

EU and NATO confront hybrid threats in centre of excellence

[Content preview – Subscribe to **Jane's Intelligence Review** for full article]

Facing a growing threat from hybrid activities and attacks on election processes, EU and NATO states have established a joint centre in Finland to improve their response. Dr Rubén Arcos visits Helsinki to assess the initiative's work to date and its likely future priorities

Key Points

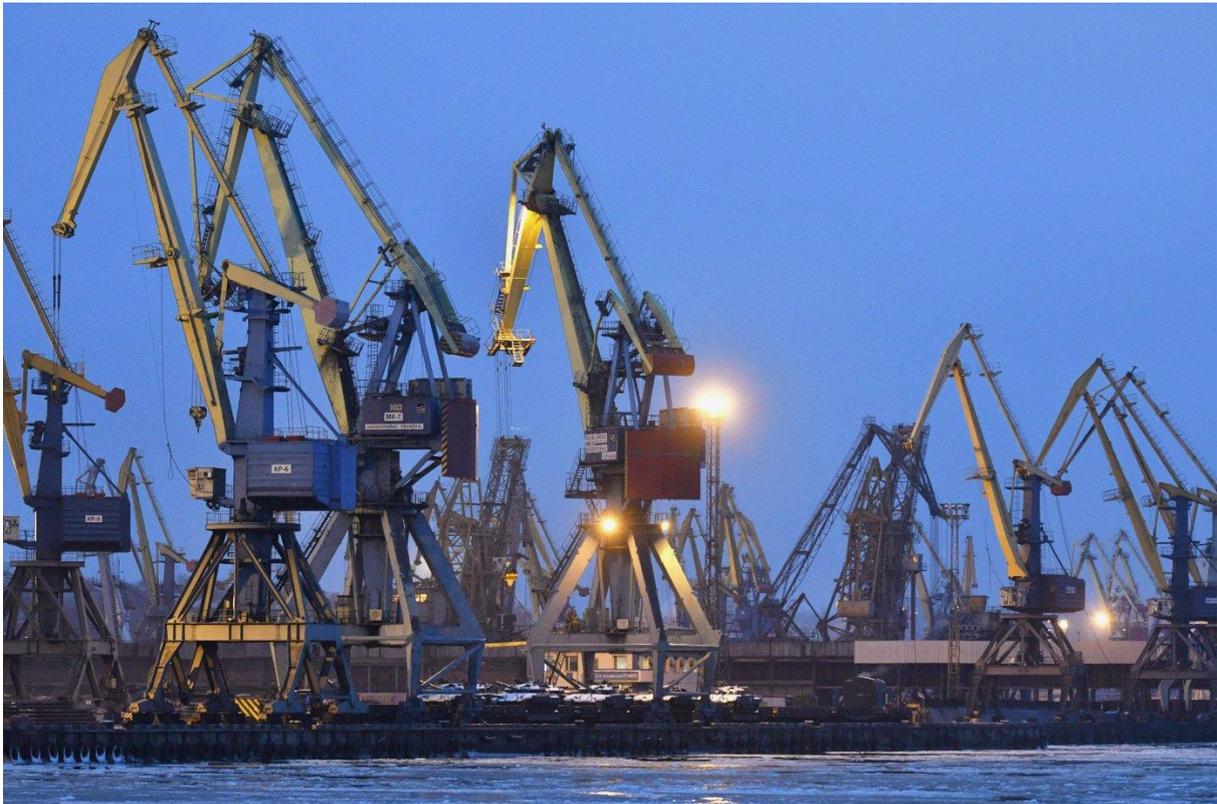
- The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki is an example of EU-NATO co-operation that aims to detect, analyse, and counter hybrid threats affecting its member states.
- The CoE is likely to consolidate its role as an international facilitation hub for practitioners and experts from government and the private sector, complementing existing national and multinational initiatives.
- A key area of future focus will be legal resilience to hybrid threats, which includes forging a better understanding about how hybrid adversaries use legal asymmetries to their advantage.

European elections will take place on 23–26 May 2019 for a new European Parliament, and securing the process from potential interference by foreign and non-state actors will be a priority in the EU's national security agenda. Protection against election interference and countering hybrid threats are live political topics that have prompted much debate, planning, and strategic thinking (see Countering hybrid warfare: selected developments box).

Russia's successful employment of hybrid activities in Ukraine is highly likely to have been a driver behind the EU's boosting of its capabilities to counter hybrid threats. An October 2015 brief of the European Union Institute for Security Studies judged, "Until the Russian operations in Crimea and Eastern Ukraine began in 2014, the assumption of many analysts was that hybrid operations were primarily a strategy used by non-state actors such as separatists in Chechnya, and terrorist organisations like Hizbullah or ISIL [the Islamic State]."

Russian disinformation subsequently continued. On 25 November, three Ukrainian navy vessels en route to the Kerch Strait – the gateway from the Black Sea to the Sea of Azov – and onwards to the Ukrainian port of Mariupol were intercepted by Russian Coast Guard vessels. Under the terms of the 2003 Russia-Ukraine bilateral treaty that regulates the use of the Sea of Azov and the Kerch Strait, "the sea is considered to be internal waters for both countries, and both Ukrainian and Russian commercial and military ships have the right of free passage through the strait".

However, according to the Disinformation Review, a flagship product of the European Union Task Force on Strategic Communication (EU StratCom), the incident had been preceded by a long-term disinformation campaign, including key messages in different outlets. Such messaging included claims in September 2017 that “Ukraine is deepening the seabed for a NATO fleet at the Azov Sea” and in July 2018 that “Ukraine infected the Azov Sea with cholera”, as well as a conspiracy theory in November 2018 that Russia’s seizure of the vessels was because the “UK and Ukraine secret services were apparently transporting a portable nuclear device to explode the Crimea bridge”.



Ukrainian armour on the dockside at the port of Mariupol, Sea of Azov, eastern Ukraine, on 2 December 2018. Since Russia's annexation of Crimea in 2014, the Kremlin has deployed a range of hybrid techniques against Ukraine and the West. (Genya Savilov/AFP/Getty Images)

1734882

Globally, there has also been a notable increase in the attention paid to legislation as a dimension of hybrid warfare. As argued in the written evidence submitted to the UK parliamentary Defence Committee on 23 January 2019 by Aurel Sari, director of the Exeter Centre for International Law, “Adversaries conducting hybrid warfare and gray zone campaigns rely on law and legal arguments predominantly in order to legitimize their own behaviour and maintain their own freedom of action and to delegitimize their opponents’ behaviour and restrict their respective freedom of action”.

EU-NATO co-operation

Hybrid threats have been an area of growing EU-NATO co-operation since the July 2016 Joint Declaration identified an urgent need to “boost our ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between staffs; and cooperating on strategic communication and response”. The first action included in the common set of proposals for the implementation of the Joint Declaration encouraged NATO and EU participation, alongside allies, in the work of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

The Hybrid CoE was one of the actionable proposals made on 6 April 2016 by the High Representative of the EU for Foreign Affairs and Security Policy in the ‘Joint Framework on Countering Hybrid Threats’. At the same time, the Framework created an EU Hybrid Fusion Cell within the EU Intelligence and Situation Centre (INTCEN) of the European External Action Service (EEAS) for the analysis of hybrid threats. According to European commissioner Elżbieta Bieńkowska, writing in a statement to the European Parliament on 12 January 2018, the Hybrid Fusion Cell staff co-operate with the Hybrid CoE and the NATO Hybrid Analysis Cell.

Earlier, in June 2015, the EU had already presented an action plan on strategic communication by mandate of the European Council that included the creation of the East StratCom Task Force within the EEAS. This responded to the role played by the strategic use of communication tools “in the dramatic political, economic and security related developments that have affected the EU’s eastern neighbourhood over the past year and a half”, and more specifically Russia’s disinformation campaigns.

Jane’s visited the Hybrid CoE headquarters in Helsinki on 13 December 2018 and met some of its senior management to discuss perspectives on hybrid activities and the centre’s initiatives. The Hybrid CoE was established on 11 April 2017 in Helsinki through a memorandum of understanding signed initially by nine states, and reached initial operational capability on 1 September 2017 under the direction of Matti Saarelainen.

By December 2018, there were 20 EU or NATO member states actively participating in the Hybrid CoE and 20 people working at the Helsinki headquarters. According to the *Jane’s* interviewees, the centre’s estimated annual budget for 2019 was approximately EUR2.2 million (USD2.5 million), excluding funding for specific projects, with the core budget coming from membership fees. It is managed by a steering board responsible for policy, programming, and budgeting, and has a secretariat that manages everyday functions with its core staff and member states’ personnel secondees.

[Continued in full version...]

(867 of 2727 words)

For the full version and more content:

Jane's Military & Security Assessments Intelligence Centre

This analysis is taken from [Jane's Military & Security Assessments Intelligence Centre](#), which delivers comprehensive and reliable country risk and military capabilities information, analysis and daily insight.

*IHS country risk and military capabilities news and analysis is also available within **Jane's Intelligence Review**. To learn more and to subscribe to **Jane's Intelligence Review** online, offline or print visit: <http://magazines.ih.com/>*

For advertising solutions visit [Jane's Advertising](#)