



## Background Note

### Session III: Ensuring Continuity and Security in Times of Hybrid Threats and Parliamentary Vulnerability

Hybrid threats employ a mix of tools – from disinformation and cyberattacks to physical intimidation and interference with critical infrastructure – all aimed at creating uncertainty, eroding trust, and disrupting decision-making. As prominent symbols of democratic legitimacy, parliaments are attractive targets, and their reliance on open communications and digital systems, in addition to their need to be publicly accessible, creates vulnerabilities that hostile states and non-state actors can exploit.

#### *Protecting Parliamentary Openness and Infrastructure*

A key aspect of resilience is the safeguarding of the physical and digital infrastructure that enables parliamentary work. Cyberattacks on email systems, voting platforms and parliamentary websites can disrupt legislative processes, while physical intrusions, drone surveillance and acts of intimidation around parliamentary buildings can undermine the sense of safety and authority. An effective response requires an integrated security approach, combining digital and physical security measures, as well as contingency planning and robust crisis management procedures.

#### *Institutional Resilience and Political Preparedness*

Beyond infrastructure, institutional resilience also relies on awareness, preparedness and a robust political culture. Hybrid threats often exploit internal divisions and procedural complexities, while disinformation campaigns may influence debates, target individual members, or create polarisation. Harassing and putting pressure on parliamentarians can further inhibit democratic deliberations.

Actions to build institutional resilience include, among other things, the continuous investment in skills and training for both members and staff. At the same time, there is also a need within parliaments for a better understanding of disinformation, cyber risks and influence operations in order to ensure early and effective responses. Strong cross-party dialogue and cooperation are equally essential, as they help safeguard institutional integrity and reduce vulnerabilities by ensuring that democratic actors can present a united front against hybrid threats.

#### *Acting together in the EU*



While the primary responsibility for the countering of hybrid threats lies with the individual EU Member States, this is complemented by coordinated action within the EU. EU efforts focus on protecting critical infrastructure and democratic processes, tackling cyberattacks, foreign information manipulation and interference, and other destabilising hybrid activities. On 16 March 2026, the Council reaffirmed the EU's determination to use all available tools to prevent, deter and respond to hybrid campaigns.

Session III will focus on how parliaments can prepare for and respond to hybrid threats that may disrupt their operations, and on the measures that can strengthen institutional resilience and ensure the continued functioning of parliamentary democracy under pressure.

### **Guiding questions for the discussion:**

- How can parliaments strengthen their ability to detect and respond to hybrid threats at an early stage?
- How should parliaments balance the need for enhanced physical and digital security with the democratic principles of openness, transparency and public accessibility?
- What role can cross-party cooperation and shared political responsibility play in reducing the vulnerability of parliaments to disinformation, polarisation and other forms of hybrid interference?
- How can parliaments support and protect individual members and staff who may be targeted by harassment, pressure, or influence operations, while also ensuring that democratic debate remains free, open and robust?