A EUROPE THAT PROTECTS: COUNTERING HYBRID THREATS

JUNE 2018

The EU and its Member States continue to face serious and acute threats, which are increasingly taking non-conventional forms, such as radicalisation leading to terrorist attacks, chemical attacks, cyber-attacks or disinformation campaigns. All these actions have one thing in common - they seek to destabilise and endanger our society and undermine our core European values.

HYBRID THREATS – WHAT ARE THEY?

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, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion to hinder swift and effective decision-making.

Hybrid threats can range from cyberattacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions.

Chemical, Biological, Radiological and Nuclear (CBRN) threats delivered by non-conventional means fall within a category of their own because of the potential scale of the damage they can cause. As attribution is difficult, these challenges require specific and coordinated measures to counter; for example detection of the transfer of dangerous chemicals, reducing access to them, or decontamination.

EU'S RESPONSE

Awareness, resilience and response are at the heart of EU action to counter hybrid threats. We are improving our capacity to detect and understand malicious activities at an early stage. At the same time, we are enhancing the resilience of our critical infrastructure, our societies and institutions. This is fundamental to improving our ability to withstand and recover from attacks. Countering hybrid threats requires action mainly from Member States, as well as closer cooperation between the EU, the **Member States**, partner countries and NATO.

WHAT HAS BEEN DONE?

22 action areas were identified in 2015 ranging from raising awareness to building resilience – for example:

Creation of the **EU Hybrid Fusion Cell**, to gather information and intelligence from Member States to inform decision-makers both in EU institutions and Member States.	Creation of the **European Centre of Excellence for Countering Hybrid Threats** in Helsinki to establish a research institutions that can make sound analysis, organise trainings and exercises for EU member States and NATO Allies.	Delivering a pro-active strategic communication and optimising media monitoring to counter fake news
Increasing resilience in the energy sector by diversifying energy sources and routes and promoting safety and security standards.	Taking measures to prevent disruption of transportation.	Organising EU-wide health and civil protection exercises to test preparedness.
Strengthening cybersecurity in Europe, with wide-ranging concrete measures to provide a major boost to EU cybersecurity structures and response capabilities.	Tackling online disinformation to have a safer internet, to prevent interference in elections, and to provide better information about the EU and its policies.	Cooperating with NATO as outlined in the July 2016 Warsaw Joint Declaration

WHAT ADDITIONAL EFFORTS WILL BE MADE IN THE FUTURE?

- Expanding the capacity to detect hybrid threats and scale up the measures against **disinformation campaigns:** efforts to counter and respond to hybrid threats have to be underpinned by a capacity to detect malicious activities and their sources, which can come both from within and outside the Union, at an early stage and to understand links between often seemingly unrelated events by connecting the dots.

- Building up the preparedness against **CBRN attacks**: develop a list of chemical substances posing a particular threat, as a basis for action to reduce their accessability; set up a dialogue with private actors in the supply chain to work towards restricting the availability of chemicals that can be used as precursors; make a complete overview of threat scenarios and an analysis of existing detection methods to improve the detection of chemical threats.

- Reinforce **cybersecurity measures**: the EU is aiming to build up capacity through support measures, stronger coordination and new structures to improve counter-measures and accelarate their deployment.

- Reinforce **counter-intelligence** expertise at EU level: concrete practical measure will be put in place to step up coordination among and between Member States and other international partners, such as NATO.

- Improved capacity to **detect hybrid threats**: efforts to counter and respond to hybrid threats have to be underpinned by a capacity to detect early malicious hybrid activities and sources. To this end, the EU Hybrid Fusion Cell will be expaneded with specialised chemical, biological, radiological and nuclear, counter intelligence as well as cyber analytical components.