HYBRID THREATS' NEXUSES: TAKING EU-NATO COOPERATION TO THE NEXT LEVEL

How are the threats evolving, and how should the two institutions tackle them?

EUISS side session at the GLOBSEC Forum 2024 – 31 August, Prague, Czechia

EVENT SUMMARY

Hybrid warfare tools, tactics and techniques are rapidly evolving, and democratic allies need to step up their cooperation to counter increasingly interconnected threats. Hostile actors deploy foreign interference tactics in parallel and across various sectors, aiming to amplify their impact. While the EU and NATO broadly share common membership and security challenges, their partnership has been limited due to practical and political obstacles. The growing nexus between foreign information manipulation and interference (FIMI) and cyber threats offers a valuable opportunity for enhanced and fruitful cooperation between the two institutions. To effectively address these evolving threats, the EU and NATO should adapt their policies to the changing security landscape across multiple domains.

On 31 August 2024, the EUISS hosted a side session as part of the GLOBSEC Forum in Prague to discuss the evolving nature of hybrid threats, and particularly the growing cyber-FIMI nexus, as well as the institutional responses by the EU and NATO to these evolving threats. The event brought together experts on hybrid threats as well as policymakers from the EU and NATO. The EUISS also presented its latest Chaillot Paper, *Hacking Minds and Machines: Foreign Interference in the Digital Era*.

The first panel, 'Breaking Hybrid Silos', focused on the growing cyber-FIMI nexus within the foreign interference toolkit. Speakers highlighted the increasing interconnectedness of activities carried out by malign actors to disrupt and manipulate across various domains, citing the examples of political coercion and deepfakes. The panel concurred that these activities present not merely technical challenges, but also significant political and strategic risks. Compartmentalising these risks and activities into separate

silos hinders a holistic and integrated understanding of the nature of the threats faced by the EU and other states and societies. Potential responses discussed included enhanced digital literacy, media independence, regulatory measures, fines, and robust checks and balances.

The second panel, 'Institutional Response', aimed to map the future of EU-NATO cooperation in countering evolving hybrid threats. Speakers argued that the two institutions should regard the FIMI-cyber nexus as a strategic threat and as a tool of warfare used by actors such as Russia and China. The EU, NATO and their respective member states and partners must develop a comprehensive response to malign hybrid activities. They should focus on enhancing common threat analysis, and on developing a stronger deterrence posture, consisting of measures to enhance resilience and tangible response options. The EU and NATO can and should closely collaborate to enhance their capacities, as well as those of partners such as Ukraine and countries in the Western Balkans, in the face of hybrid campaigns.

List of speakers, discussants and moderators

Opening remarks:

Steven Everts, Director, EU Institute for Security Studies (EUISS)

Moderators:

Nad'a Kovalčíková, Senior Analyst for Transnational Security, and Director of the Countering Foreign Interference (CFI) project, EUISS

Giuseppe Spatafora, Associate Analyst for Transatlantic and EU-NATO relations, EUISS

Speakers:

Ivana Karásková, China Team Lead, Association for International Affairs

Andrea Salvi, Senior Analyst for Cyber and Digital issues and Project Director, EUISS

Benedetta Berti, Director of Policy Planning, Office of the Secretary General, NATO

Eva Horelová, Deputy Head of Representation in Czechia, European Commission

Discussants:

Ondrej Ditrych, Senior Analyst for Eastern Europe, EUISS

Alexandra Martin, Senior Analyst, NATO SHAPE