Article

Wilfried Martens Centre for European Studies

European View
2020, Vol. 19(1) 62–70

DOI: 10.1177/1781685820912041
journals.sagepub.com/home/euv
SAGE

Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond

Eitvydas Bajarūnas

Abstract

This article discusses hybrid threats and the steps that Europe, through various national, EU and NATO initiatives, has taken in recent years to address them. Although these threats do not constitute a new challenge for states and international actors, they became a major concern for European countries following Russia's conventional and unconventional war in Ukraine in 2014. The article argues that addressing hybrid threats is a constant, never-ending process that requires the development of societal and governmental resilience. Hybrid threats are constantly changing and evolving, which means that our response to them also needs to be constantly evolving in order to keep up. The article also provides some recommendations for European policymakers on the next steps that Europe, especially the EU, should take when addressing hybrid threats.

Keywords

Hybrid threats, Resilience, EU, NATO, Russia, Ukraine

Introduction[1]

The challenge of hybrid threats has become a key aspect of security policy discourse. European Council conclusions and national strategies frequently mention hostile activities or meddling in elections by external actors. Although state and non-state actors have long exploited various hostile technologies,[2] it has only been since the effective implementation of hybrid tactics by Russia in Crimea and Eastern Ukraine in 2014 that Western politicians and the expert community have turned their eyes towards this phenomenon.

Corresponding author:
Eitvydas Bajarūnas, Ministry of Foreign Affairs of the Republic of Lithuania, J.Tumo- Vaižganto str. 2, Vilnius, LT-01511, Lithuania.
Email: eitvydas.bajarunas@urm.lt

The 'little green men' without insignia not only became a symbol of this manipulative approach, but their presence also indicated to the West where and how Ukraine was suffering from political, diplomatic, energy-related and economic pressure; deception; unprecedented informational warfare; cyberattacks; and actions by Russian special forces (the 'Spetsnaz'), which eventually turned into conventional military action. Many analysts have emphasised that, although hybrid threats are not new, Russia has successfully tailored them to the twenty-first century context using globalisation and new state-of-the-art technologies, thereby taking advantage of the vulnerabilities of a country or region in order to destabilise the adversary and hinder the process of decision-making.

Hybrid threats encompass elements of asymmetry and unexpectedness. Another widely discussed element is the ambiguity of the conflict, as hybrid warfare intentionally blurs the distinction between peacetime and wartime. The term 'grey zone' refers to this ambiguity.

Despite lacking a complete understanding of this phenomenon, national governments and international organisations have started to seriously consider actions to counter malign activities by state or non-state actors. According to the EU (and, indeed, NATO), countering hybrid threats is a national responsibility. However, international cooperation, particularly through the EU and NATO, using regional and multilateral initiatives such as the Helsinki-based European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), can enable states to unite their separate, scattered national resources to solve these issues more broadly.

On the level of national responses, many EU and NATO states and neighbours have rushed to implement so-called comprehensive security concepts as a reaction to the phenomenon of hybrid threats. Many of the steps taken are self-evident and are based on the experiences of countries which already have substantial competences in the area of comprehensive security (e.g. the UK and Finland): the well-functioning coordination of various institutions at the government level; strong links between government, civil society and the private sector; a well-tuned legal base; civilian–military cooperation; and constant preparation, training, exercises and education. This 'whole of government' approach has become a mantra among security-policy practitioners.

The article argues that addressing hybrid threats is a constant, never-ending process that is fundamentally about the development of resilience at the societal, the national and the European level. This is because hybrid threats are constantly changing and evolving, which means that our response to them needs to constantly evolve to keep up.

Although many steps have already been taken to boost Europe's resilience to hybrid threats since Russia's annexation of Ukraine's Crimea region in 2014, there is much more to do at the EU (and NATO) level. The rest of this article is divided into three main sections. The first will provide an overview of the steps that the EU and NATO have already taken to address hybrid threats since 2014. The second provides some

suggestions on the possible next steps for Europe to enhance its resilience to hybrid threats. The third and final section concludes the paper.

Big decisions and practical steps taken

With the ambiguity of the nature of hybrid threats, many national governments, as well as international organisations such as the EU, were forced to start by clearly defining this phenomenon. In the EU's 2016 Joint Communication the concept of a hybrid threat is defined as a mixture of coercive and subversive activity, using conventional and unconventional methods (i.e. diplomatic, military, economic and technological), coordinated by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare (European Commission 2016b). NATO also adopted a similar definition at about the same time. Various expert and think-tank communities have established several other definitions (see Bajarūnas and Keršanskas 2019). However, in all of them, the critical emphasis is on the coordinated nature of hybrid threats.

The second important step in the direction of countering hybrid threats was to agree on strategic practical steps to be implemented by the EU and its member states. In April 2016, the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy approved the Communication *Joint Framework on Countering Hybrid Threats: A European Union Response*, which has become a fundamental document in terms of structuring EU efforts in this area (European Commission 2016b). This document was later reinforced by other EU decisions. In April 2016, the Communication to establish a Security Union recognised that it is necessary to fight hybrid threats and that it is important to assure a greater consistency of internal and external action in the security area (European Commission 2016a). In July 2016, in Warsaw, the president of the European Council, the president of the Commission and the secretary general of NATO signed a joint declaration that defines seven specific areas of cooperation, including the fight against hybrid threats (Tusk et al. 2016). Moreover, in response to the Salisbury poisoning of former Russian intelligence agent Sergei Skripal and his daughter, on 22 March 2018 the European Council agreed that the EU must strengthen its resilience to chemical, biological, radiological and nuclear-related risks through closer cooperation both between the EU and its member states and with NATO (European Council 2018). In June 2018, the Joint Communication *Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats* was issued (European Commission 2018c). In December 2018, the European Council agreed on an EU Action Plan for disinformation (European Commission 2018a). Moreover, the EU's new strategic agenda for 2019–24, agreed in June 2019, explicitly mentions resilience, hybrid threats and disinformation for the first time—and considers them to provide a strong mandate for the EU's future work (European Council 2019a). According to the agenda, the main priorities of the EU in the area of 'protecting citizens and freedoms' are increasing the EU's resilience to both natural and man-made disasters and protecting our societies from malicious cyber activities, hybrid threats and disinformation.

As regards the external aspect of resilience, in November 2017, the EU adopted *A Strategic Approach to Resilience in the EU's External Action*, which contains 'Ten Guiding Considerations of a Strategic Approach to Resilience' (European Commission 2017). Moreover, the Eastern Partnership Summit Declaration of 2017 (Council of the EU 2017) refers to resilience in quite a number of instances. Along with societal and economic definitions of resilience, the declaration also elaborates on resilience in the security field—for example, cooperation and EU support in security sector reform, the implementation of integrated border management, the disruption of organised crime, and tackling hybrid threats and disinformation.

Finally, in December 2019 the European Council Conclusions on complementary efforts to enhance resilience and counter hybrid threats were adopted (European Council 2019b). The Conclusions explicitly noted the need to strengthen the role of and support for the Hybrid Fusion Cell of the EU Intelligence Centre. The Conclusions also place emphasis on the importance of providing continued support to partners in terms of strengthening resilience and countering hybrid threats. This decision by the EU member states will place additional pressure on the EU institutions to contribute to the resilience of Georgia, Ukraine and Moldova. Additionally, the Conclusions also focus on EU–NATO cooperation, with the role of the Hybrid CoE and NATO Centres of Excellence being mentioned in this context. The Conclusions also outline an agreement to ask the Commission to carry out a mapping exercise on the enforcement of existing hybrid threat tools which could lead to the development of new initiatives; by creating such a map we will have a comprehensive picture of where the EU is in the fight against hybrid threats. Finally, the Conclusions emphasise the need to provide the European External Action Service's strategic communication teams (Stratcom Task Forces) with the necessary resources. The Commission is also encouraged to look for more effective tools to enhance the implementation of anti-disinformation commitments by social media platforms.

The Finnish EU Presidency of the second half of 2019 did a fabulous job of moving the work of combating hybrid threats forward within the EU and keeping this topic high on our political agenda. There is a need for Croatia in the first half of 2020 and Germany in the second half to keep the same pace and maintain momentum.

The aforementioned actions represented big decisions for the EU, hardly imaginable in 2014. Nevertheless, these big decisions have also been accompanied by a number of practical steps.

After long debates, access has been granted to the European Defence Fund for projects that aim to counter hybrid threats. A permanent European Council working party—the Enhanced Resilience and Countering Hybrid Threats group—was established in the summer of 2019. Over the last year the East Stratcom Task Force and Hybrid Fusion Cell have been established, a cyber strategy has been agreed, the above-mentioned Action Plan for disinformation (including its Rapid Alert System and enhanced strategic communications teams) has been implemented and the European Commission's September 2019 proposal on election protection has been approved. Both the Action Plan for disinformation and the

Commission's proposals on election protection demonstrate the strong shift in focus towards internal security: actions have included the establishment of the Fact-Checkers network, support for election cooperation networks, the implementation of protections against cybersecurity breaches and unlawful data manipulation, battles against disinformation campaigns, and the tightening of rules on European political party funding.

A critical step in the right direction was the decision to establish the Hybrid CoE in April 2017. Established by 9 like-minded EU and NATO states, the centre's membership had grown to include 27 participating states by the end of 2019, with more candidates due to join. From the day of its establishment the centre started to promote dialogue and consultation among participating countries at the EU–NATO strategic level; to research and analyse hybrid threats and methods of countering such threats; and to organise exercises to strengthen the participating countries' individual capabilities, as well as cooperation among the participating countries, the EU and NATO in the battle against hybrid threats. The centre promotes dialogue among governmental and non-governmental experts from a wide range of professional and academic sectors. It also cooperates with interested communities, dedicating special attention to the problems that give rise to hybrid threats, how they are best detected and ways to improve the ability of organisations to deal with hybrid threats. However, there are still many areas in which the centre should apply focus, including exercises and training, countering election interference, deterrence in a hybrid threat environment, critical infrastructure protection against hybrid threats and conceptual modelling for hybrid threats. The centre should also become a trusted partner for actors in the academic community.

Both in parallel to the EU and in many cases in concert with it, NATO is also doing a lot in this context. The best deterrent, and only way to achieve regional stability, is to deploy US and NATO troops in the Baltic states and Poland on a permanent basis. NATO's enhanced forward presence, with four battle groups (American, German, Canadian and British) deployed in Poland, Lithuania, Latvia and Estonia, is an important contribution. At the NATO summit in Warsaw in July 2016 a decision was taken on NATO's seven baseline resilience requirements.[3] At the NATO summit in Brussels in July 2018 it was agreed to establish Counter Hybrid Support Teams. With regard to NATO's response to hybrid threats and disinformation, it has also made two important decisions: to establish strategic communication capabilities at NATO headquarters and to initiate the establishment of the NATO Strategic Communications Centre of Excellence (Riga). NATO Crisis Management Exercises have begun to include hybrid scenarios comprising disinformation, threats to critical infrastructure and 'grey zone' situations. Also as part of NATO's response to hybrid threats, regular hybrid-scenario-based North Atlantic Council (NAC) discussions have been initiated.

Next steps

As the above discussion shows, significant progress has already been achieved in recent years on countering hybrid threats and enhancing resilience at national and European levels. However, there is still a lot more that Europe could and should do.

In spite of the growing awareness of Russia's actions, there is still a lack of top-level political commitment in the EU and NATO to fight them in earnest. Countering hybrid threats should be one of the top priorities on the agendas of the EU and NATO. Security experts and political leaders now have an increased understanding of Russia's hybrid threat activities. However, this is not enough: we have to constantly seek more information and exchanges of experience on the issue among EU and NATO countries. Moreover, there is a constantly growing need to understand China's use of hybrid threats, among other factors in this context.

The EU and its member states should continue to define hybrid threats. The key parameters are well known (ambiguity, coordinated approach, emphasis on vulnerabilities etc.), but there is still a lot to do in the context of determining the indicators of hybrid threats, and their prioritisation, tracking, detection and attribution. Here the contribution of the Hybrid CoE, alongside other top EU think tanks, will be vital.

The EU and its members states should speed up the implementation of the 2016 Joint Framework on Countering Hybrid Threats and other relevant EU decisions. The Joint Framework encompasses 22 specific and practical steps, many of which deserve to be more rapidly implemented. In the discussion and clarification of hybrid threats, it is even more imperative to pursue concrete actions to fight these threats, both domestically and through multilateral actions. Thus a key priority should be to strengthen resilience and deterrence against hybrid threats at EU level.

With the new strategic agenda agreed and the new European Commission in place, the Commission should, without delay, form a roadmap for how to implement tasks concerning resilience, hybrid threats and disinformation. The EU should invest more in effective technical and intellectual means of monitoring hybrid threats (e.g. strengthening the EU's Hybrid Fusion Cell and Stratcom units), as well as analysing them, refuting lies and disinformation in case of informational attacks, and designing critical strategies for countering hybrid threats.

Work at the EU level on countering disinformation remains of vital importance. The European Commission has done well to encourage online platforms to take responsibility for tackling disinformation. Facebook, Google and Twitter have all made some progress under the self-regulator Code of Practice on disinformation agreed in 2018, and they continue to work in this direction. There is a need to make use of the EU's Rapid Alert System, agreed with the adoption of EU Action Plan for disinformation, even more effective.

The Finnish EU Presidency of the second half of 2019 was extremely helpful in bringing the topic of hybrid threats to the top of the EU's agenda. The presidencies of Croatia, in the first half of 2020, and Germany, in the second half, should keep up the pace and maintain momentum. We should continue to keep hybrid threats visible at the strategic level—especially through the ministerial-level scenario-based policy discussions that were implemented during the Finnish Presidency.

The protection of elections from hostile propaganda and interference from abroad should remain our top priority. Our citizens should have the right to express their democratic choices in elections freely and without manipulation or interference from abroad. In this regard the Commission's 2019 proposal on electoral protection is yet to be fully implemented.

The involvement of civil society remains crucial. Unpredictability and uncertainty make hybrid threats more difficult to identify. Therefore, national elites and the media have the important, yet difficult task of clarifying these threats so that our societies remain vigilant and resilient. Indeed, such clarification is crucial to enhancing societal resilience and engaging civic society, the media and the IT sector in our efforts to counter hybrid threats. There is a need to support information pluralism, invest in civic awareness through education and maintain an independent press that responds swiftly to any disinformation. EU resources should be made available in this context. The European Commission could also pay more attention to and help independent social resilience initiatives in member states. One such example is Lithuania's private initiative, Debunk.eu (Delfi 2020), which unites media outlets, journalists and volunteers for a single purpose: to make society more resilient to orchestrated disinformation campaigns. With this in mind, there is even a strong case for replacing the phrase 'whole of government' with 'whole of society'.

Although implementation of the response to hybrid threats should remain part of the national competences, the EU should provide assistance for interested national governments to implement a coordinated response at the national level. Coordination is very important, but it is not enough—the enemy is ingenious and has the advantage of the initiative, so the 'old toolbox' will not always help. In all areas of security, bold actions and new tools are needed. The EU should become a platform for sharing experience and information between member states.

There is an urgent need to strengthen EU efforts to support Eastern Partnership countries—especially Georgia, Moldova and Ukraine—in countering hybrid threats and bolstering resilience. Resilience, as the capacity to sustain and overcome external and internal shocks to society and to the state and its institutions, has a special value and importance for the Eastern neighbourhood as it goes hand in hand with sustainable development. As part of the post-2020 development of the Eastern Partnership initiative, it would be advisable to expand the profile of resilience as a key domain for cooperation with our Eastern Partners. A practical, project-driven way of addressing resilience should complement the employment of resilience as a strategic principle.

Another new area that should be explored is hybrid threats to economic security. Here, again, the Commission could play an important role, even if this remains a national prerogative.

Last but not least, we need more EU–NATO coordination of activities and multilateral initiatives, exchanges of sensitive intelligence, preparation of joint reports and,

especially, joint EU–NATO exercises covering hybrid-threat scenarios. There should be more and closer cooperation between the EU's Hybrid Fusion Cell and NATO's Hybrid Analysis Branch. In an ideal situation, an informal coordinating community of EU and NATO experts constantly exchanging information and experience could be formed. Also in the context of EU–NATO cooperation, there is an obvious need to strengthen the activities of the Hybrid CoE.

Conclusion

Since Russia's annexation of Ukraine's Crimea region in 2014, a great deal has already been done to strengthen the resilience of the EU and NATO with regard to hybrid threats. These efforts should be acknowledged and their pace and intensity maintained. However, due to the ever-changing nature of hybrid threats, constant vigilance is needed. We need a more strategic approach to countering hybrid threats, the implementation of national adjustments (to embrace the 'whole of government' and 'whole of society' approaches), more EU and NATO cooperation, and the greater involvement of our societies.

Notes

1. The assessments and views expressed in the article are entirely those of the author and should not be treated as the official position of the Ministry of Foreign Affairs of the Republic of Lithuania.
2. These technologies include the employment of military force; economic, financial, and energy-related measures; social pressure; the use of asymmetric tactics; the implementation of combined and coordinated overt and covert military, para-military and civilian measures; attempts to intimidate an enemy before battle; the manipulation or distortion of information; Soviet Cold War–era 'active measures'; guerrilla warfare and many more.
3. NATO's seven baseline resilience requirements are assured continuity of government and critical government services; resilient energy supplies; the ability to deal effectively with the uncontrolled movement of people; resilient food and water resources; the ability to deal with mass casualties; resilient civil communications systems; and resilient civil transportation systems.

References

Bajarūnas, E., & Keršanskas, V. (2019). Hybrid threats: Analysis of their content, challenges posed and measures to overcome. *Lithuanian Annual Strategic Review*, *16*(1), 123–70. https://content.sciendo.com/configurable/contentpage/journals$002flasr$002f16$002f1$002farticle-p123.xml. Accessed 14 February 2020.

Council of the EU. (2017). Eastern Partnership Summit – Joint declaration. 24 November. Press Release, 695/17. https://www.consilium.europaeu/en/press/press-releases/2017/11/24/eastern-partnership-summit-joint-declaration/pdf. Accessed 14 February 2020.

Delfi. (2020). Google presented Lithuanian initiative to world. 17 February. https://en.delfi.lt/politics/google-presented-lithuanian-initiative-to-world.d?id=83550653. Accessed 2 March 2020.

European Commission. (2016a). *Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union*. Communication, COM (2016) 230 final, 20 April. https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0022.02/DOC_1&format=PDF. Accessed 14 February 2020.

European Commission. (2016b). *Joint framework on countering hybrid threats: A European Union response*. Communication, JOIN (2016) 18 final, 6 April. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. Accessed 14 February 2020.

European Commission. (2017). *A strategic approach to resilience in the EU's external action*. Communication, JOIN (2017) 21 final, 7 June. https://ec.europa.eu/knowledge4policy/publication/2017-joint-communication-strategic-approach-resilience-eus-external-action_en. Accessed 14 February 2020.

European Commission. (2018a). *Action plan against disinformation*. Communication, JOIN (2018) 36 final, 5 December. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf. Accessed 14 February 2020.

European Commission. (2018c). *Increasing resilience and bolstering capabilities to address hybrid threats*. Communication, JOIN (2018) 16 final, 13 July. https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf. Accessed 14 February 2020.

European Council. (2018). European Council meeting (22 March 2018) – Conclusions. 23 March. https://www.consilium.europa.eu/en/meetings/european-council/2018/03/22–23/. Accessed 14 February 2020.

European Council. (2019a). *A new strategic agenda, 2019–2024*. Brussels, 20 June. https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019–2024/. Accessed 14 February 2020.

European Council. (2019b). Countering hybrid threats: Council calls for enhanced common action. Press Release, 10 December. https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/. Accessed 14 February 2020.

Tusk, D., Juncker, J.-C., & Stoltenberg, J. (2016). Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg. 8 July. https://www.consilium.europa.eu/en/press/press-releases/2016/07/08/eu-nato-joint-declaration/. Accessed 14 February 2020.

Author biography

Eitvydas Bajarūnas *is Ambassador-at-Large in the Ministry of Foreign Affairs of Lithuania. He has previously held various foreign postings, including ambassador to Sweden, consul general of Lithuania in Saint Petersburg (Russia), and deputy chief of the Lithuanian mission to NATO. He has been political director of the Ministry of Foreign Affairs, and the director of various units in the Ministries of Foreign Affairs and Defence.*