PARLEU2017.EE

Parliamentary Dimension of the Estonian Presidency of the Council of the European Union

Interparliamentary Conference for the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP)
7–9 September 2017, Tallinn

Background information

Practical aspects of the hybrid world including the cyber sphere and strategic communication

The modern world is increasingly dependent on digital technologies which make it vulnerable to cyber threats. At the same time, hybrid means are being used to put pressure on sovereign countries. Hybrid threats have been described as *the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare*.[1]

EU has taken several steps to target hybrid and cyber threats.

EU actions to tackle cyber and hybrid threats

EU Cybersecurity Strategy, published in 2013, sets five priorities for a secure EU cyberspace, one of which is developing cyber defence policy and capabilities related to the CSDP. The EU is working towards a new cyber security strategy.

On 6 April 2016, the Commission published a Joint Communication to the European Parliament and the Council (Joint Framework on Countering Hybrid Threats). 22 actions were proposed to counter hybrid threats, enhance resilience and improve cooperation between different actors, adding to other existing policies and documents: European Agenda on Security, the then-upcoming European Union Global Strategy for foreign and security policy and European Defence Action Plan, the EU Cybersecurity Strategy, the Energy Security Strategy, the European Union Maritime Security Strategy. On 19 July 2017, the Commission published a report on the implementation of the Joint Framework on countering hybrid threats, presenting a substantial progress on the 22 actions proposed. In July 2016, the EU Playbook was adopted outlining practical arrangements for coordination, intelligence collation, analysis, and cooperation with NATO. In 2016, the EU Hybrid Fusion Cell was established within the European External Action Service to provide all-source analysis on hybrid threats.

StratCom Task Forces

In the age of post-truth, alternative facts and a surplus of information, it is of utmost importance to distinguish between accurate information and facts from those made to distract decision makers and the public. This has led to the creation of task forces against disinformation. While East StratCom Task Force is dedicated to Russia's disinformation campaigns, the Arab StratCom Task Force tackles the radicalisation of the Arab world.

[1] JOIN (2016) 18 final

NATO-EU cooperation on cyber and hybrid threats

The Joint Declaration on NATO-EU cooperation was signed by EU leaders and the Secretary General of NATO in July 2016. It was followed by 42 concrete proposals in December 2016. Both cyber security and countering hybrid threats are among the priorities of the proposals. The first Progress Report was published in June 2017 with considerable efforts reported (including in the cyber sphere), and further expansion of cooperation will possibly be considered in the next report to be submitted in December.

Other initiatives

Additionally, other initiatives have been taken by Member States and NATO:

Several research centres have been established to counter hybrid and cyber threats. For one, the European Centre of Excellence for Countering Hybrid Threats was established in April 2017. It is aimed at raising awareness of hybrid threats and the vulnerabilities of societies which can be exploited in hybrid operations, and at fostering the resilience of societies. Two other research centres, namely the NATO Strategic Communications Centre of Excellence in Latvia and the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, target similar threats regarding cyber-sphere, hybrid treats and strategic communication.

NATO Cooperative Cyber Defence Centre of Excellence led the process of drafting and publishing Tallinn Manual 2.0 (an updated version of Tallinn Manual published in 2013) in 2017 that analyses the applicability of international law to cyber operations.

Points for discussion

1. How to build resilience against cyber attacks in a world of fast changing technology?
2. Are hybrid threats anything new?
3. How to develop citizens' sense of responsibility and critical thinking regarding media consumption?