Facing Hybrid Threats through Consolidated Resilience and Enhanced StratCom

Final report

Conference proceedings from an event co-organised by the Romanian Ministry of Foreign Affairs and the EU Institute for Security Studies (EUISS). The high-level conference was an official event of the Romanian Presidency of the Council of the EU.

28 February - 1 March 2019, Bucharest

Overview

From 28 February to 1 March 2019, the Romanian Ministry of Foreign Affairs and the EUISS organised a high-level conference and a simulation in Bucharest, Romania, with a view to enhancing EU action on hybrid threats, resilience and strategic communication (HRS). The conference took place on the 28 February at the Palace of the Parliament and panellists included senior representatives from the European Commission, the European External Action Service, the European Centre of Excellence for Countering Hybrid Threats, NATO and the governments of Germany, Lithuania, Romania and the United Kingdom, plus a host of think tank analysts and academics. The conference opened with keynote speeches from the Romanian Minister of Foreign Affairs, Teodor Melescanu, and the European Commissioner for the Security Union, Sir Julian King. Over 130 participants attended the HRS conference, with representatives from 25 EU member state governments and over 15 different ministries and bodies present. A wide array of EU institutions were also present, as were numerous academics and think tankers and partners such as NATO and the United States. The HRS simulation that took place on 1 March at the Romanian National Defence University (Carol I) brought together over 75 governmental and EU experts to play out a crisis situation in a fictitious country bordering the EU and to design an effective HRS response at the EU level.

Main conclusions

The two-day initiative was characterised by rich debate and a healthy exchange of ideas on how best to enhance the EU's response to HRS. In particular, it gave rise to a number of relevant conclusions that can be seen as a contribution to future EU initiatives on hybrid threats. The overarching conclusions include:

EU norms and values are the guiding principles of the Union's action when countering hybrid threats

If the EU is to maintain its credibility in the face of hybrid threats, it needs to have a consistent joined up approach to tackling hybrid threats and enhancing resilience and strategic communication. The EU should maintain an open economy and champion freedom of expression, but the Union should also ensure the protection of EU citizens from disinformation by employing both a top-down and bottom-up approach and investing in societal resilience. This form of 'soft resilience' is as important as enhancing the security of critical infrastructure. The power of the EU's ability to counter harmful and false messaging rests in the Union's ability to stay true to its core values.

Better coordination among institutions, governments and policy sectors is of paramount importance
It has become almost cliché to talk about overcoming silo mentalities and approaches, but the reality is that there is a lack of effective coordination and permanent dialogue on HRS topics among EU member states, EU institutions, the private sector, civil society organisations and broader society. The EU has taken important steps forward to overcome 'hybrid silos'. Initiatives such as the Hybrid Fusion Cell, the EU Hybrid Playbook and the StratCom Taskforces have bolstered EU capacity, but there is still scope to improve coordination within and between EU member states, particularly in order to reach higher operational effectiveness.

Deepen EU-NATO cooperation on hybrid threats
Cooperation between the EU and NATO on hybrid threats cannot be overstated. Although NATO has a distinct approach to hybrid threats, the alliance clearly does not have all of the tools needed to counter hybrid threats. Both organisations have enhanced their cooperation – as can be seen from the Parallel and Coordinated Exercises (PACE). Given the fact that a host of new state and non-state actors are employing hybrid tactics, there remains a strong impetus for more and better EU-NATO cooperation in this field.

Exploiting communities of expertise is a vital part of resilience
Effective strategic communication presumes that policymakers, media professionals and the intelligence community work together to detect and refute false and harmful messaging. Building and sustaining such expert communities is an important component of the EU's resilience. Steps to bring together experts in health, energy, transport, finances, space, media, cyber, etc. should be championed and there is no substitute for regular hybrid exercises to test the EU's preparedness and responsiveness.

Resilience and the challenge of new technology and digitalisation
Technological changes can expose vulnerabilities in the EU's critical infrastructure while also bringing huge economic and social benefits. The development of sophisticated telecommunications networks and emerging technologies such as artificial intelligence mean that the security of the EU's digital supply networks and infrastructure should be galvanised. There is clearly a need to think about personal data usage, digital resilience, foreign direct investment, the security of electoral processes and free and fair electoral campaigns, intellectual property rights and the responsible use of social media as key aspects of critical infrastructure.

Where hybrid threats are concerned, timing is everything
A challenge is ascertaining whether an isolated incident is connected to a larger strategy or series of actions design to subvert, weaken and/or destabilise societies in the EU and/or its partners. Understanding hybrid threats relies on having in place expertise from different policy domains and academic disciplines. Rapid identification of and reaction to hybrid threats is a key challenge, especially given that 'hybrid expertise' is unevenly located across the EU. Furthermore, there is scope to enhance the resilience of EU partners from an HRS approach and for the EU to learn from the experiences of external partners.

There is no one-size-fits-all approach to strategic communication
Audiences in each EU member state receive and process information in different ways, and so nuanced strategic communication approaches that target specific audiences are required. Historical, cultural and linguistic nuances in each EU member state and partnering countries should be catered for when strategies are developed and deployed. Proactive and positive strategic communication can complement longer-term approaches that are designed to refute fake news and disinformation campaigns.

Patterns of media and information consumption are rapidly changing
Individuals and societies consume media and information in different ways. In a social media rich environment, it has become easier and cheaper to spread disinformation to a mass audience. Sometimes facts-based reporting can be side-lined in favour of 'click baiting'. Increased media literacy is required but there is also a need to think through how our personal data is collected. Increasing amounts of data are shared via online applications and this data can be harvested to create more effective disinformation campaigns. Developing resilience in the digital world is of vital importance especially as awareness is at an incipient stage.