

ASSOCIATION DES SECRETAIRES  
GENERAUX DES PARLEMENTS



ASSOCIATION OF SECRETARIES  
GENERAL OF PARLIAMENTS

**COMMUNICATION**

by

**Anabela CABRAL FERREIRA**  
**Secretary General of the Assembleia da República (Portugal)**

On

**“Building Parlimentary Cyber Resilience: An Annual Cybersecurity  
Programme for Parliaments”**

**Arusha Session**  
**October 2026**

The fast and unpredictable development of digital technologies, together with the growing sophistication of hybrid threats, presents parliaments around the world with challenges of a new order. As institutions that handle sensitive information, conduct their work in public and depend fundamentally on the trust of citizens, parliaments are targets of considerable value to those who seek to undermine democratic processes. Any incident affecting a parliament has a significant impact not only on its functioning, but also on its reputation and on public confidence in democratic institutions. It is in this context that I would like to present a proposal which the Assembleia da República considers important for the future of our democratic institutions: an inter-parliamentary cooperation programme on cybersecurity, coordinated by the Assembleia da República.

The scale of the threat is well documented. In its report on the public administration sector, published in November 2025, ENISA, the European Union Agency for Cybersecurity, identified central government as the most targeted segment in the European Union. It accounted for 69 per cent of recorded incidents, the majority of which were directed at the websites of parliaments, ministries and national authorities.

Among the principal threats, I would particularly mention espionage conducted by advanced persistent threat (APT) groups, which are frequently state-sponsored and seek to intercept communications and classified documents. This threat is by no means theoretical. In April 2024, the FBI provided the Belgian authorities with a forensic report revealing that malware had been present on the laptop of a Member of Parliament since mid-2021, allowing remote access to the device and the undetected extraction of data for almost three years. ENISA expects such campaigns to continue, particularly on the part of groups aligned with Russia and China.

Ransomware, which is capable of paralysing legislative activity, ranks among the four most common threats to public administration, alongside denial-of-service attacks, data breaches and social engineering. Influence operations and disinformation, now amplified by generative artificial intelligence, represent a further area of concern. More than 80 per cent of phishing campaigns worldwide already use AI-generated or AI-optimised content, and there is a growing trend towards the use of voice cloning, face swapping and language models to manipulate public opinion. The Inter-Parliamentary Union has also drawn attention to very concrete risks associated with the application of AI to the legislative process, such as the manipulation of draft legislation or the introduction of bias into the information provided to Members of Parliament.

Other significant threats include the compromise of the accounts of Members of Parliament and their advisers through social engineering and targeted phishing, which remains the main entry point for attackers in Europe and features in approximately 60 per cent of attacks. Electronic voting systems and citizen participation platforms are also exposed to attack, including coordinated hacktivism. Between July 2024 and June 2025, hacktivism accounted for around 80 per cent of the incidents recorded in the European Union, with peaks during electoral periods and at other politically significant moments.

The threat is not, however, confined to information systems. A survey of 519 parliamentarians from 85 countries, published by the Inter-Parliamentary Union in February 2026, found that 71 per cent had been subjected to violence by members of the public, and that the majority of these cases, between 65 and 77 per cent, occurred in the digital environment. In my view, the conclusion is clear: protecting parliaments requires a response that brings together cybersecurity, information integrity and the personal safety of their members.

The Assembleia da República is well placed to lead such an initiative. It combines the legitimacy of a parliament with a historic role in European democracy, the technical capacity of its cybersecurity team, and a network of inter-parliamentary relations built up over many years by its services, committees and political parties. Coordinating this programme will also strengthen Portugal's presence and influence within the European and international cybersecurity ecosystem. The timing is, moreover, opportune: organisations such as the Westminster Foundation for Democracy have emphasised that parliaments, while high-value targets, remain comparatively underfunded in terms of cybersecurity. It is precisely this gap that the programme seeks to help close through cooperation among legislative institutions.

The programme has six strategic objectives. The first is to strengthen the cybersecurity of participating parliaments through an annual cycle of training, practical exercises and threat-information sharing, supporting each institution in complying with the national transposition of the NIS 2 Directive. The second is to establish an inter-parliamentary network capable of responding in a coordinated manner to cross-border incidents since, as threats do not respect borders, neither can our response. The third is to raise awareness among political decision-makers, so that parliamentary cybersecurity is regarded as a matter of governance rather than merely a technical issue. The fourth is to produce shared reference documentation, including reports, good-practice guides and incident response plans, of use to parliaments at different levels of digital maturity. The fifth is to prepare parliaments for emerging technologies, in particular post-quantum cryptography and the secure use of artificial intelligence, in line with the 2024 European Recommendation and the European transition roadmap, which sets 2030 as the deadline for critical infrastructure and 2035 for all other systems. The sixth is to position the Assembleia da República as a centre of excellence in parliamentary cybersecurity, consolidating Portugal's role as a bridge between different spheres of cooperation.

The programme rests on three principles: technical depth combined with strategic relevance, inspired by ENISA's Cyber Europe exercises and by major technical conferences, but adapted to the realities of parliaments; accessibility for non-specialists, through TEDx-style sessions designed for political decision-makers and the leadership of our institutions; and constant topicality, through webinars on emerging issues such as quantum computing, digital sovereignty, operational resilience and the threat landscape facing parliaments.

The programme is organised into four quarterly modules, each devoted to a different dimension of parliamentary cybersecurity and combining several session formats in order to balance technical depth with political accessibility. These include eighteen-minute TED talks offering a thought-provoking perspective to a broad audience, including political leadership; forty-five-minute keynote addresses providing technical depth and the analysis of real cases,

preferably European ones, in the style of the DEF CON and Black Hat conferences; thematic webinars of sixty to seventy minutes, held in a hybrid format with live questions; half-day practical workshops with simulation exercises bringing together technical and political teams; and red team briefings with restricted access, classified as TLP:RED, providing threat intelligence to decision-makers. Each cycle will close with an annual in-person, full-day assembly to take stock of the year's work, strengthen the network and jointly set the agenda for the following cycle.

Each module will conclude with a concrete outcome, as we wish training and knowledge-sharing to translate into instruments that parliaments can genuinely use. The first quarter will produce a threat report shared among parliaments, accompanied by a good-practice guide on secure parliamentary communication in the face of the risks posed by generative AI. The second will deliver a post-quantum readiness guide, including a cryptographic inventory template, a phased migration plan aligned with the 2030 and 2035 targets, and crypto-agility contractual clauses for suppliers. The third will produce an incident response plan tailored to the specific circumstances of parliaments, and the fourth a public annual report together with the approved agenda for the following cycle, closing the year with accountability and planning. All these documents will follow the six functions of the Portuguese National Cybersecurity Reference Framework (QNRCS), namely govern, identify, protect, detect, respond and recover, so that they may serve as evidence of compliance for entities covered by the Legal Framework for Cybersecurity. The annual report will also include a comparison of the cybersecurity legal regimes applicable to each participating parliament.

Coordination of the programme will rest with the Assembleia da República, through its COSI team, within a three-tier structure. At the political level, a Programme Committee comprising representatives of each parliament will set the annual agenda, approve deliverables and validate the strategy. At the technical level, a Technical Working Group composed of the parliaments' cybersecurity teams will produce content, coordinate sessions and ensure liaison with CERT.PT and other bodies. At the operational level, a Permanent Secretariat based at the Assembleia da República will ensure continuity between cycles, the logistics of events and communication with parliaments and the public. The National Cybersecurity Centre will also be invited to join the Programme Committee as a permanent observer, ensuring alignment with the QNRCS, liaison with CERT.PT and the use of training materials already made available by the national authority.

As the programme involves the sharing of sensitive information among parliaments of different sovereign States, particular attention will be paid to confidentiality. In the first quarter, the Permanent Secretariat will propose an information classification and sharing protocol inspired by the Traffic Light Protocol, which is widely used by CERT.PT and the cybersecurity community, together with a memorandum of understanding, to be signed by each parliament, setting out clear rules on the confidentiality, retention and use of information. As regards resources, the allocation for the launch phase is still under assessment and will depend on the parliaments that decide to join the project. It is, therefore, a programme to be built jointly, with the participation of each partner.

The success of the programme will be measured against quantitative and qualitative indicators, reviewed annually by the Programme Committee. We aim for at least eight participating parliaments in the first year and fifteen by the third, a session attendance rate above 80 per cent, four reference documents per cycle (one per module), participant satisfaction above four out of five, the presence of both technical experts and political decision-makers in every module, and at least two simulation exercises each year. With regard to post-quantum readiness, the objective is for the Assembleia da República, and those partners who wish to join in, to complete their cryptographic inventory by the end of the first cycle. In terms of maturity and compliance, we seek annual progress against the QNRCS and recorded training for all senior officials. All indicators will be published in the annual report in order to ensure transparency and to allow subsequent cycles to be adjusted on the basis of evidence.

Parliaments are essential to a democratic society and the rule of law, and as parliamentary administrations we share the responsibility of ensuring that Members can exercise their mandates efficiently and safely. In an era of hybrid threats, cognitive warfare and a growing tide of disinformation, the threats to our democracies no longer recognise borders, and I am convinced that our response should not recognise them either. This programme is an invitation to cooperation, and the Assembleia da República looks forward to building it together with the parliaments represented here.