



ASSEMBLEIA DA REPÚBLICA

---

THEME: Mechanisms for international and regional cooperation among Parliaments

# Building Parliamentary Cyber Resilience: Annual Cybersecurity Programme for Parliaments

*Speaker: Anabela Cabral Ferreira*

# 1. Executive Summary

Establishment and implementation of an Annual Cybersecurity Programme for International Parliaments, coordinated by the Assembleia da República of Portugal.

Parliaments have become priority targets for cyberattacks, influence operations and disinformation. ENISA, the Inter-Parliamentary Union and the Westminster Foundation for Democracy document a systematic escalation of these threats.

The programme is structured into four quarterly modules, inspired by leading international conference formats (TED, DEF CON, Black Hat) and adapted to legislative institutions.

69%

of incidents in the EU target central government

80%

of incidents in the EU are linked to hacktivism

4

quarterly modules in the annual cycle

## 2.1 The Threat Environment Facing Democratic Institutions

*Principal threat categories identified by ENISA and leading international bodies*



### Espionage by APT groups

State-sponsored cyber-espionage, with documented cases of multi-year persistence within parliamentary systems.



### Ransomware

Risk of paralysing legislative activity; among the four most prevalent threats to public administration.



### Generative AI-driven disinformation

Over 80% of phishing campaigns now use AI-generated or AI-optimised content.



### Social engineering / phishing

The primary intrusion vector at European level, present in approximately 60% of recorded attacks.



### Attacks on voting systems

Coordinated hacktivism, accounting for approximately 80% of incidents recorded in the EU.



### Digital violence against Members of Parliament

71% of parliamentarians surveyed across 85 countries have been targeted by violence, predominantly in the digital sphere.

## 2.2 The Role of the Assembleia da República de Portugal



### A unique position to lead the initiative

- The institutional legitimacy of a founding parliament of European democracy
- The established technical capability of the cybersecurity team (COSI)
- A network of inter-parliamentary relations built over many years



### A gap to be addressed

The Westminster Foundation for Democracy emphasises that parliaments are high-value targets that remain comparatively underfunded in matters of cybersecurity.

*Coordination by Portugal strengthens the country's presence and influence within the European and international cybersecurity ecosystem.*

### 3. Strategic Objectives



Strengthen the cybersecurity posture of participating parliaments through training and threat intelligence sharing.



Establish an inter-parliamentary network capable of coordinated response to transnational incidents.



Raise awareness among political decision-makers of the strategic implications of cyber threats to democracies.



Produce shared reference documentation - reports, guides and incident response plans.



Position the Assembleia da República as a centre of excellence in parliamentary cybersecurity.

# 4.1 Guiding Principles

*Three principles inspired by international best practice*



## Technical depth

With strategic relevance, in the style of DEF CON and Black Hat, adapted to legislative institutions.



## Accessibility and impact

TED-style sessions designed for political decision-makers and institutional leadership.



## Continuous relevance

Thematic webinars addressing emerging threats: generative AI, disinformation and resilience.

## 4.2 Modular Calendar

*Four quarterly modules, each dedicated to one dimension of parliamentary cybersecurity posture\**

### Q1

Jan – Mar

**Threat landscape and strategic intelligence**

TED talk · ENISA/CERT keynote · Threat intelligence webinar · Red team briefing

### Q2

Apr – Jun

**Generative AI, disinformation and influence operations**

TED talk · Keynote · Deepfakes workshop · AI regulation webinar

### Q3

Jul – Sep

**Operational resilience and incident response**

Keynote · Tabletop workshop · CERT.PT webinar · NIS2/DORA webinar

### Q4

Oct – Dec

**Annual assembly and inter-parliamentary governance**

Plenary assembly · External keynote · Panel · Agenda co-design

*\*tentative programme*

## 4.3 Session Formats



### **TED talk**

18 minutes - a thought-provoking perspective for a broad audience, including political leadership.



### **Keynote**

45 minutes - technical depth with real-case analysis, in the style of DEF CON/Black Hat.



### **Thematic webinar**

60 minutes - hybrid format with remote participation and a live question-and-answer session.



### **Practical workshop**

Half-day - tabletop exercise with mixed technical and political teams.



### **Red team briefing**

Classified - threat intelligence for decision-makers, with restricted access.



### **Annual assembly**

Full day, in person - review of the cycle and joint development of the agenda.

# 5. Deliverables by Module

*Each module culminates in the production of a practical, actionable instrument*

**Q1**

Threat report shared among participating parliaments.

**Q2**

Best-practice guide for secure parliamentary communication in the age of generative AI.

**Q3**

Incident response plan tailored to the institutional context of parliaments.

**Q4**

Public annual report and approved agenda for the following cycle.

# 6. Governance Model

*Inter-parliamentary structure organised across three complementary levels*



## POLITICAL LEVEL

### Programme Committee

Representatives of each participating parliament. Sets the annual thematic agenda and approves deliverables.



## TECHNICAL LEVEL

### Technical Working Group

Parliamentary cybersecurity teams. Produces content and coordinates liaison with CERT.PT.



## OPERATIONAL LEVEL

### Permanent Secretariat

Based at the Assembly of the Republic. Ensures institutional continuity, logistics and communication with parliaments.



**Confidentiality and information sharing:** a protocol inspired by the Traffic Light Protocol (TLP) and a memorandum of understanding (MOU) to be signed by each participating parliament.

## 7. Resource and Budget Estimate

*Cost structure to be budgeted, subject to validation by the Office of the Secretary-General*



### **Coordination and secretariat**

Allocation of internal AR team staff to programme management.

*To be determined*



### **Digital platform and communications**

Website, communication materials and webinar/streaming platform.

*To be determined*



### **Speakers and content**

Fees for external keynote speakers and production of module materials.

*To be determined*



### **In-person annual assembly (Q4)**

Travel, accommodation and hosting logistics for partner delegations.

*To be determined*



### **Contingency**

Allowance for unforeseen costs (customary reference: 10% of total).

*To be determined*

## 8. Success Indicators

**8 → 15**

participating parliaments (year 1 → year 3)

**>80%**

session attendance rate

**4**

reference documents produced per cycle

**>4.0/5.0**

post-session participant satisfaction

**100%**

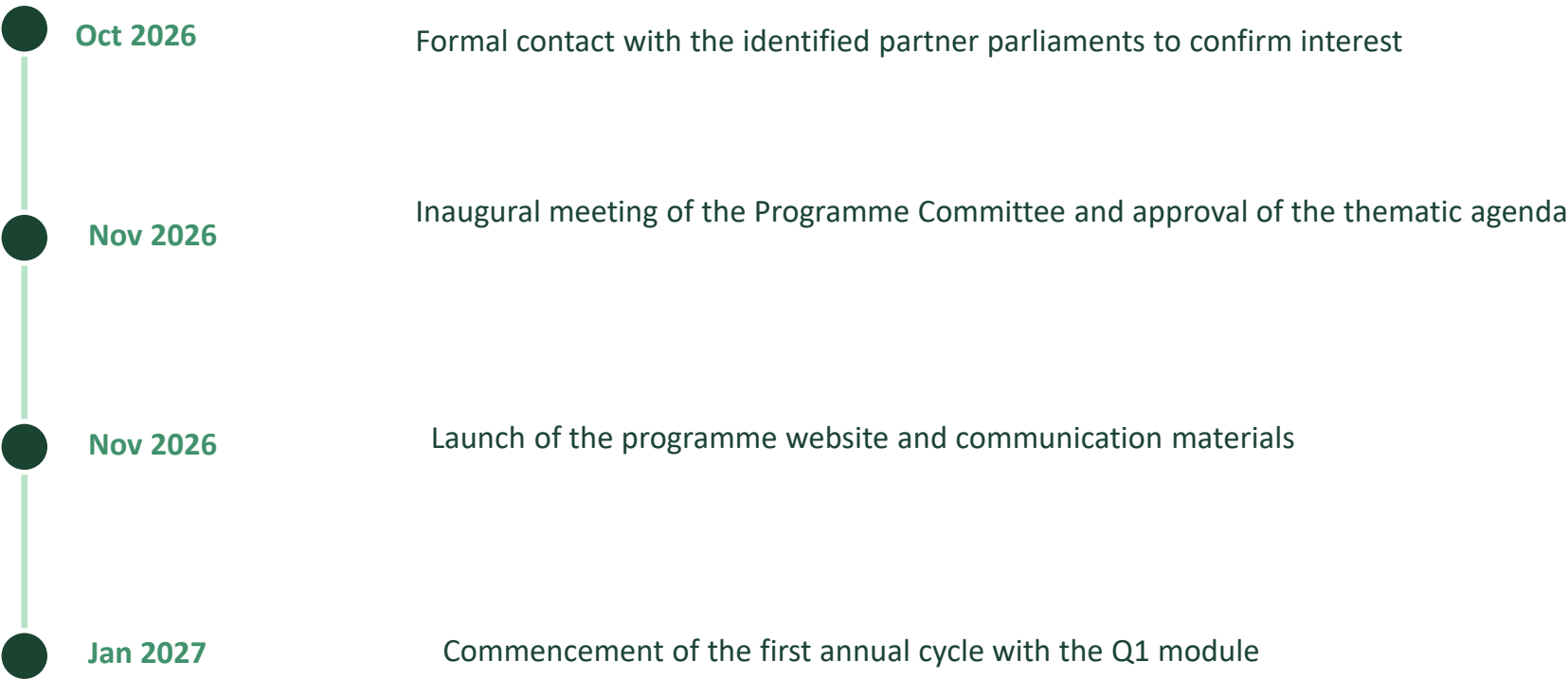
modules involving both technical and political profiles

**≥2**

tabletop simulation exercises per year

# 9. Next Steps

*Immediate action plan, subject to approval by the Board of Administration*





**THANK YOU**