CFSP/CSDP Inter-Parliamentary Conference 4-6 September 2019, Helsinki

Background Paper: Workshop 2

Countering Hybrid Threats: Assessing the EU's Policies and Instruments

Europe has been increasingly exposed to hybrid threats that comprise hostile actions designed to destabilize a region or a state. To counter these and other threats, and foster the security and resilience of the EU, its member states and also neighbours, the EU has aimed to build up policies and instruments in the field of security and defence, cybersecurity, energy and strategic communications.

The EU's recent focus and action in countering hybrid threats is largely related to Russian aggressive behaviour and its illegal annexation of the Crimea in 2014. Methods used by Russia sounded an alarm in many European capitals, and led to fears that similar tactics could be employed elsewhere. In addition, the wave of ISIS inspired jihadist terrorist attacks on European soil has highlighted the use of social media and other types of networks to radicalize people, as well as to direct terrorist operations. Moreover, cyber-attacks have disrupted European critical infrastructure, and information campaigns have been detected in relation to elections, for instance.

Hybrid threats refer to the notion of unconventional threats that fall under the threshold of the use of military force. While there are a number of alternative concepts such as irregular warfare, non-linear combat and grey zone conflict, the EU has agreed upon a working definition of hybrid threats. Hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives.

Hybrid campaigns are multidimensional, and designed to be hard to detect. One of their key goals is to create confusion and hinder effective decision-making and response.

Detecting and countering hybrid threats and building resilience remains predominantly the EU member states' responsibility. The EU's role is to provide support for member states and complement their actions. Given the broad and undefined nature of hybrid threats, the EU however has many assets and notable strengths as it operates across several policy domains.

The 2016 *Joint Framework on Countering Hybrid Threats – a European Response* outlines 22 actions ranging from improving information fusion and situational awareness, to protecting critical infrastructure, cybersecurity, building resilient societies and stepping up cooperation with NATO.

Importantly, the EU has also aimed to adapt to the changing security landscape. In 2018, it reinforced the focus on strategic communications and situational awareness, chemical, biological, radiological and nuclear threats, resilience and cybersecurity as well as counter intelligence.

On cybersecurity, a directive on the security of networks and information systems has been adopted and fully committed to by all member states by May 2018 and the EU Agency for Cybersecurity has been established. Cooperation and synergies between several EU organisations have been strengthened in order to develop expertise, operational and technical support under rubric of cyber defence. Sector specific preparedness has been increased in transport (including aviation), energy and financial sectors, for instance.

Importantly, in May 2019, the EU Council established a framework which allows the EU to impose targeted restrictive measures (i.e. sanctions) to deter and respond to cyberattacks which constitute an external threat to the EU or its member states.

The EU has also rapidly built capabilities to tackle disinformation from external and internal sources. The *Action Plan against Disinformation* was endorsed by the European Council in 2018 and it provides a road map to enhance cooperation between EU institutions and services, as well as with national authorities, industries and civil society. The aim is to detect, analyse and expose disinformation, and the implementation of the plan was tied to securing free and fair elections to the European Parliament in May 2019.

In a related move, the Strategic Communications Division of the European External Action Service, its three task forces and Hybrid Fusion Cell have been strengthened. In addition, a Rapid Alert System has been established to facilitate data sharing, enable common situational awareness, and forge common responses and resource efficacy.

There also seems to be an increasing awareness of the need to prepare for hybrid threats at the EU's external borders within the general EU aim of securing its borders. Hybrid threats at the border are tied to flows of migrants, goods and waste, weapons, information and crime, which could endanger the functioning of the Schengen Area. Countering hybrid threats at the border requires a readiness to detect and respond to various kind of scenarios on the part of border guards and law enforcement officials. This has constituted a part in actions to strengthen the Frontex.

Outside EU structures, yet in close cooperation with the EU and NATO the Helsinki based European Centre of Excellence for Countering Hybrid Threats has been set up. To date it has 21 members (EU members and NATO allies), and it provides support in key areas such as training and exercises. Currently the Centre is working together with the European Defence Agency (EDA) with a view to contribute to the EU capability development with a focus on harbour protection, mini drones, CBRN related threats as well as countering improvised explosive devices.

In light of these and other developments, the EU has evidently emerged as a more credible actor in countering hybrid threats and building resilience. Fully implementing past decisions as well as assessing the need for new policies and instruments is continuously needed as the security environment keeps changing.

Points of discussion:

- What are the most urgent new initiatives needed to build up capabilities to counter hybrid threats and build resilience?

- How the EU can further forge adequate and shared situational awareness enabling swift decision-making and response to hybrid operations?

Further reading:

- Daniel Fiott and Roderick Parkes (2019) *Protecting Europe: The EU's response to hybrid threats*. Chaillot Paper 151, Paris: EUISS. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf