACTICE: TOPICAL RATHER THAN STRATEGIC ACCESSION SUPPORT

The conclusions of the preceding section do not mean that the EU has not been taking concrete action against hybrid threats in the candidate countries. As will be detailed in this section, the EU has made significant efforts to support the partner countries that have applied for EU membership, but again, those efforts have not been framed in a strategic and comprehensive accession context.

To shed light on the enlargement dimension in the EU’s practice of countering hybrid threats, this paper analyses references to the EU accession process in (a) the annual progress reports by the Commission and the European External Action Service (EEAS) on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing

¹⁷ Ibid., Annex: Strategic Agenda 2024-2029.

¹⁸ European Commission, Communication on countering hybrid threats from the weaponisation of migration and strengthening security at the EU’s external borders (Brussels, 11 December 2024, COM(2024) 570 final).

¹⁹ European Commission, Communication on the European democracy action plan (Brussels, 3 December 2020 COM(2020) 790 final), p. 13, 21, 25.

²⁰ European Commission, Communication on defence of democracy (Strasbourg, 12 December 2023, COM(2023) 630 final).

resilience and bolstering capabilities to address hybrid threats²¹; and (b) the annual reports on EEAS Activities to counter foreign information manipulation and interference (FIMI).²² This analysis is complemented by its mirror image, through an examination of the passages on hybrid threats in the Commission's annual enlargement package, which consists of (a) a general Commission Communication on enlargement policy that takes stock of the developments over the past year and (b) individual country reports in which the Commission services present their detailed annual assessment of the state of play in each candidate country.²³

(a) Overall findings

A first overall finding is that, within the EU enlargement context, the hybrid threat concept made its debut rather late. Looking at the annual Commission Communications on enlargement policy, the first mentioning of hybrid threats came in an annex of the 2019 version. It was only in 2020 that hybrid threats made their way into the main text. This is remarkable since the foundational EU policy documents in the field dated from 2016 and 2018, and the annual reports on countering hybrid threats had included references to some of the candidate countries since 2017. It thus proved far from self-evident to incorporate the transversal hybrid threats theme in the EU's traditional accession logic that focuses on the transposition of the EU *acquis* through pre-established negotiating chapters.

Secondly, after 2020, Commission's annual enlargement packages reported on actions countering hybrid threats mainly under negotiating chapters 31 (Foreign, security and defence policy) and 10 (Digital transformation and media). The percentage of text devoted to hybrid threats remained very modest.

Thirdly, it is striking and somewhat of a paradox that even the annual Communications on enlargement policy refrained from putting hybrid threats in a more strategic accession context, apart from stating on occasion that disinformation campaigns were aiming to discredit the EU and the ambition of membership. The only time hybrid threats figured in the overall conclusions and recommendations of the annual Communication on enlargement policy, in 2022, illustrated the point. The conclusions highlighted the priority of strengthening the capacities of the Western Balkans against hybrid threats such as cyber security, enhancing the resilience of critical infrastructure, and countering disinformation. However, the rationale that preceded this conclusion could have been used for any country situated in the EU's neighbourhood, whether a candidate country or not. It stated as follows:

The "current geopolitical challenges call for strengthening our cooperation with the region, whose security is ultimately tied up with that of the EU itself. The EU has long been the most important economic partner of the Western Balkans. With the adoption of the EU's Strategic Compass, the foundations are laid for the EU and its Member States to further entrench their role as the region's most important security and defence partners, acting also in close cooperation with likeminded international security actors".²⁴

²¹ See the annual progress reports by the European Commission and the EEAS on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (from 2017 to 2023), Accessed on 30.11.2024 https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.

²² See the annual reports on EEAS Activities to counter foreign information manipulation and interference (FIMI) (from 2021 to 2023), Accessed on 30.11.2024 https://www.eeas.europa.eu/eeas/eeas-stratcom%E2%80%99s-responses-foreign-information-manipulation-and-interference-fimi-2023_en.

²³ See the European Commission's annual enlargement packages (from 2015 to 2024), Accessed on 30.11.2024 https://neighbourhood-enlargement.ec.europa.eu/enlargement-policy/strategy-and-reports_en.

²⁴ European Commission, 2022 Communication on EU Enlargement Policy (Brussels, 12 October 2022, COM(2022) 528 final), p. 35, point 11.

Not a word in this rationale referred to the enlargement process, or to the need of combatting hybrid threats and disinformation as an essential precondition for a successful accession.

Fourth, EU actions to counter hybrid threats in the Western Balkans and the Eastern Partnership countries seemed largely driven by events, in particular the Russian invasion of Ukraine, and not by a long-term EU strategy related to the candidate status of the countries in question. None of the annual reports on countering hybrid threats and FIMI mentioned that Bosnia-Herzegovina, Ukraine, Georgia and Moldova had been granted candidate status in 2022-2023. Furthermore, the number of times a country was mentioned in these reports did not seem related to its candidate country status. For example, with respect to Georgia, the highest number of EU support actions were signalled in 2020 (i.e. before it applied for EU membership), in the form of cyber resilience activities in reaction to cyber-attacks that targeted the country in October 2019.

(b) Dominant themes

In conformity with the definition of hybrid threats in the 2016 Joint Framework, the analysed reports used the concept in a relatively open and flexible way. In practice, however, only two themes were treated in a systematic manner: disinformation and cybersecurity. Other hybrid threats, for example, related to critical infrastructure, economic coercion or espionage were hardly mentioned.

Regarding disinformation, the Communications on enlargement policy underlined year after year that the Western Balkans were facing particularly intense FIMI campaigns: during the Covid-19 pandemic, after the Russian invasion of Ukraine, and in the run-up to elections. The reports also stressed that such campaigns found a particularly fertile local ground given the region's low media literacy, low trust in institutions, limited space for professional journalism and low level of media freedom. The bulk of the disinformation was reported to be produced and disseminated by domestic actors for domestic purposes, but third states' proxies were also signalled, in particular Russia-sponsored. Their aim was to undermine public trust in democratic institutions, deepen polarisation, challenge the EU's credibility, and derail the region from its EU path. In the same vein, after 2022, Ukraine, Moldova and Georgia also became the target of a reinforced wave of information manipulation after their applications for EU membership, mainly to discredit their aspirations to join the EU.

Cyber resilience and cybersecurity were a subject that more easily fit the traditional pre-accession focus on conformity with the EU law. Thus, the 2023 Communication on enlargement policy signalled progress on alignment with the EU *acquis* in cybersecurity in Albania, North Macedonia, Montenegro, Ukraine and Moldova. At the same time, the 2024 country reports emphasised the need for Bosnia and Herzegovina, Montenegro, North Macedonia, Georgia, Moldova and Ukraine to fully implement the 5G Cybersecurity Toolbox measures. In the same vein, North Macedonia, Serbia, Georgia and Ukraine were prodded to achieve legal alignment with the EU Directive on measures for a high common level of cybersecurity across the Union (NIS2).

(c) Main intervention tools to counter hybrid threats

In addition to the two dominant policy domains, the reports also highlighted several key EU intervention tools.

First, in response to the disinformation campaigns mentioned above, every single report on countering hybrid threats and FIMI underscored the central role of the EEAS Strategic Communication Division (StratCom).²⁵ The reports highlighted in particular the numerous actions of the East StratCom Task Force (created in 2015) and the StratCom's Western Balkans Task Force

²⁵ For the background, see https://www.eeas.europa.eu/countering-disinformation/tackling-disinformation-information-work-eeas-strategic-communication-division-and-its-task-forces_und_en (Accessed on 30.11.2024).

(operational since 2017) to improve the EU's strategic communication with the partners (with the help of the EU Delegations), uncover, compile and debunk Russian disinformation, ensure support for independent media, conduct public and cultural diplomacy, and regularly coordinate with the Member States and NATO.

The second policy instrument highlighted in the analysed activity reports were the civilian missions under the common security and defence policy (CSDP) to address hybrid threats. They included the EU Monitoring Mission Georgia (that started after the military conflict with Russia in 2008), the EU Advisory Mission Ukraine (that started after the Russian invasion of the Crimea in 2014), and the EU Partnership Mission in Moldova (that started in 2023) to strengthen the areas of crisis management and hybrid threats, including cybersecurity and countering FIMI.

A third key tool that was put in the spotlights in many annual activity reports were the Hybrid Risk Surveys. Following a 2017 pilot project with Moldova, Hybrid Risk Surveys were launched with Georgia, Jordan, Albania, North Macedonia, Kosovo and Montenegro. The purpose was to help identify each country's key hybrid vulnerabilities, formulate specific recommendations to increase each partners' resilience, and ensure that EU assistance would specifically target those areas, and develop an appropriate framework for provision of support in becoming more resilient to hybrid threats.

Fourthly, the European Peace Facility (EPF) was reported to have financed and delivered cyber defence to the Ukrainian Armed Forces, the Moldovan Armed Forces and the Georgian Military Defence Cybersecurity Bureau.

Fifth, another instrument, highlighted particularly in 2023, was support under the Rapid Response Pillar of the Neighbourhood, Development and International Cooperation Instrument (NDICI) for Moldova as well as Albania, Montenegro and North Macedonia to increase their resilience to hybrid threats resulting from Russia's war of aggression against Ukraine, in particular disinformation and cyber threats.

Sixth, several reports highlighted how the successive generations of the Instrument for Pre-Accession Assistance (IPA) had been mobilised to support reforms in the partner countries to strengthen resilience against hybrid threats and FIMI. This included the 2019 regional programme to strengthen cyber resilience in the Western Balkans under IPA II (2014-2020) and the 2023 comprehensive regional cybersecurity programme for the Western Balkans under IPA III (2021-2017).

Finally, it is worth signalling the numerous references in the activity reports to support provided under the Commission's Technical Assistance and Information Exchange instrument (TAIEX) in the form of expert missions and workshops in the domain of cybersecurity, strategic communication, disinformation and critical information infrastructure.

(d) Country-specific comments

Looking at the annual reports on countering hybrid threats and FIMI, Ukraine was the country that was mentioned the most.²⁶ This is not surprising considering the disinformation campaign that accompanied the Russian invasion of the country. On the other side of the spectrum, the EU reports on countering hybrid threats and FIMI (that largely focus on achievements and positive cooperation with the EU) very seldom mentioned Serbia and Bosnia and Herzegovina.²⁷ In the Commission's annual enlargement package reports, however, these two countries (as well as Georgia in 2024), were the subject of strong critical remarks.

²⁶ In total, Ukraine was mentioned 98 times in the annual reports on countering hybrid threats (of which 50 times in the 2020 report) and 68 times in the annual reports to counter FIME (of which 49 times in the 2022 report).

²⁷ Serbia was never mentioned in any of the annual reports on countering hybrid threats and only once in the 2023 reports to counter FIME. Bosnia and Herzegovina was mentioned once in the 2018 report on countering hybrid threats and once in the 2023 reports to counter FIME.

The 2022, 2023 and 2024 Communications on enlargement policy each time summoned Serbia to take urgent action to protect its citizens against foreign information manipulation and interference and from anti-EU narratives. It was also noted that several Russian state-sponsored outlets on the EU sanctions list were broadcasting the Kremlin's disinformation from Serbia, with spill-over effects across the region. This message was reinforced in the country reports on Serbia. The 2024 report underlined that the Serbian authorities needed, as a matter of priority, to take much more responsibility for proactive and objective communication on Serbia's EU accession process and the EU and for countering disinformation in its national media. The country report also pointed out that Serbia did not align with EU declarations and restrictive measures in reaction to cyber-attacks in 2023 and 2024, and that it should as a matter of priority improve its alignment with EU common foreign and security policy and avoid actions and statements that go against EU foreign policy positions.

Regarding Bosnia and Herzegovina, the 2024 country report noted that the country lacked an overall assessment or policy framework for addressing hybrid threats. It also remained the only country in the region without a countrywide strategy on cybersecurity, which rendered it vulnerable to recurring cyber-attacks. With a local provider continuing to carry the signal of the RT channel, Bosnia and Herzegovina was prodded to make further efforts on closing space for foreign information manipulation and interference, and to take actions towards building societal resilience against all forms of hybrid threats.

With respect to Georgia, the 2024 Communication on enlargement policy stressed that its authorities needed to stop spreading disinformation against EU values and step up actions to combat disinformation. The 2024 country report on Georgia added that, since the re-introduction of the draft law on transparency of foreign influence in April 2024, harsh anti-EU messages, actively spread by high level ruling party officials and MPs, had become recurrent. Furthermore, in the run-up to the 2024 Parliamentary elections, the report noticed an amplification of disinformation narratives by ruling party officials and government-affiliated media. The report regretted that cooperation with the EU on hybrid threats and countering disinformation was limited. It observed there was little evidence of political will to take measures to limit the spread of manipulative narratives, including targeting the EU. Like Serbia, Georgia declined to align with the statement of October 2024 by the High Representative for Foreign Affairs and Security Policy, on behalf of the EU, strongly condemning Russia's intensifying campaign of hybrid activities against the EU, its Member States and partners.²⁸

TOWARDS A STRATEGIC VISION OF THE ENLARGEMENT DIMENSION IN THE EU'S HANDLING OF HYBRID THREATS

The annual reports reviewed above provide an impressive overview of EU actions in support of partner country resilience against hybrid threats, mobilising a wide array of policy tools, with a strong thematic focus on countering disinformation and ensuring cybersecurity. However, none of these reports presented the EU's actions as part of a comprehensive strategic vision on the link between EU enlargement and countering hybrid threats. The lack of a broader perspective on the accession dimension of hybrid threats can be seen as a logical corollary of the way enlargement was treated in the EU's foundational policy documents on countering hybrid threats. The recent flood of hybrid attacks against the democratic political and electoral processes in the candidate countries underscores that the current state-of-play is not satisfactory. Creating resilience against hybrid attacks

²⁸ Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States (Brussels, 8 October 2024), Accessed on 30.11.2024 <https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/hybrid-threatsrussia-statement-by-the-high-representative-on-behalf-of-the-eu-on-russia-s-continued-hybrid-activity-against-the-eu-and-its-member-states/>.

in the candidate countries requires an EU policy upgrade and the development of a strategic vision that seems largely absent at present.

The main rationale for such a strategic approach is that hybrid attacks are putting at risk the fundamentals of the European construction. First, hybrid campaigns actively try to undermine the values underpinning the EU such as democracy, the rule of law, pluralism and tolerance as well as the principle of mutual trust. As the Court of Justice of the EU has held, the “fundamental importance” of those values and of the mutual trust principle resides in the fact that “they allow an area without internal borders to be created and maintained”.²⁹ It is no exaggeration, therefore, that hybrid actions that erode EU values and the mutual trust principle, are also undercutting the EU itself. Secondly, as former Finnish President Sauli Niinistö has emphasized in his report on the strengthening of the EU’s civilian and military preparedness, hybrid action also affects the democratic decision-making processes. Hostile actors exploit the dependencies and vulnerabilities of individual (new and old) member states to interfere with and undermine EU decision-making through targeted pressure. In Niinistö’s view, this poses “a significant risk to the EU’s readiness for decisive crisis response and its capacity for proactive preparedness, ultimately putting at stake the Union’s legitimacy, credibility, and ability to deliver for citizens”.³⁰ Looked at from the perspective of the integrity of the EU’s political system, providing support to countries in transition to become member states should, therefore, be conceptualized very differently from assisting other partner countries struggling with hybrid threats outside the EU.

Mutual trust in an enlarging EU requires mutual resilience of the member states and the incoming countries. When Niinistö pleads for an EU that “emphasises mutual resilience as a key element of its diplomacy and external action”, this should be applied as a matter of priority and in an enhanced or intensified manner with the candidate countries.³¹ The EU should consequently extrapolate its own interests in resilience building against hybrid threats to include the applicants. This should be one of the top priorities of the European Democracy Shield announced by President von der Leyen.

The successful inclusion of the enhanced mutual resilience perspective (involving both EU and the candidate countries) in the European Democracy Shield calls for a roadmap that ensures (a) a better definition of the hybrid concept, with a concrete identification of its main components and (b) a sharper and more proactive operationalisation at EU-level of what enhanced mutual resilience entails for the EU and the candidate countries alike.

On the need for a better definition, it must be signalled that the concept of hybrid threats has been the subject of much debate during recent years.³² Some have highlighted that the “the term nicely captures the blurring of public and private, state or non-state, formal and informal that is characteristic of new wars”³³ and shows that “[n]o single aspect of the threat facing Europe exists in isolation from others”.³⁴ Others have expressed serious doubts on the concept’s inherently open and flexible nature, considering it as “a misguided attempt to group everything Moscow does under one

²⁹ Court of Justice of the EU, Judgment of 28 October 2022, C-435/22, *PPU, HF*, EU:C:2022:852, para. 92; Judgment of 22 February 2022, C-562/21 *PPU* and C-563/21, *PPU, XY*, EU:C:2022:100, para. 40; Judgment of 15 October 2019, *Dorobantu*, C-128/18, EU:C:2019:857, para. 46.

³⁰ Sauli Niinistö, “Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness”, Brussels, European Commission, 30 October 2024, p. 62.

³¹ *Ibid.*, p. 15 and 137.

³² Chiara Libiseller, ‘Hybrid warfare’ as an academic fashion, in “Journal of Strategic Studies”, Vol. 46, No. 4, 2023, p. 858–880.

³³ Mary Kaldor, “New & Old Wars: Organized Violence in a Global Era”, Stanford, Stanford University Press, 1998, p. 2.

³⁴ Daniel Fiott and Roderick Parkes, Protecting Europe: The EU’s response to hybrid threats, in “Chaillot Paper”, No. 151 (EU Institute for Security Studies), 2019, p. 2.

rubric”³⁵ and as “an elusive and catch-all term” that Western decision-makers should “forget”, while shifting their “focus on the specificity and the interconnectedness of the threats they face”.³⁶ Several strategic analysts have pointed out that the “conceptual ambiguity” behind the hybrid term makes it very difficult to develop an effective counterstrategy. “Logically”, states Tarik Solmaz, “it is not possible to develop an efficient defence strategy against a threat that is not exactly identified in its scope and features”.³⁷ Likewise, Jan Joel Andersson and Thierry Tardy emphasise that “the confusion intentionally created by hybrid tactics is likely to further complicate the ability of EU countries and institutions to craft a truly coherent and comprehensive response”.³⁸ In this sense, Bettina Renz and Hanna Smith conclude that the hybrid threats concept is not merely “unsuitable as an analytical tool” but “could even be playing into Russia’s hands”.³⁹

Notwithstanding such critical comments, the EU policy documents reviewed in this paper make clear that “the hybrid terminology is now firmly established and seems poised to continue being used in strategic planning”.⁴⁰ This use should, however, not be without taking on board the gist of the criticism. For the European Democracy Shield to become successful, the different components of the hybrid threats concept should be better identified in the new roadmap, in a manner that facilitates delineating institutional responsibilities and formulating operational countermeasures.⁴¹ This is not to dispute the necessity for a whole-of-government and whole-of-society approach (as highlighted in several EU documents), but those approaches are impossible to implement without a clear breakdown of what is needed where and when, and guidance and leadership through a new control and command system. At the same time, room should be made in the roadmap for handling new or unexpected hybrid problems, for which predefined standard operating procedures are not yet available.⁴² This requires an operational European control and command system with the capacity to react in a quick manner. Crucially, and in the spirit of enhanced mutual resilience, the European Democracy Shield and its operational roadmap should come with clear pro-active guidance and support for the candidate countries regarding each identified line of action. No longer can the EU afford to forget candidate countries and the accession process in its main EU policy documents on tackling hybrid threats.

Additionally, the EU should give itself the means to determine the existence in a candidate country of a serious and persistent failure to effectively counter hybrid threats. Such a determination should, in last resort, bring the accession process to a halt, until the failure has been remedied. In implementation of the mutual resilience principle, it would be invoked in case a candidate country systematically refuses to take the necessary measures, including by aligning itself with EU’s CFSP statements and policies to counter hybrid threats. It might also be relied upon when a candidate country has persistently been incapable of tackling hybrid threats, particularly those affecting its democratic political processes, pluralism, tolerance, and the rule of law. In such a case, moving

³⁵ Michael Kofman and Matthew Rojansky, A Closer look at Russia’s ‘Hybrid War’, in “Kennan Cable” (Wilson Center), No. 7, 2015.

³⁶ Damien Van Puyvelde, Hybrid war: Does it even exist?, in “NATO Review”, 7 May 2015, Accessed on 30.11.2024 <https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html>,

³⁷ Tarik Solmaz, ‘Hybrid warfare’: A dramatic example of conceptual stretching, in “National Security and the Future”, Vol. 23, No. 1, 2022, 89-102, p. 96.

³⁸ Jan Joel Andersson and Thierry Tardy, Hybrid: what’s in a name?, in “Brief Issue” (EU Institute for Security Studies), No. 32, 2015, p. 3.

³⁹ Bettina Renz and Hanna Smith, Russia and Hybrid warfare - going beyond the label, in “Aleksanteri Papers” (University of Helsinki), No. 1, 2016, p. 1.

⁴⁰ Mikael Wigell, Harri Mikkola and Tapio Juntunen, “Best Practices in the whole-of-society approach in countering hybrid threats”, Brussels, European Parliament Policy Department for External Relations, PE 653.632, May 2021, p. 11.

⁴¹ *Ibid.*

⁴² Robert Person, Isak Kulalic and John Mayle, Back to the future: the persistent problems of hybrid war, in “International Affairs”, Vol. 100, No. 4, 2024, p. 1749-1761.

forward with a country's accession would only undercut the integrity of EU decision-making and the sustainability of its own functioning. As already stated by the Delors Commission in 1992: "to proceed to enlargement in a way which reduces [the EU's] effectiveness would be an error".⁴³

BIBLIOGRAPHY/REFERENCES:

Studies published in journals and think tank series:

Andersson Jan Joel and Thierry Tardy, Hybrid: what's in a name?, in "Brief Issue" (EU Institute for Security Studies), No. 32, 2015.

De Waal Thomas, Dimitar Bechev & Maksim Samorukow, Between Russia and the EU: Europe's Arc of Instability (Carnegie Europe & Carnegie Russia Eurasia Center), 2024, Accessed on 30.11.2024
<https://carnegieendowment.org/research/2024/05/bosnia-moldova-armenia-between-russia-eu?lang=en¢er=russia-eurasia>.

Fiott Daniel and Roderick Parkes, Protecting Europe: The EU's response to hybrid threats, in "Chaillot Paper", No. 151 (EU Institute for Security Studies), 2019.

Kofman Michael and Matthew Rojansky, A Closer look at Russia's 'Hybrid War', in "Kennan Cable" (Wilson Center), No. 7, 2015.

Libiseller Chiara, 'Hybrid warfare' as an academic fashion, in "Journal of Strategic Studies", Vol. 46, No. 4, 2023, p. 858–880.

Person Robert, Isak Kulalic and John Mayle, Back to the future: the persistent problems of hybrid war, in "International Affairs", Vol. 100, No. 4, 2024, p. 1749-1761.

Renz Bettina and Hanna Smith, Russia and Hybrid warfare - going beyond the label, in "Aleksanteri Papers" (University of Helsinki), No. 1, 2016.

Solmaz Tarik, 'Hybrid warfare': A dramatic example of conceptual stretching, in "National Security and the Future", Vol. 23, No. 1, 2022, 89-102.

Van Puyvelde Damien, Hybrid war: Does it even exist?, in "NATO Review", 7 May 2015, Accessed on 30.11.2024
<https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html>.

Book:

Kaldor Mary, "New & Old Wars: Organized Violence in a Global Era", Stanford, Stanford University Press, 1998.

EU institutional documents and publications:

Council conclusions on a framework for a coordinated EU response to hybrid campaigns (Brussels, 21 June 2022, 10016/22).

Council conclusions on complementary efforts to enhance resilience and counter hybrid threats (Brussels, 10 December 2019, 14972/19).

Council conclusions on foreign information manipulation and interference (FIMI) (Brussels, 18 July 2022, 11429/22).

Council conclusions on safeguarding a free and pluralistic media system (Brussels, 27 November 2020, 13260/20).

Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic (Brussels, 15 December 2020, 14064/20).

Council Decision (CFSP) 2024/2643 of 8 October 2024 concerning restrictive measures in view of Russia's destabilising activities, OJ L, 2024/2643, 9 October 2024.

Council Regulation (EU) 2024/2642 of 8 October 2024 concerning restrictive measures in view of Russia's destabilizing activities, OJ L, 2024/2642, 9 October 2024.

⁴³ European Commission, Europe and the challenge of enlargement (24 June 1992), in "Bulletin of the European Communities, Supplement 3/92", p. 14, para. 18.

- Council, A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security (Brussels, 21 March 2022, 7371/22).
- Court of Justice of the EU, Judgment of 15 October 2019, *Dorobantu*, C-128/18, EU:C:2019:857.
- Court of Justice of the EU, Judgment of 22 February 2022, C-562/21 PPU and C-563/21, *PPU, XY*, EU:C:2022:100.
- Court of Justice of the EU, Judgment of 28 October 2022, C-435/22, *PPU, HF*, EU:C:2022:852.
- European Commission and High Representative for Foreign Affairs and Security Policy, Joint Framework on countering hybrid threats: a European Union response (Brussels, 6 April 2016 JOIN(2016) 18 final), p. 14.
- European Commission and High Representative for Foreign Affairs and Security Policy, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (Brussels, 28 May 2019, SWD(2019) 200 final), p. 2.
- European Commission and High Representative for Foreign Affairs and Security Policy, Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (Brussels, 13 June 2018 JOIN(2018) 16 final).
- European Commission and High Representative for Foreign Affairs and Security Policy, Joint Communication - Action Plan against Disinformation (Brussels, 5 December 2018 JOIN(2018) 36 final).
- European Commission, Communication - Securing free and fair European elections (Brussels, 12 September 2018, COM(2018) 637 final).
- European Commission, Communication - Tackling online disinformation: a European approach (Brussels, 26 April 2018, COM(2018) 236 final).
- European Commission, Communication on countering hybrid threats from the weaponisation of migration and strengthening security at the EU's external borders (Brussels, 11 December 2024, COM(2024) 570 final).
- European Commission, Communication on defence of democracy (Strasbourg, 12 December 2023, COM(2023) 630 final).
- European Commission, Communication on the EU Security Union strategy (Brussels, 24 July 2020 COM(2020) 605 final).
- European Commission, Communication on the European democracy action plan (Brussels, 3 December 2020 COM(2020) 790 final).
- European Commission, Europe and the challenge of enlargement (24 June 1992), in "Bulletin of the European Communities, Supplement 3/92".
- European Council Conclusions (Brussels, 27 June 2024, EUCO 15/24).
- European Council, Conclusions (Brussels, 20 June 2019, EUCO 9/19).
- European Council, Conclusions (Brussels, 22 March 2019, EUCO 1/19).
- Niinistö Sauli, "Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness" (Brussels, European Commission, 30 October 2024), Accessed on 30.11.2024
https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en.
- Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States (Brussels, 8 October 2024), Accessed on 30.11.2024
<https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/hybrid-threatsrussia-statement-by-the-high-representative-on-behalf-of-the-eu-on-russia-s-continued-hybrid-activity-against-the-eu-and-its-member-states/>.
- Von der Leyen Ursula, Europe's choice: Political guidelines for the next European Commission 2024-2029 (Strasbourg, 18 June 2024), Accessed on 30.11.2024
https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en, p. 23.
- Von der Leyen Ursula, Statement at the European Parliament plenary as candidate for a second mandate 2024-2029 (Strasbourg, 18 June 2024), Accessed on 30.11.2024
https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_24_3871.

Wigell Mikael, Harri Mikkola and Tapio Juntunen, “Best Practices in the whole-of-society approach in countering hybrid threats” (Brussels, European Parliament Policy Department for External Relations, PE 653.632, May 2021).

Collective EU source location:

EEAS, Annual reports on EEAS activities to counter FIMI (from 2021 to 2023), Accessed on 30.11.2024
https://www.eeas.europa.eu/eeas/eeas-stratcom%E2%80%99s-responses-foreign-information-manipulation-and-interference-fimi-2023_en.

European Commission and EEAS, Annual progress reports by the on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (from 2017 to 2023), Accessed on 30.11.2024
https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.

European Commission annual enlargement packages (from 2015 to 2024), Accessed on 30.11.2024
https://neighbourhood-enlargement.ec.europa.eu/enlargement-policy/strategy-and-reports_en.

European Commission mission letters, Accessed on 30.11.2024
https://commission.europa.eu/about-european-commission/towards-new-commission-2024-2029/commissioners-designate-2024-2029_en.