EU2022.CZ
Parliamentary Dimension

SENÁT
PARLAMENTU
ČESKÉ REPUBLIKY

POSLANECKÁ
SNĚMOVNA
PARLAMENTU
ČESKÉ REPUBLIKY

Inter-Parliamentary Conference for the Common Foreign and Security Policy and the Common Security and Defence Policy (IPC for CFSP/CSDP)

Prague, Czech Republic

Date: 4-5 September 2022

Disinformation and hybrid threats, cyber defence

Czech Presidency of the Council of the European Union

Parliamentary Dimension

Prevention and resilience as key measures

Hybrid threats, along with threats from the cyber domain, are turning into common means of modern warfare. There is a significant interdependence between these types of threats, not only in how they threaten our security, but also in how we counter and prevent them.

The European Union and its Member States are prepared for these developments. Already in 2016, the Commission presented the Joint Framework on countering hybrid threats – a European Union response that captured the changing shape of hybrid threats and the hybrid campaigns that emerge from them ["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"]; it has also presented a set of 22 measures that combined responses in four areas/axes – improving awareness, building resilience, preventing, responding to crisis and recovering.

Preparing for hybrid threats is not only about analytical work, as it also involves systemic building of internal EU resilience. The steps taken by the Union and its Member States were aimed at systemically strengthening cyber security through the necessary reform and subsequent creation of the European Union Agency for Cybersecurity (ENISA). Furthermore, the Union is progressively introducing regulation of actors in digital services (e.g. through the Digital Services Act), which has the potential to influence the behaviour of actors in the cyberspace.

The existence of a specialised agency for cyber security is based on the non-military nature; cyber security starts with preventive action aimed at the technical security of key infrastructure. In addition to technical security, there has also been an emphasis on building the soft resilience skills of society in terms of resistance to information warfare, the spread of disinformation and misleading information; furthermore, the Union is developing activities to positively disseminate verified and relevant information (strategic communication). In the area of hybrid threats, the Union is also dedicated to leveraging its position on the international stage, secured through its economic and political strength. Aware of the said position, the Union compiled a set of already existing tools, contained in the Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU and a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, which can be used to deter actors from their activities, and tools that can potentially serve as a response to ongoing cyber-attacks, including the possibility of imposing restrictive measures.[1] In addition, the Union seeks to raise awareness of cyber threats at international level and in cooperation with partners (notably EU-NATO).

The inclusion of cyberspace among the target areas of the 2022 Strategic Compass confirmed the importance of this area for the further development of the Union's defence. Building resilience is a key element of the fight against hybrid and cyber threats. As technology develops, the range of tools that can be used by state and non-state actors for hybrid campaigns is expanding as well. For this reason, both the Strategic Compass and the Council Conclusions of June this year mention the preparation and presentation of an EU Hybrid Toolbox, which should include preventive, cooperative, stability, restrictive and recovery measures. Furthermore, work is underway to develop a toolbox to address activities involving foreign information manipulation and interference in the information domain (FIMI), i.e. activities that impact on the conduct and outcome of the democratic process. The FIMI Toolbox is expected to be introduced in autumn 2022.

In its June 2022 conclusions on a Framework for a coordinated EU response to hybrid campaigns, the General Affairs Council pointed to, in the wake of the Russian invasion of Ukraine, the veracity of earlier findings that hybrid threats are gradually becoming part of the toolkit involved in contemporary warfare, while reaffirming the earlier concept of hybrid threats and campaigns as the systematic, targeted activities of external hostile

[1] https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/

actors, state and non-state, combining a variety of means and specifically targeting the systemic vulnerabilities in democratic societies.[2]

National parliaments as actors in resilience to hybrid campaigns and strengthening cyber security

The primary targets of hybrid threats are the individual Member States, their democratic establishments, critical infrastructure, and ultimately their citizens, with the transnational community being a secondary target. The responsibility for building resilience thus lies primarily with the Member States, which must coordinate their actions. Therefore, the Union has an indispensable role to play in supporting and coordinating these efforts.

The confirmation of the previous findings on hybrid threats to Member States and the Union puts increased pressure on the various actors not to take the measures presented lightly, but rather to work hard on their implementation. The European Union institutions must continue to prepare measures on the macro level, in particular to develop a framework for cooperation of its Member States. The key to cooperation between the different actors lies in sharing information and early detection of threats. By definition and experience, hybrid threats are vague and take many forms; but it is their nature to confuse – citizens and institutions alike.

Defending against a vague and unclear threat is quite difficult. Therefore, preparedness and resilience are key elements of defence. Defence against hybrid threats is a long-term mission. The speed and quality of preparation depends on the quality of the legislative framework defining said preparation. Therefore, the policy-making institutions, government and parliament, are directly linked to the building of resilience.

So far, documents on hybrid threats have highlighted the role of Member States. The current Interparliamentary Conference allows members of national parliaments to discuss ways of engaging in the development of this framework at national level and to unify their positions.

As the latest Council conclusions also underline, action on hybrid campaigns does not take place solely in the external dimension; the Union and the Member States must actively build security through legislative action, which is expected to involve the individual parliaments. The defence against hybrid threats is cross-cutting, it spreads through varying areas and hybrid threats can target different social and age groups. This legislative action should also include the preparation of European legislation, not just national legislation. However, EU legislation is also subject to parliamentary scrutiny at national level.

The national parliaments also have a unique relationship with their citizens and can thus mediate important communications related to the latest developments in initiatives and measures related to cyber and hybrid threats. An informed and educated public, particularly in the area of the dissemination of manipulative news, is essential for the defence of the democratic principles of the Member States and the Union.

[2] : Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model. Available at: https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf. p. 11.

Topics for discussion

1) How can national parliaments contribute to strengthening Member States' resilience to hybrid threats?
2) Should members of parliament get involved in communicating the risks of hybrid threats and external interference to their citizens and if so, how?
3) What tools should be included in the emerging EU Hybrid Toolbox and FIMI Toolbox?