ASSEMBLEIA DA REPÚBLICA

A PROPOSAL FROM THE ASSEMBLEIA DA REPÚBLICA

Building Parliamentary Cyber Resilience

Annual Cybersecurity Programme for Parliaments

An interparliamentary cooperation programme on cybersecurity.

Speaker Anabela Cabral Ferreira

Secretary-General, Assembleia da República, Portugal

Arusha, 09.10.2026

A SIMPLE OBSERVATION

Parliaments are high-value targets

We handle sensitive information

Classified documents and confidential communications.

Our activity is public

Every incident is visible and widely reported.

Reputation and trust are at stake

Any incident hits citizens' confidence in the institution.

AND THE THREAT IS GROWING

69%

of recorded incidents in the EU targeted central administration, most of them aimed at the websites of parliaments, ministries and national authorities.

ENISA, Public Administration Threat Landscape, November 2025

We believe the same holds true for countries outside the European area.

THE THREAT LANDSCAPE

Five threats to parliaments, and one beyond the systems

01

State-sponsored espionage

Malware sat undetected on a Belgian MP's laptop for almost three years (2021–2024).

02

Ransomware

Can paralyse legislative activity. One of the four most common threats to public administration.

03

AI-powered disinformation

Over 80% of phishing campaigns now use AI-generated content; voice cloning and face swapping are rising.

04

Account compromise

Targeted phishing of MPs and advisers remains the main entry point, in around 60% of attacks.

05

Voting and participation platforms

Hacktivism caused around 80% of EU incidents (July 2024–June 2025), peaking at elections.

71% of 519 parliamentarians from 85 countries report having been targeted by violence from the public, and most of those cases, between 65% and 77%, took place in the digital environment. Protecting parliaments means joining cybersecurity, information integrity and the personal safety of members.

Sources: FBI forensic report to Belgian authorities (April 2024); ENISA; Inter-Parliamentary Union survey (February 2026)

OUR COMMITMENT

The Assembleia da República is ready to coordinate this initiative.

Coordinating this programme reinforces our commitment to cybersecurity and emerging technologies, at an opportune moment.

Parliaments are high-value targets yet comparatively underfunded in cybersecurity.

Westminster Foundation for Democracy. This is the gap the programme helps to close, through cooperation between parliaments.

THE PROGRAMME

Six strategic objectives

01

Strengthen cybersecurity

An annual cycle of training, practical exercises and threat-intelligence sharing.

02

Build an interparliamentary network

Coordinated response to cross-border incidents. Threats ignore borders; so must our response.

03

Raise awareness among decision-makers

Parliamentary cybersecurity is a governance matter, not just a technical one.

04

Produce shared reference documentation

Reports, good-practice guides and incident response plans for every level of digital maturity.

05

Prepare for emerging technologies

Post-quantum cryptography and the safe use of artificial intelligence.

06

Make parliaments a reference

A bridge between different spaces of cooperation in cybersecurity.

HOW WE DELIVER

Three guiding principles

1

Technical depth with strategic relevance

Content adapted to the reality of parliaments, not generic training.

2

Accessibility for non-specialists

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

3

Permanently up to date

Webinars on emerging threats: quantum computing, digital sovereignty, operational resilience and the parliamentary threat landscape.

STRUCTURE

Four quarterly modules, one dimension each

Q1

Threats and secure communication

Threat landscape and generative AI risks.

Q2

Post-quantum readiness

Cryptographic inventory and phased migration.

Q3

Incident response

Planning and exercises for the parliamentary context.

Q4

Accountability and planning

Annual report and agenda for the next cycle.

Each module combines several session formats, pairing technical depth with political accessibility.

DELIVERABLES

Each module ends with a concrete result

Quarter	Deliverable	What it contains
Q1	Shared threat report	Plus a good-practice guide for secure parliamentary communication in the face of generative AI risks.
Q2	Post-quantum readiness guide	Cryptographic inventory template, phased migration plan aligned with the 2030 and 2035 targets, crypto-agility clauses for suppliers.
Q3	Incident response plan	Adapted to the specific reality of parliaments.
Q4	Public annual report and next agenda	Closing the year with accountability and planning, including a comparison of the cybersecurity legal regimes of each participating parliament.

All documents follow the six cybersecurity functions: Govern | Identify | Protect | Detect | Respond | Recover

Structured this way, the documents can also serve as evidence of compliance.

GOVERNANCE

Three levels, coordinated by the Assembleia da República

ADMINISTRATIVE

Programme Committee

Secretary General of each parliament. Sets the annual agenda, approves deliverables and validates the strategy.

TECHNICAL

Technical Working Group

The parliaments' cybersecurity teams. Produces content, coordinates sessions and liaises with other entities.

OPERATIONAL

Permanent Secretariat

Proposed to be based at the Assembleia da República. Continuity between cycles, event logistics and communication.

A word on confidentiality

In the first quarter the Permanent Secretariat will propose a classification and information-sharing protocol inspired by the Traffic Light Protocol (TLP), and a memorandum of understanding for each parliament to sign, with clear rules on confidentiality, retention and use of information.

RESOURCES

A programme built together, with the participation of each one of you.

The allocation for the start-up phase is still under assessment and will depend on who joins the project.

MEASURING SUCCESS

Indicators we define together, reviewed every year

Quantitative and qualitative

Defined jointly by the participating parliaments.

Reviewed annually

By the Programme Committee, at the close of each cycle.

Published in the annual report

For transparency, and to adjust the next cycles on the basis of evidence.

Threats to our democracies no longer know borders. Neither should our response.

This programme is an invitation to cooperate, and we count on you to build it. Thank you.

ASSEMBLEIA DA REPÚBLICA

Asanteni

Muito Obrigada