idn E-Briefing Papers

Hybrid Threats in the Context of European Security

Report of the international conference organized at the National Defence Institute (IDN) on 18 May 2021 under the framework of the Portuguese Presidency of the Council of the European Union

Rita Costa

idn Instituto da Defesa Nacional

Os *E-briefing Papers* do Instituto da Defesa Nacional visam proporcionar o acompanhamento de temas e debates atuais nos planos da segurança internacional e das políticas de defesa nacional, incluindo resultados da investigação promovida pelo IDN, sobretudo na sua vertente aplicada e de apoio à decisão política, bem como contributos de outros analistas e investigadores associados do Instituto.

FICHA TÉCNICA

Diretora
Helena Carreiras

Coordenação Cientifica
Isabel Ferreira Nunes

Editor
Luís Cunha

Centro Editorial
António Baranita e Luísa Nunes

Propriedade, Edição e Design Gráfico
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa, Portugal
Tel. + (351)211 544 700 **Fax**: + (351)211 548 245
Email: idn.publicacoes@defesa.pt
http://www.idn.gov.pt

ISNN: 2184-8246

Introduction

Hybrid threats are not a new theme in the security agenda. However, two main developments at the international level – increased geopolitical competition and new technological developments – have enabled a wider expression of this phenomenon. The most visible face of hybrid warfare comes in the form of cyber-attacks, disinformation, services denial, rising extremism or surveillance, and targeting of critical infrastructures, necessary to the normal functioning of states, societies, and businesses. The less visible but no less harmful dimension of hybrid threats comes under the form of influence operations, which may hinder the pursuit of foreign policy objectives of states or even the business continuity of public and private sectors and services.

In the European context, the emergence of hybrid challenges not only had a political impact on how the EU and member states collectively address it, but it has also had consequences on its institutional architecture, leading to essential adaptations within the EU itself. These institutional developments are meaningful from an European political and operational point of view and for potential cooperation with other partners, namely with NATO. From a political perspective, it formally signals how the EU perceives and assesses the importance of hybrid threats and their disruptive potential. From an operational perspective, it underlines the EU collective intent and capacity to protect and rapidly respond to a new scale of security threats. This new dimension of insecurity has also strengthened European cooperation with NATO, in both the hybrid and the cyber contexts.

Considering the challenges they pose to democratic systems, it is not surprising that tackling hybrid threats has been defined as a priority by the EU's Strategic Agenda 2019-2024 and by the Portuguese Presidency of the Council of the European Union. In this regard, the Strategic Compass will provide a unique framework to address hybrid threats and render more concrete the collective ambitions concerning CSDP. Living up to this challenge requires a far-reaching whole-of-society and whole-of-government approach in order to build resilience and sustain a more comprehensive understanding of security.

To tackle these issues, the National Defence Institute (IDN) and the Ministry of Foreign Affairs organized a high-level conference on 18 May 2021, under the framework of the Portuguese

Presidency of the Council of the European Union. The event took place under Chatham House rule and promoted a reflection on the conceptual and policy boundaries posed by hybrid threats; the need for a more comprehensive approach to security in order to counter these threats; the opportunities posed by closer dialogue, coordination, and cooperation with partners; and how a more resilient stand may lead to a more preventive and reactive collective approach. The event gathered over 200 registered participants from governments, EU institutions, academia and think tanks. This report outlines the main conclusions of the conference.

Hybrid threats – What is in the name?

Despite the growing discussion on hybrid threats in recent years, there is still no common definition over this category of threats, which risks jeopardizing the credibility and legitimacy of the EU. In general terms, hybrid threats can be characterized as a complex set of actions used by state or non-state actors to manipulate the systemic vulnerabilities of target states or organizations. Hybrid methods and techniques are usually employed ambiguously, making plausible deniability easier by actors with totalitarian views of power towards the achievement of their own foreign policy objectives. Hybrid tactics are intentionally designed to create confusion and hide the intent of perpetrators. For this reason, it is essential to analyze these activities not just individually, but as elements of complex cross-domain threats, taking into account the geopolitical and cultural peculiarities of each hybrid actor, in order to understand their goals.

Hybrid threats are not a new phenomenon, but the current reality – characterized by technological developments and broad social media use – has enhanced their level of sophistication and impact, providing hybrid actors with new and more effective means to reach target audiences, with lesser costs and lower risks of attribution. In this context, the role of social media is paramount as hybrid actors can access personal information to target individuals in a personalized manner, in order to manipulate their views through disinformation campaigns or even for espionage purposes. In the future – as further technological developments ensure wider access and ambiguity and new global players emerge and learn from old hybrid actors – it is expected that authoritarian regimes will continue to target democracies by using hybrid methods to degrade democratic values and undermine policymaking, while guaranteeing the stability of their own regimes.

To effectively tackle hybrid threats, the role of intelligence services is vital. Intelligence increases knowledge and awareness of hybrid activities, which, in turn, supports decision-making at the political level. As such, even though the EU has been moving in the right direction, increased tools and capacities could further help strengthen intelligence services and provide a stronger basis for policymaking.

The multidimensions of hybrid threats

Hybrid threats challenge conventional expectations. Therefore, it is essential to shift away from a traditional linear rationale in order to fully understand the strategic thinking of hostile actors. Hybrid actors are characterized by strong strategic patience. They can be both state and non-state entities, while having different natures. Hence, in order to understand them, it is essential to grasp, first and foremost, their strategic culture. Multiple hybrid actors can act in the same space simultaneously, creating chaos even in the most prepared countries. Their strategic interests and goals – which can be both short, translating into real-life changes, or long term – define their respective targets, such as nations, regions, institutions, or even themes. The multidimensionality of their targets, in turn, poses challenges on how to respond, as it is not easy to understand what exactly is being threatened and the possible spillover effects of those same activities. Moreover, the domains and tools used by hybrid actors are employed through tailor-made approaches that focus on finding the vulnerabilities of potential targets and/or creating enablers to generate vulnerabilities. The tools are then combined in complex ways, which creates a cascading effect that results in the product of interactions, including the actions of hybrid actors and the reaction of their targets.

The bulk of the activity of these actors unfolds in phases below the detectability threshold. These are the priming phase, meaning the preparation phase, when hybrid actors are concerned with understanding patterns and learning about the field; and the destabilization phase. The two phases entail actions such as interference, influence and campaigns. Hybrid actors aim to stay below this threshold. However, when their objectives are not fulfilled and the matter is important enough, escalation can lead to a visible coercion phase, which entails warfare-like activity. Yet, it is essential to remember that long before this more visible level is reached, hybrid activities have been creating damage in the background.

Countering these threats relies on three different elements – understanding, resilience, and deterrence – which relate to the phases of activity by hybrid actors. When it comes to understanding the different dimensions, activities, domains, tools, targets and nature of actors, the role of intelligence is essential in order to achieve adequate situational awareness, which, in turn, allows the employment of an ecosystem-based approach where all relevant areas are addressed in a synergetic way towards building enough resilience. Resilience-building requires a whole-of-government and whole-of-society approach that focuses on securing identified vulnerabilities. Furthermore, besides identifying vulnerabilities, it is necessary to prioritize them, which should be done while taking into account the capabilities factor of each actor, as they define which vulnerabilities they are able to explore. It is also essential to understand that all EU countries must be prepared to tackle these threats, as one single country not prepared remains a vulnerability for the entire bloc. In this regard, continuous lessons learned and identified processes, technical solutions and innovation are of vital importance to enhance of all those three aspects.

Countering hybrid threats – An opportunity for cooperation

The EU's ultimate goals regarding hybrid threats are to prevent attacks on EU institutions and member states by raising their resilience to a level too costly for perpetrators; to detect threats in advance by establishing the best possible situational awareness; and to develop internal capacity mechanisms and cooperation frameworks within member states in order to ensure a swift recovery from any attack. Overall, the aim is set on improving individual and collective responses. To accomplish these goals, cooperation is essential even for the most well prepared states, as it can improve the awareness of states concerning threats and establish the highest possible level of resilience and response.

Taking into account the inherent linkage between internal and external security, and even though the responsibility to counter hybrid threats lies primarily at the national level, the EU has been promoting cooperation initiatives to improve resilience and situational awareness. Accordingly, it contributes to the development of effective national strategies and responses. At the internal level, the EU has fostered a whole-of-government approach, as a necessary condition to tackle hybrid threats. Furthermore, the establishment of the Hybrid Fusion Cell, the Rapid Alert System, the

European Cooperation Network on Elections and the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats are important steps taken towards further internal cooperation. These steps lay the foundation for further action under the EU Security Union Strategy, such as on situational awareness and on the expansion of the network of sources, including EU agencies such as FRONTEX, ENISA and Europol. Also in progress is the introduction of EU resilience baselines, inspired by NATO's seven baseline requirements.

The external component of cooperation efforts entails two tracks. The first is cooperation with like-minded partners. In this regard, NATO is an essential partner with hybrid threats already identified as one of the seven priority areas for reinforced cooperation between both entities. Also important are the G7 format and the Australian-led Countering Foreign Interference Summit. These networks of cooperation are extremely valuable as they combine individual geographic experiences with various best practices. The second track entails sharing know-how and assisting partners in the EU neighborhood towards increasing their own capabilities to counter hybrid threats. Hybrid risk surveys are a particularly vital initiative in this regard.

Due to their nature, tackling hybrid threats remains an extremely complex endeavor. This complicates the development of a hybrid toolbox since this toolbox would have to entail both internal and external components. Whilst the internal side would focus on sectoral resilience measures aimed at preventing hybrid attacks, the external one would involve detection and response tools. In this regard, the response should be focused on imposing costs on perpetrators, since the ambiguity of hybrid threats makes attribution extremely difficult, both in technical and political terms, complicating the imposition of sanctions.

Improving the resilience of states and societies

Strengthening the resilience of states and societies is perhaps the most ambitious task of the EU's external action efforts. Together with the integrated approach, it was one the most innovative elements of the European Union Global Strategy and has genuinely become a dogma amidst the implementation of EU foreign policy ever since. However, this dogma must also face the changing reality of resilience. Resilience is fluid, evolutional, dynamic, multifaceted and, above all, a long term investment. As such, this investment may see a return, but may also be exposed to risks and losses.

In this sense, building resilience is a daunting task that might take years to show results, and at the same time, can be easily jeopardized by unforeseen shocks, like the COVID-19 pandemic. Hybrid threats, whether from a technological or geopolitical standpoint, are the mirror of a fast changing world, giving us a clear indication of the pace at which the complex task of resilience-building is changing.

As one of the frontlines of the EU's external action, CSDP missions and operations are both a potential victim and a solution vis-à-vis hybrid threats. While hybrid actors target them as part of a broader attempt to disrupt the EU presence and interests in host countries, they can also build resilience that reduces the countries vulnerabilities to these threats. Hence, increasing resilience in host states and enhancing CSDP capacities should be understood as a mutually reinforcing task.

Three general lessons should be taken into account in the future, particularly for the delivery of the Civilian CSDP Compact. The first lesson is that stronger geopolitical competition increases the risk of hybrid activities against the EU's interests. In the face of increasing geopolitical competition, a boost in strategic communications is needed to better communicate deployments and better calculate all possible repercussions and threats to EU interests on the ground posed by hybrid activities. In order to fully achieve this, civilian-military synergies should be better leveraged, as the military side is essential, not only for the protection of civilian deployments, but also to provide the necessary awareness and information. Finally, there is also a need for a reversed understanding of the role of strategic communications and civilian CSDP missions, meaning that CSDP missions should be understood as an instrument that serves broader communication goals, and not the other way around.

Second, some threats are increasingly being produced at an industrial scale, like the case of disinformation. To counter these industrialized threats, appropriate investment towards resilience is needed so that the response matches the scale of production of disinformation. In this regard, the use of artificial intelligence should play a significant role.

Lastly, as hybrid threats encompass a wide variety of tactics, both overt and covert, improving the resilience of host states requires the ability to see the whole picture. In this regard, strategic foresight techniques are essential to better capture the future evolution of these threats and anticipate them. Since hybrid actors act faster than the EU, timely anticipation is particularly

relevant to counter hybrid threats as it allows time to prepare. Even though the EU already has considerable analytical capacities, more intelligence cooperation would enhance these skills.

In order to reinforce resilience-building efforts, strategic adaptability is critical. In this sense, the EU should go beyond the integrated approach in order to make sure that, not only are the EU's structures coordinated, but that these instruments are also synergistically deployed, in an effective and flexible format at the theatre of operations. However, the effectiveness of resilience-building is not easily measured due to its long-term character, which makes commitment and progress towards the improvement of the instruments a key evaluation measure. The Civilian CSDP Compact should also play an important role, especially if it fully delivers through the fulfillment of political commitments.

Main takeaways

- Hybrid activities must be analyzed as elements of complex cross-domain threats, with regard to the strategic cultures of hybrid actors, in order to best assess their goals and aims.
- All EU member states must be prepared to tackle hybrid threats, as the vulnerabilities of one country represent a liability for the whole block.
- The role of intelligence is paramount to tackling hybrid threats. Increased tools and capacities and intelligence cooperation could further strengthen this capability.
- Hybrid threats challenge the conventional linear strategic rationale, so it is essential to shift towards a non-linear way of thinking to comprehend these threats in full.
- Resilience-building should be prioritized, taking into account the vulnerabilities that hybrid actors have the capability to explore.
- Due to the ambiguity of hybrid threats, detection, let alone attribution, remain difficult tasks. In this regard, the EU should focus on raising the costs of activities led by hybrid actors in order to increase deterrence.
- Cooperation is a win-win situation as it allows for exchanging best practices, leading to the best possible preparation.
- The resilience of neighbors is in the best interest of the EU as hybrid threats recognize no borders.

- Strategic communications are key when building resilience in partner countries and CSDP missions and operations should be interpreted as an instrument that serves broader strategic communication goals.
- The effectiveness of resilience-building can be evaluated by the level of commitment and progress made towards the improvement of the EU toolkit.

Recommended readings

De Coning, C., 2021. *Strengthening the resilience and adaptive capacity of societies at risk from hybrid threats*. Helsinki: Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210601_Hybrid_CoE_Working_Paper_9_Strengthening_the_resilience_and_adaptive_capacity_of_societies_WEB.pdf

European Commission, 2020. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy (COM/2020/605 final).* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

Faleg, G. and Secrieru, S., 2020. *Russia's Forays into Sub-Saharan Africa: Do you want to be my friend, again?.* European Union Institute for Security Studies, Brief 6. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%206%20Russia%20Africa_0.pdf

Falk, B. J., 2020. *Strategic citizens: Civil society as a battlespace in the era of hybrid threats*. Helsinki: Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2020/11/SA25_Strategic-Citizen.pdf

Giannopoulos, G., Smith, H. and Theocharidou, M., 2020. *The Landscape of Hybrid Threats: A Conceptual Model.* Luxembourg: Hybrid CoE and European Commission. Available at: https://euhybnet.eu/wp-content/uploads/2021/01/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf

Ivan, C., Chiru, I. and Arcos, R., 2021. *A whole of society intelligence approach: critical reassessment of the tools and means used to counter information warfare in the digital age*. Intelligence and National Security, online first, pp. 1-17.

Kalniete, S. and Pildegovičs, T., 2021. *Strengthening the EU's resilience to hybrid threats*. European View, 20(1), pp. 23-33

Keršanskas, V., 2021. *Deterring disinformation? Lessons from Lithuania's countermeasures since 2014*. Helsinki: Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210427_Hybrid-CoE-Paper-6_Deterring_disinformation_WEB.pdf

Missiroli, A., 2021. *Geopolitics and strategies in cyberspace: Actors, actions, structures and responses*. Helsinki: Hybrid CoE. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210622_Hybrid_CoE_Paper_7_Geopolitics_and_strategies_in_cyberspace_WEB.pdf

Policy Department for Citizens' Rights and Constitutional Affairs, 2019. *Disinformation and propaganda - impact on the functioning of the rule of law in the EU and its Member States*. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

International Conference "Hybrid Threats in the Context of European Security"

National Defence Institute - Ministry of Foreign Affairs, 18 May 2021

The purpose of this conference is to analyse the conceptual and policy boundaries posed by hybrid threats and to examine the role played by a more comprehensive approach to security, in order to counter hybrid threats, across all EU relevant policy sectors in a strategic, coordinated and effective manner. It will evaluate the opportunities offered by closer dialogue and coordination within the EU and by better cooperation with other partner organisations. Lastly, it will reflect on how a more resilient approach, from states and societies, may offer the best preventive and reactive tool to countering hybrid threats.

09:00 Welcome Remarks

Helena Carreiras, Director of the National Defence Institute

Madalena Fischer, Political Director, Ministry of Foreign Affairs of Portugal

09:15 - 10:00 Hybrid threats – What is in the name?

Casimiro Morgado, Director Intelligence and Situation Centre, EEAS

Chair: Isabel Ferreira Nunes, Director Research Centre, National Defence Institute

10:00 - 10:45 The multidimensions of hybrid threats

Hanna Smith, Research and Analysis Director of the European Centre of Excellence for Countering Hybrid Threats, Helsinki

Chair: Carlos Pires, Director of the Portuguese External Intelligence Service

Pause

11:00 - 11:45 Countering hybrid threats - An opportunity for cooperation

Joanneke Balfoort, Director Security and Defence Policy, EEAS

Chair: Jorge Aranda, Security Policy Director, Ministry of Foreign Affairs of Portugal

11:45 - 12:30 Improving the resilience of states and societies

Giovanni Faleg, European Union Institute for Security Studies

Chair: Navy Captain Sérgio Caldeira Carvalho, Cyber Defence Centre

12:30 Augusto Santos Silva, Minister of Foreign Affairs