A Europe that protects: good progress on tackling hybrid threats

The European Union and Member States have made good progress in tackling hybrid threats through a number of concerted actions in a wide range of sectors to significantly boost capacities, shows the latest report adopted today by the Commission and the European External Action Service.

The 22 measures identified under the 2016 Joint Framework on Countering Hybrid Threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats range from improving exchange of information and strengthening protection of critical infrastructure and cybersecurity, to building resilience in our societies against radicalisation and extremism. Member States have received support through the framework, and the EU's response to hybrid threats has been successfully tested, including in a parallel and coordinated way with NATO in a number of exercises.

Key findings

The report outlines detailed progress on a large number of areas, which include:

- **Strengthening strategic communications to tackle disinformation:** The Action Plan against Disinformation, endorsed by the European Council in December 2018, is a key development of the last 12 months. In March 2019, a Rapid Alert System on Disinformation was set up to enable Member States and EU institutions to facilitate sharing of data and development of common responses, enable common situational awareness, , and ensure time and resource efficiency. Ahead of the European Parliament elections, the Computer Emergency Response Team for the EU institutions (CERT-EU) launched a new Social Media Assurance service. This service allows detecting impersonation, non-official content and proceed to takedowns, on demand. The Hybrid Fusion Cell, created inside the European External Action Service (EEAS) continues to provide strategic analysis to EU decision makers.
- **Cybersecurity and cyber defence:** To deter and respond to cyber-attacks which constitute a threat to the EU and its Member States, a new sanctions regime was established on 17 May. This further expands the set of tools available to the EU Member States under the Cyber Diplomacy toolbox, a framework encompassing CFSP measures to respond to malicious behaviour in cyber space. The toolbox has been put to use on several occasions since the last progress report, most recently through the HRVP declaration on behalf of the EU on 12 April. Also, a range of projects and measures have been adopted to boost cybersecurity, including the April 2019 sector-specific guidance on cybersecurity in the energy sector that identifies the main actions to be taken by the Member States and energy operators in order to preserve cybersecurity and be prepared for possible cyber-attacks. Furthermore, several Member States are

developing and contributing to two cyber defence-related projects under Permanent Structured Cooperation.

- **Chemical, Biological, Radiological and Nuclear related risk:** the Commission, in cooperation with a number of Member States, developed a classified list of more than 20 chemical substances of concern. The Commission has also continued to engage with private actors in the supply chain to work together towards addressing evolving threats from chemicals that can be used as precursors. In October 2018, the Council established an autonomous sanctions regime against the use of chemical weapons to which in January 2019 nine persons and one entity were added. They are now subject to travel bans, assets freeze and the prohibition to make funds available to them. Member States also decided in April 2019 to support core activities of the Organisation for the Prohibition of Chemical Weapons, providing €11.6 million funding for the years 2019-2022 to fight against impunity and re-emergence of chemical weapons use, capacity building as well as upgrading of the Organisation's laboratory to a Centre of Chemistry and Technology, with increased capacity to verify chemical substances, research and contribute to capacity building.
- **Protection of critical infrastructure:** The Commission, in cooperation with Member States, has finalised the work on developing vulnerability indicators for the resilience and protection of critical infrastructure against hybrid threats. The Commission also continues close engagement with Member States and third countries on efforts to diversify energy sources, for example by progressing on the geographical supply diversification via greater engagement with the United States on Liquefied Natural Gas (LNG) imports to the EU, as well as unlocking the potential of priority projects such as the Southern Gas Corridor and the development of East Med Gas.

Conclusions

Amongst the key achievements, a large number of legislative proposals have been adopted to underpin efforts at national and EU level – the Regulation on the screening of foreign direct investments into the EU is a recent example. Chemical and cyber sanctions regimes have been added to the array of response measures. Countering disinformation, election protection, cybersecurity, defence industry cooperation add on to the list of areas concerned but, by far, do not exhaust it.

Cooperation within and between EU entities – institutions, services and agencies – has been key to steady progress on the hybrid files. Cooperation with partner countries in this field has been stepped up: Hybrid risk surveys have been launched in 7 partner countries in the EU's neighbourhood.

The same goes for cooperation with strategic international partners like the North Atlantic Treaty Organisation, including in the framework of the Hybrid Centre of Excellence in Helsinki, and with third countries in the frame of multilateral formats, notably the G7.

Close coordination between EU entities and the Member States based on a whole-of-society approach – government, civil society, private sector,

including, inter alia, media and online platforms – is at the core of the EU's counter-hybrid policies.

Background

Security has been a political priority since the beginning of the Juncker Commission's mandate – from President Juncker's Political Guidelines of July 2014 to the latest State of the Union address on 13 September 2017.

Hybrid activities by State and non-state groups continue to pose a serious and acute threat to the EU and its Member States. Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional means and tactics. They are designed to be difficult to detect or attribute to any individual or group.

For More Information

Report

Factsheet on countering hybrid threats