Cybersecurity

for parliaments

< 2026 >

Editors
Fotios Fitsilis
Stéphane Gagnon
Franklin De Vrieze

WFD

Copyright and disclaimer

Attribution-NonCommercial-Share Alike CC BY-NC-SA

All rights in this work, including copyright, are owned by the Westminster Foundation for Democracy Limited (WFD) and are protected by applicable UK and international laws. This work is licensed under an Attribution Non-Commercial ShareAlike Creative Commons license. This license allows you to remix, adapt, and build upon this work non-commercially, provided that you credit WFD and license your new creations under the identical terms. Any permissions outside the scope of this license should be requested from WFD.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of WFD, its funders, or the UK Government. Neither WFD nor any person acting on its behalf may be held responsible for the use which may be made of the information contained therein.

The present version of the publication was finalised on April 2026.

ISBN (electronic version EN) 978-1-0676698-0-5

Cybersecurity
for parliaments

< 2026 >

WFD

Editors
Fotios Fitsilis
Stéphane Gagnon
Franklin De Vrieze

Editors

Prof. Fotios Fitsilis
Hellenic Parliament, Greece, and Universidad Austral, Argentina

Prof. Stéphane Gagnon
Université du Québec en Outaouais, Canada

Franklin De Vrieze
Westminster Foundation for Democracy, UK

Authors

Prof. Fotios Fitsilis
Hellenic Parliament, Greece, and Universidad Austral, Argentina

Prof. Stéphane Gagnon
Université du Québec en Outaouais, Canada

Franklin De Vrieze
Westminster Foundation for Democracy, UK

Vasileios Alexiou
CISO, Hellenic Parliament, Greece

Leonidas Kallipolitis
Aegis IT Research, Germany

Sean McSpaden
Oregon State Legislature, USA

Dr Vasilis Tountopoulos
Aegis IT Research, Germany

Mark Thomas,
Escoute LLC, USA

Prof. Victoria Baines
Gresham College, UK

Dr Hedi Touati
CISO, Parliament of Canada, Canada

Acknowledgements

The development of this publication has been a long and genuinely collaborative effort, driven by our shared ambition to support parliaments around the world in what is, we hope, not a solitary journey toward the parliament of the future. The authors are deeply grateful to all those whose expertise, time, and commitment have contributed to shaping and improving this work.

We would like to express our sincere thanks to the external reviewers of the publication, listed below in alphabetical order, for their critical perspectives and valuable suggestions throughout the review process: Guillaume Contat (Chief Information Security Officer, Assemblée Nationale, France), Gustavo Perri Galegale (Galegale & Associados and ISACA São Paulo Chapter, Brazil), Panagiotis Krommydakis (cybersecurity professional, Greece), Prof. George Mikros (Hamad Bin Khalifa University, Qatar), Prof. Vassilis Prevelakis (Technical University of Braunschweig, Germany), and an independent reviewer from the National Cyber Security Centre, United Kingdom.

The authors would also like to acknowledge the dedicated work of the production team for their professionalism and attention to detail in bringing this publication to fruition. We express our sincere appreciation to the Westminster Foundation for Democracy for its visionary approach in embracing and supporting this initiative, as well as its continued commitment to strengthening democratic institutions and parliamentary capacity worldwide.

Contents

Foreword 08

Executive summary 09

Introduction 10

Chapter 1: Introduction 11

Part I: Understanding parliamentary cyber vulnerabilities 14

Chapter 2: Mapping the threat landscape 15

Chapter 3: Institutional complexity and security 23

Chapter 4: Technological ecosystem vulnerabilities 27

Chapter 5: Infrastructure Security Measures 30

Part II: Developing a parliamentary cybersecurity framework 38

Chapter 6: Governance and risk management 39

Chapter 7: Digital sovereignty and cybersecurity in parliaments 53

Chapter 8: Compliance issues and regulatory landscape 56

Part III: Emerging technologies in cybersecurity 64

Chapter 9: AI and cybersecurity 65

Chapter 10: Information security 72

Chapter 11: Technological and political transition 77

Part IV: Implementation and strategic approaches 84

Chapter 12: Budgeting and resource allocation 85

Chapter 13: Creating and Cultivating a Security-Conscious Parliamentary Culture 88

Chapter 14: The creation and maintenance of cyber resilience networks 93

Part V: Cybersecurity policies and future considerations 102

Chapter 15: Toward Cybersecurity Policies for Parliament 103

Chapter 16: The Future of parliamentary cybersecurity 110

Conclusions and guidelines 120

Conclusions 121

Guidelines 133

List of Acronyms 136

Contributor bios 139

References 142

Foreword

In a rapidly evolving geopolitical and technological landscape, democratic parliaments stand as pillars of political stability, balancing the tension between democratic tradition and institutional innovation driven by emerging technologies. Yet none of these advances will matter without cybersecurity designed and applied in a meaningful way.

Cybersecurity is no longer a specialised domain for technical experts alone. It has become a horizontal institutional priority that involves every member of the parliamentary organisation and its stakeholders. As this publication demonstrates, robust cybersecurity is the essential prerequisite for integrating any advanced technology, including artificial intelligence, into parliamentary operations.

The introduction of advanced technology to parliamentary work inevitably raises concerns: Will the technical complexity, training requirements, and oversight burdens justify the benefits? Will proceedings genuinely improve? Are the security risks too great? Some fear that parliaments will become more vulnerable, not less. These legitimate concerns must be addressed early and transparently.

Westminster Foundation for Democracy stands at the forefront of supporting parliaments globally to become future-ready. Following our Guidelines for AI in Parliaments, published in 2024 and now translated into ten languages, this publication on cybersecurity forms the essential companion volume. Together, they provide parliaments with a comprehensive framework for dealing with the complexities of our multi-polar, digital world.

We, alongside our editors and authors, remain committed to driving this transformation and supporting legislative institutions as they secure their democratic mandates for the digital age.

Anthony Smith
Chief Executive,
Westminster Foundation for Democracy

Executive summary

The advancement of digital tools, particularly those based on artificial intelligence (AI), has created unprecedented risks for parliamentary institutions. From phishing and denial-of-service attacks to deep fakes and coordinated agentic swarm attacks, the digital parliamentary workspace has evolved into a highly complex and expanding threat landscape. A landscape in which cyber incidents can disrupt legislative work, undermine public trust, and even threaten national security. Unless these risks are properly confronted and mitigated, further investment in digital infrastructure and applications would make little sense, as such systems may remain uncontrollable and, worse, pose direct risks to parliamentary organisations and the institutions themselves.

This is where Cybersecurity for Parliaments: The Protection of Legislative Institutions in the Digital Age steps in. The publication constitutes a timely and authoritative exploration of one of the most underexamined frontiers of democratic resilience: the cybersecurity of parliaments.

Parliaments are unlike any other organisation. They must remain open, transparent, and accessible under all circumstances, while simultaneously safeguarding highly sensitive political, procedural, and personal data. This often happens within a highly volatile political environment characterised by privileges and immunities, separation of powers, political pluralism, and personnel turnover. These boundary conditions create a security context that cannot simply replicate off-the-shelf executive-branch or private-sector models. The publication starts from this premise and develops cybersecurity approaches explicitly tailored to parliamentary realities.

Drafted by parliamentary experts, scholars, and industry professionals, the publication is designed for parliamentary leaders, chief information security officers (CISOs), policymakers, and practitioners alike. It is structured in interlinked parts that move from diagnosis to concepts and ultimately to action. It begins by mapping the hybrid threat landscape confronting parliaments, where cyber-attacks, disinformation, espionage, and physical security risks increasingly converge. Drawing on real-world case studies, it demonstrates how parliaments have become high-value targets for both state and non-state actors.

The publication then turns to system architecture and governance, examining how institutional complexity shapes cybersecurity outcomes. It highlights the central role of diverse parliamentary actors in building digital trust. Gradually, concepts such as risk management, zero-trust architecture, compliance, and regulatory frameworks are transformed from purely technical considerations into parliamentary governance-relevant guidance. Emerging technologies are addressed not only as sources of risk but also as strategic enablers, provided they are integrated securely and responsibly.

The final sections focus on implementation, addressing, among other issues, budgeting, the cultivation of a security-conscious parliamentary culture, the strengthening of supply chain security, and the development of inter-parliamentary cooperation networks.

More than a technical manual, this publication positions cybersecurity as a democratic safeguard in a way never attempted before, yet critically necessary for sustaining the future of parliaments. Ultimately, protecting parliamentary digital infrastructure is inseparable from protecting legislative independence and democratic legitimacy.

// Introduction

Chapter 1

Introduction

Authors: Fotios Fitsilis, Stéphane Gagnon, Franklin De Vrieze

In an era where democratic institutions face unprecedented physical and digital threats, Cybersecurity for Parliaments presents the first comprehensive framework addressing the unique security challenges of legislatures worldwide. The book represents the outcome of a groundbreaking collaboration that brings together leading experts in parliamentary studies, information security, and digital governance to address a critical gap in institutional protection.

Parliaments represent distinct cybersecurity environments that cannot simply adopt solutions designed for the executive branch or private-sector organisations. The constitutional separation of powers, public-facing operations, and diverse user populations, (e.g. from elected representatives to staff, constituents, and suppliers) create complex security requirements that demand specialised approaches.

Moreover, the cybersecurity landscape extends far beyond traditional technological safeguards, encompassing an intricate web of geopolitical, organisational, and technological challenges. Modern parliaments face a multifaceted threat environment where digital vulnerabilities can translate into physical security risks, creating a complex range of potential breaches that defy standard technological solutions.

At the core of these challenges lies the unique institutional structure of parliamentary bodies. Unlike private-sector organisations, legislatures operate within a delicate balance of public accessibility, political sensitivity, and limited resources. Their digital infrastructure must simultaneously protect sensitive governance information while maintaining transparency and democratic engagement. This creates a paradoxical security requirement where openness and protection must coexist.

Technological complexity further compounds these challenges. Parliaments operate within a diverse technological ecosystem. Mixed equipment environments, varied communication channels, and the increasing sophistication of cyber threats create multiple potential vulnerability points. Hence, the risk is not merely of a technological nature but extends to how different technologies interact, potentially creating unforeseen security gaps.

Human dynamics play a critical role in this security landscape. The constant transition of elected officials, the diverse skill levels of parliamentary staff, and the complex network of external stakeholders, such as vendors, suppliers, and visitors, introduce significant human-factor risks. Transition periods, particularly after elections and after the end of a mandate of a member of the parliament, become potential moments of increased vulnerability, requiring sophisticated risk-management strategies.

Geopolitical considerations further complicate the cybersecurity challenge. Parliaments are not just technological systems but political institutions that represent national democratic processes. This means their cybersecurity is inherently political, with threat landscapes shaped by international tensions, political sensitivities, and the increasing weaponisation of digital technologies. The digital footprint of a parliamentary institution can potentially enable physical threats, blurring the lines between cybersecurity and national security.

Regulatory compliance adds another layer of complexity. With directives like the European Union's Network and Information Systems Directive (NIS2 Directive), the NIST cybersecurity framework (CSF), and emerging

guidelines around artificial intelligence (AI) and digital governance, parliaments must continuously adapt their security frameworks. This requires not just technological updates but a holistic approach to parliamentary governance that can accommodate rapid technological change while maintaining institutional integrity.

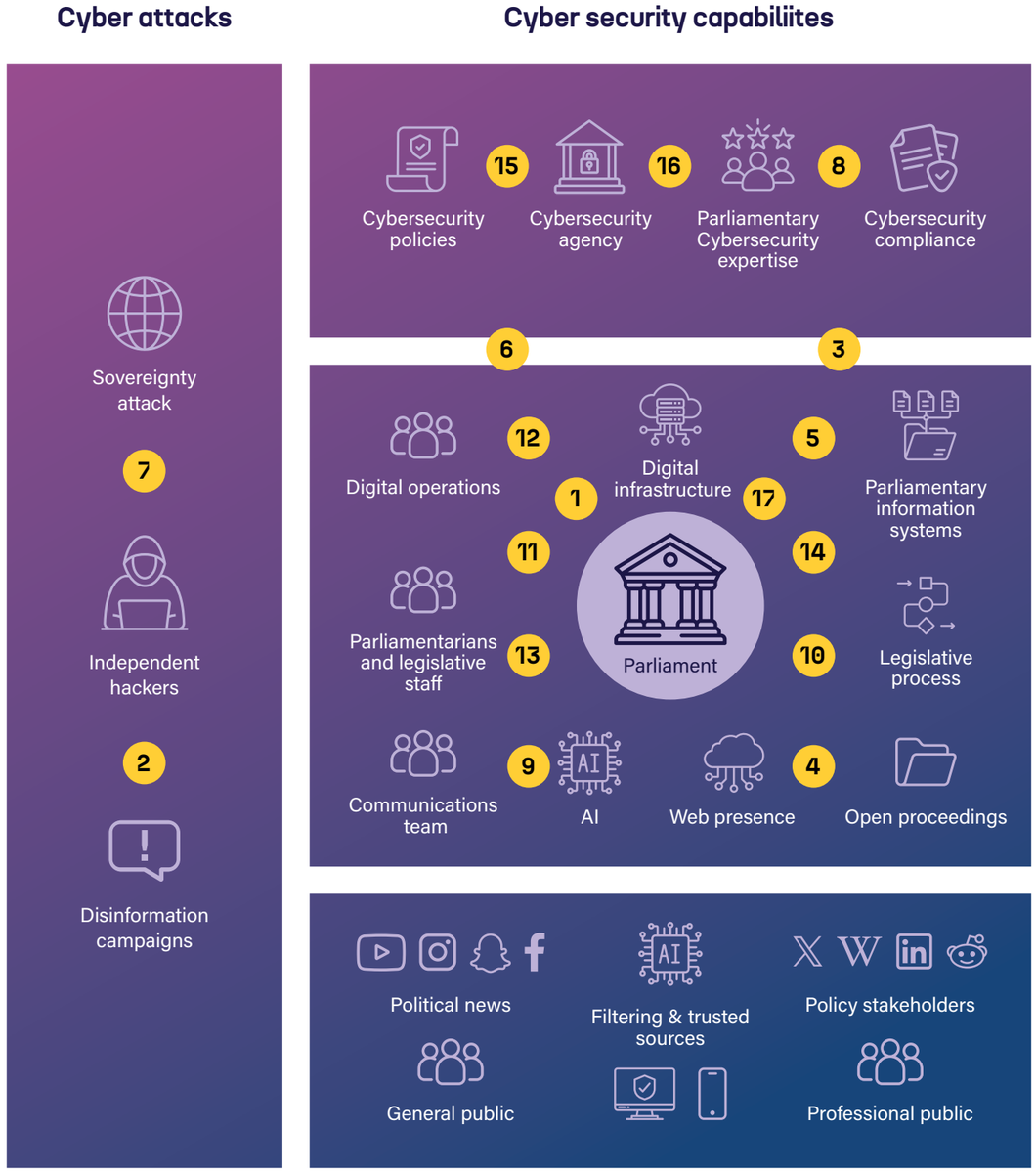
Perhaps most critically, parliamentary cybersecurity cannot be a one-size-fits-all solution. Each parliament operates within its unique political, cultural, and technological context. What works for a national parliament may be entirely inappropriate for a regional or local legislative body. This necessitates a flexible, adaptive approach to cybersecurity that can be customised while maintaining core security principles. At the same time, this means that parliaments must develop robust frameworks for information sharing, create clear governance mechanisms, and invest in continuous awareness and technological adaptation. It is not merely about protecting systems but about building digital resilience that can withstand the increasingly sophisticated and dynamic threat landscape.

This practical resource explores multiple dimensions of cybersecurity for parliaments:

- **Governance frameworks:** Establishing clear roles, responsibilities, and oversight mechanisms specifically adapted for parliamentary environments, addressing the challenges of limited resources and separation from executive-branch security infrastructure.
- **Risk assessment methodology:** Identifying parliament-specific digital assets, threat vectors, and vulnerability points, with special attention to the geopolitical aspects of parliamentary cybersecurity.
- **Secure-by-design architecture:** Implementing principles and strategies tailored to the multi-stakeholder nature of parliaments, addressing both software and hardware aspects.
- **Transition management:** Address the unique vulnerabilities during changeovers when new parliamentarians and staff enter the institution.
- **Compliance and standards:** Use of frameworks like the NIS2 Directive while establishing minimum security requirements appropriate for legislative bodies.
- **Inter-institutional collaboration:** Developing mechanisms for information sharing and collaborative defence among legislatures and other institutions facing similar threats.

The book also examines emerging challenges, including AI implementation in parliamentary operations, post-quantum cryptography requirements, and the evolving relationship between digital security and physical safety of representatives. Through case studies of actual security incidents affecting parliaments globally, practical implementation guides, and governance recommendations, this resource serves as an essential blueprint for parliamentary leadership, CISOs, IT departments, and security teams seeking to protect the digital infrastructure of representative democracy. In this context, legislatures and democratic institutions should be treated as "Critical National Infrastructure", while maintaining independence from judiciary or executive-branch cyber authority.

Throughout the different book chapters, and as displayed in Figure 1.1, the most significant cybersecurity aspects will be analysed, examined, and integrated into a set of distinct, actionable policies. These policies will be consolidated into a dedicated chapter, providing parliamentary actors with a clear, concise, and accessible synthesis of the key insights derived from the in-depth exploration of cybersecurity in the parliamentary workspace.



1. **Why parliaments must prioritize cybersecurity**
2. **Mapping the threat landscape**
3. **Institutional complexity and security**
4. **Technological ecosystem vulnerabilities**
5. **Infrastructure security measures**
6. **Governance and risk management**
7. **Digital sovereignty of parliaments**
8. **Compliance issues and regulatory landscape**
9. **AI and cybersecurity**
10. **Information security**
11. **Technological and political transition**
12. **Budgeting and resource allocation**
13. **Security-conscious parliamentary culture**
14. **Cyber resilience networks**
15. **Cybersecurity Policies for Parliament**
16. **Future of parliamentary cybersecurity**
17. **Cybersecurity Guidelines for Parliaments**

Figure 1.1: Book chapters and cybersecurity concerns in parliaments (source: Stéphane Gagnon)

< part I >

...

// Understanding parliamentary cyber vulnerabilities

Chapter 2

Mapping the threat landscape

Author: Victoria Baines

Introduction

The threat landscape for parliaments has changed considerably in the last three decades and continues to evolve rapidly. Established security concerns related to physical unauthorised access, disruption, foreign influence, and terrorism have been joined by their digital counterparts. This chapter provides a brief outline of the current cyber threat landscape: tactics, techniques, and procedures, the motivations and objectives of bad actors, and where they focus their activities. Security threats to parliaments and parliamentarians are now very often hybrid. Targets' digital communications and footprints may be accessed in order to compromise their physical security or to gather intelligence that may be exploited for offline influence. Recent high-profile prosecutions of individuals alleged to have been engaged in espionage on behalf of China highlight the value of sensitive data to some nation states, and the importance of protecting parliamentary networks and information systems, and the people who use them[1].

Hybrid threats

In the wider geopolitical context, hybrid threats may have more destructive aims. Cyber offence and defence are now key components of a country's national security capability, with cyberspace now recognised as an operational domain alongside land, sea, air, and space. As seen in the 2022 invasion of Ukraine, simultaneous attacks on communications infrastructure and public organisations very often complement more traditional kinetic attacks[2]. Cyber-attacks on nations supportive of Ukraine, including members of NATO, have been condemned in a statement by multiple national intelligence agencies and attributed to a team within the Russian General Staff Main Intelligence Directorate (GRU) Unit 29155 – the same unit believed to be responsible for poisoning a former Russian double agent and his daughter in the UK in 2018[3]. Attempts at digital compromise and disruption are equally likely during election periods, and in response to political decisions that some groups in society find unpalatable.

CASE STUDY

Estonia, 2007

In April and May 2007, a network of nearly a million compromised computers (botnet) conducted a distributed denial-of-service (DDoS) attack, flooding Estonian servers with traffic, and overloading the websites of the prime minister, the parliament, and several government ministries. Leading private-sector entities including media outlets, banks, and telecommunications providers were also targeted. The attacks followed the relocation of a Soviet war memorial in Tallinn. As a result, it has been suggested that these attacks were sponsored by or otherwise affiliated to the government of the Russian Federation. The Estonian government has never formally identified Russian authorities as suspects. For its part, the Russian government has always denied its involvement in the attacks[4].

Disrupting the business of, interrupting access to, and undermining trust in democratic institutions by digital means is now a common feature of the playbook of some nation states or their affiliates. Not unlike their physical counterparts, common cyber threats to

parliaments and parliamentarians typically have the following objectives:

- **Unauthorised access** to networks and systems. This may be for the purposes of data theft, intelligence gathering, or extortion.
- **Interference** by means of data manipulation. An example of this is tampering with a voting system in order to alter the results of a parliamentary debate or election[5]. As the use of generative AI tools has become more widespread, bad actors have also begun to exploit opportunities to skew their results by manipulating the data on which Large Language Models are trained. In one recent case, a pro-Kremlin group was discovered doing just that in an attempt to re-write the global narrative on the Russian invasion of Ukraine[6].
- **Disruption** of parliamentary activity, be this through defacing a website or rendering it inaccessible, hijacking social media accounts, or disabling systems. Disruption of parliaments and parliamentarians can occur even when their networks and systems are not the primary target – for example, in indiscriminate attacks on third-party software.
- **Influencing operations**, for example by undermining public trust in democratic institutions on social media and through high-profile data breaches, exploitation of privileged information gained through unauthorised access, and the distribution of disinformation on social media.

Security threats

Cyber-attacks on parliaments and parliamentarians exhibit similarities to other security threats in as much as they exploit vulnerabilities in people, processes, and technology. The last of these will be explored in detail elsewhere in this book (see Chapter 4). For now, it is worth noting that at least one case study in the present chapter, the 2021 compromise of the Norwegian Parliament (Storting), refers specifically to the exploitation of a previously unknown technical vulnerability. The most prevalent technical threats currently include:

- **Ransomware:** malicious software which encrypts files, rendering them inaccessible. Payment of a ransom is demanded for their decryption. Although variants of ransomware have been in the wild for over a decade, its increasing deployment against critical services, such as education, healthcare, and manufacturing, and much larger ransom demands in recent years mean that it is now a national security priority for many states.
- **Infostealers:** malicious software designed to harvest data such as login credentials, application tokens, and session cookies from infected devices. These can then be used to access any relevant services used by the victim. Infostealer malware is commonly delivered by phishing (social engineering). Threat actors may use both ransomware and infostealers in the combined attack of "double extortion". As the name suggests, this involves stealing sensitive data as well as encrypting files, and demanding payment both for decryption and non-publication of the data. Stolen personal data may also be subject to non-consensual publication, known as doxxing.
- **Denial of service:** these attacks direct a large amount of traffic to an organisation's servers in order to overwhelm them and render them inoperable. A DDoS attack makes use of a large number of disparate computers to do this, with or without the owners' consent.
- **Botnets:** these are networks of infected "zombie" computers, whose processing power is hijacked to conduct attacks on other networks and systems, including by means of DDoS (see above).
- **Trojans:** these are pieces of malicious software that masquerade as legitimate software, and can often lie dormant on a system or network until activated remotely (kill switch) or by an insider (whether complicit or by mistake).

CASE STUDY

Norway, 2020 and 2021

In August 2020, the Norwegian Parliament (Storting) disclosed that its email systems had been hacked. In October, the Minister of Foreign Affairs attributed the attack to Russia, based on the information available to the government. In March 2021, the Storting reported that it had been the victim of a further cyber-attack, which exploited a previously unknown ("zero-day") vulnerability in Microsoft Exchange products. In this case, the Storting was not the sole target. Organisations all around the world were affected, and the vulnerability is believed to have been exploited by several criminal groups.

Human vulnerabilities

In terms of human vulnerabilities, social engineering remains one of the dominant vectors for cyber-attacks. Phishing emails purporting to be from a legitimate source continue to be successful in causing victims to click on malicious links, thereby downloading malicious software (malware). This is reported to have been the delivery mechanism for the 2015 attack against the German Bundestag. Crucially, this tactic is only successful if the recipient of the communication takes the action requested – for example, clicking on a web link or opening an attachment.

CASE STUDY

Germany, 2015

In early 2015, hackers gained access to the sensitive data, emails, and meetings of members of the German Federal Parliament (Bundestag), compromised a computer in the parliamentary office of the Chancellor, and stole an estimated total of over 16 gigabytes of data. They did so by means of social engineering, sending an email that pretended to be a UN News Bulletin but in fact contained malware. This malware spread and infected the Bundestag's networks. The unauthorised access was not detected until May 2015. German authorities and the UK's National Cyber Security Centre have attributed this attack to the Russian group APT28 (APT standing for "advanced persistent threat" in cybersecurity parlance), which is believed to be affiliated to GRU, the Russian Government's military intelligence service.

Improving user awareness of the need to verify the source of communications is therefore essential to preventing cyber-attacks. This is especially pressing in light of the fact that the techniques used by adversaries to select targets and impersonate legitimate requests are constantly evolving in line with technological developments. While text-based phishing attempts are still prevalent, increasingly AI is used to generate fake audio and video designed to deceive employees into taking actions such as granting access to systems and networks, or making a payment. In the case of public figures such as parliamentarians and officeholders, it is particularly easy to obtain the audio and video samples on which generative AI can base plausible fabricated content. AI has also simplified the process of criminal research on potential victims of both cyber and physical attacks, enabling the more efficient collection of information on parliamentarians and their activities from a range of open sources, including social media.

In recent years, parliaments and parliamentarians around the world have embraced opportunities to engage with their constituents and the wider public via a host of online platforms, including social media, messaging apps, and live video. As politicians and institutions have become more accessible by digital means, their digital footprints have increased accordingly. Each new app or format that becomes popular adds an additional layer of complexity. Managing multiple social media accounts, and by extension the security for these, is often a shared endeavour. Parliamentarians may choose to post content themselves but also allow their staff to do so. Login credentials are often shared, and this practice is exploited by malicious actors.

This renders administrative staff and advisers targets in their own right, based on the reasonable assumption that they have access not only to privileged information but also to the accounts themselves. It was reportedly by this means that attackers gained access to several email inboxes of UK parliamentarians in 2017 (see case study).

CASE STUDY

United Kingdom, 2017

In June 2017, 26 users of the parliamentary network had their accounts compromised, including: six MPs, ten members of MP staff, one member of the House of Lords, one member of their staff, and five administrative staff (comprising employed staff and contractors). In this case, the hackers gained access by means of a "brute force" attack, discovering or guessing account passwords. The parliamentary spokesperson said at the time that those affected had had weak passwords, which did not adhere to official parliamentary guidance. Parliament's public update on the case reported that "[t]hree of the six MPs had accounts compromised because their mailboxes were linked to their members of staff whose passwords were compromised". According to an unpublished assessment by British intelligence, Iran was identified as the likely source for this attack[7].

Moreover, an operational need for multiple persons to access and update the same account can lead to important security measures not being activated. This is particularly the case for multi-factor authentication, which typically requires an additional means of biometric (facial recognition) or device-based (security code) verification. Management of a presence on social media is therefore often conceived as a trade-off between security and practicality/convenience. In addition, failure to withdraw access in a timely manner when offboarding a legitimate user can result in an exploitation of credentials by those who are no longer entitled to use them, particularly in cases where that individual may be motivated by resentment.

CASE STUDY

United States, 2020

In July 2020, a number of high-profile Twitter (now X) accounts were hijacked to promote a cryptocurrency scam. The accounts were used to influence victims by enhancing the credibility of the scam. The hackers derived USD 121,000 from over 400 payments to three bitcoin addresses. Among the Twitter accounts compromised were those for Elon Musk, Bill Gates, and President Joe Biden. This modus operandi continues to be observed, with a UK Government minister's X account compromised in April 2025 for the same purpose. Ensuring the security of a parliamentarian's or parliament's social media account can be complicated by the operational need for legitimate access by more than one team member.

These gaps in process are frequently exploited by threat actors in order to gain unauthorised access to accounts, networks, and systems. So-called "brute force" attacks also exploit process vulnerabilities. The former describes a method by which passwords for services may be guessed based on information openly available, defaults for specific products such as "smart" devices, or commonly used weak passwords ("123456", "qwerty", "admin", and "password" among them). A related attack vector is "credential stuffing", in which usernames and passwords that have already been leaked are assumed to have been used by the victim for more than one service. These particular tactics profit from the fact that people tend to choose passwords that they can easily remember, and reuse them for different online services (mail, online shopping, etc.).

CASE STUDY

Doxxing, 2018

In December 2018, the personal data of hundreds of German politicians, including the email address and several letters to and from Chancellor Angela Merkel, was published on Twitter in the format of an advent calendar. The account had more than 17,000 followers. The Federal Interior Minister at the time said that the data appeared to have been obtained through "wrongful use of log-in information for cloud services, email accounts or social networks" [8]. Officials later reported that the culprit had also taken advantage of weak passwords, among them "Iloveyou" and "1234". In May 2020, a 22-year-old German man was charged with unauthorised access and attempted blackmail. His stated motivation for the offences was that he was "annoyed" by some of the victims' public statements.

National security considerations and geopolitics can also have a direct impact on the perceived safety of certain apps for parliamentarians, government officials, and institutions. In March 2023, Chinese-owned video-sharing app TikTok was removed from all US Government-issued phones and European Parliament staff devices, and access blocked from both UK Government devices and UK Parliament Wi-Fi.[9] Officials have cited national security concerns, noting that Chinese cybersecurity legislation empowers government authorities to access the data of any user of a platform based in the country. Although parliamentarians around the world had been actively engaging with their publics on the app, mixed messages from the company and its Chinese parent, ByteDance, about whether employees and authorities in China do in fact access the data of users from other countries have been taken as indicating that there is a real threat of compromise to democratic governments, including to parliamentarians[10].

The approach of both the Biden and Trump administrations has been to push for the sale of TikTok's US operations. At the time of writing (October 2025), a framework agreement for their "qualified divestiture" has been concluded, by which the US version of the app would be operated by a joint venture based in the United States and would be majority-owned and controlled by "US persons"[11]. It remains to be seen how this will impact users based elsewhere. It is also worth noting that for some countries, Russia and China among them, US tech dominance is conceived as posing a similar threat. In 2024, Beijing ordered Apple to remove Meta-owned apps WhatsApp and Threads, along with Telegram and Signal, from its app store[12]. These products have joined an ever-increasing list of banned US-based apps and products, including all Google (Alphabet) services.

Threat attribution

It can take time to establish who is responsible for a cyber-attack. Bad actors inevitably deploy operational security and technical measures to mask their identities and locations, and whatever their motivation they commonly exploit the same vulnerabilities and use similar attack vectors. Broadly speaking, attackers fall into the following categories:

- **State (and state-affiliated) actors:** as a number of the case studies in this chapter illustrate, cyber-attacks on parliaments and parliamentarians are frequently attributed to employees of foreign governments. Depending on the country and the objective, government authorities active in cyber offensive operations and cybercrimes can include military units and intelligence services.
- **Financially motivated cybercrime groups:** criminals who engage in cyber-attacks for profit can be united by a common language, may swarm to perform a specific operation, or may advertise their services to others in underground forums. The business model dictates that they rarely operate entirely alone. Until now at least, writing malicious code, designing and delivering phishing campaigns, and cashing out and laundering proceeds have required different skillsets and resources.
- **Hacktivists:** these individuals, identified by a new word created from a mix of "hacker" and "activists", are largely motivated by ideology, whether this relates to commitment to a single issue such as climate change or a political affiliation. Hacktivism first came to wider global notice in the early 2010s through the activities of the loosely coordinated "Anonymous" group, whose sympathies were somewhat similar to the offline Occupy movement. More recently, people around the world have volunteered their services and their processing power to the IT Army of Ukraine. At one point in 2022, up to a quarter of a million users were following a Telegram channel which issued instructions for targeting Russian IT infrastructure[13].
- **Mischief-makers:** this final category serves as a reminder that attempting to gain unauthorised access to or control of an information system simply to demonstrate that it is possible remains a key motivator in hacking culture. Hackers may still conduct cyber-attacks ostensibly for "the lulz" – for amusement. Their impact can of course be no less disruptive and damaging.

The distinctions between the above groups are not always as clear as they might at first appear. Some government authorities are known to hire profit-driven criminal groups to conduct "state sponsored" attacks. By distancing themselves from direct responsibility in this way, states can exercise plausible deniability, which in turn frustrate attempts of sovereign nations to hold them accountable for undue interference in accordance with Article 2 of the UN Charter. States can also be directly involved in deriving profit from cybercrime. Government operatives are believed to have been responsible for the WannaCry ransomware attack in 2017, which affected around 200,000 computers in over 150 countries, and disrupted the operations of hundreds of organisations, including the UK National Health Service[14]. Hacktivists and states often share the same belief systems and the same disruptive, destabilising motives. Equally, there is often overlap in demographics. Teenagers whom one might assume to be more likely to hack solely for amusement can also engage in attempted extortion via ransomware[15]. In one striking example of what appears to have been state-sponsored influence operations, youths in North Macedonia were paid to share disinformation on social media in the run-up to the 2016 US presidential elections[16].

Given the multifaceted nature of cyber threats – their varying motivations, personnel, and attack vectors, and speed of delivery and impact – it is widely accepted that strengthening defences is paramount, and that this can best be achieved by reducing vulnerabilities in people, processes, and the technologies used. Subsequent sections of this book (Parts II to IV) explore in greater detail how each of these can be effectively addressed. As discussion above of the emerging misuse of AI illustrates, the cyber threat landscape is constantly changing in response to geopolitical and technological developments. In Chapter 16, we will consider what these will mean for the future of parliamentary cybersecurity.

Conclusion

The cyber threat landscape facing parliaments today is broader, faster-moving, and more interconnected than at any time in the past. As this chapter has shown, modern threats rarely fall neatly into isolated categories: they merge digital and physical vectors, exploit political tensions, and capitalise on rapid technological change. From state-sponsored espionage and influence operations to financially motivated cybercrime, hacktivism, and opportunistic mischief, the spectrum of adversaries is diverse – yet their methods often converge on the same weaknesses in people, processes, and technology.

Case studies from Estonia, Norway, Germany, the United Kingdom, the United States, and beyond demonstrate both the global reach of these threats and their recurring patterns: social engineering, exploitation of unpatched vulnerabilities, weak credential management, and the manipulation of widely used platforms. The rise of AI-enabled deception – including deepfakes, automated phishing, and targeted reconnaissance – adds another layer of complexity, particularly for public figures whose voices, images, and personal information are readily accessible online.

For parliaments and parliamentarians, the implications are clear. As digital engagement, online presence, and reliance on networked systems grow, so too does the attack surface. Effective defence now requires not only robust technical safeguards but also continuous investment in user awareness, clear and enforceable security processes, and the capacity to adapt as threat actors innovate. Cybersecurity is no longer a peripheral concern but a prerequisite for the functioning, legitimacy, and resilience of democratic institutions.

Strengthening protections across people, processes, and technology – the core pillars explored throughout this book – remains the most effective strategy for reducing risk. As the cyber domain continues to evolve in step with geopolitical developments and emerging technologies, parliaments must anticipate change, cultivate agility, and embed cybersecurity into every aspect of their work. The chapters that follow will examine these requirements in detail, providing guidance for building stronger, more secure democratic institutions that are capable of withstanding the threats of today and those still to come.

Chapter 3

Institutional complexity and security

Author: Hedi Touati

Introduction

Parliaments occupy a unique place in democratic societies: they are at once political arenas, public institutions, and guardians of democratic legitimacy. Their mission depends on openness, transparency, and continuous engagement with citizens, where digital technologies create unprecedented opportunities for greater reach and efficiency[17]. Yet, this very openness creates structural vulnerabilities in an era where digital operations underpin nearly every parliamentary function. The rise of cyber threats, foreign interference, online disinformation, and digital espionage has elevated cybersecurity from a technical concern to a foundational element of institutional integrity.

In this context, the complexity of parliamentary ecosystems – diverse actors, overlapping authorities, and competing priorities – shapes not only governance but also cybersecurity posture. Modern parliaments must now perform a delicate balance: protecting sensitive information without undermining constitutional privileges, enabling technological innovation while minimising risk, and fostering digital trust and privacy among citizens who increasingly interact with their representatives online[18]. Understanding how institutional complexity influences cybersecurity is therefore essential for building resilient legislative institutions capable of functioning securely in a rapidly evolving digital landscape.

Institutional complexity in parliaments and its impact on cybersecurity posture

Parliaments are among the most complex institutional environments in modern democratic systems. They are not designed as hierarchical organisations with clear command lines, nor do they resemble private-sector entities where authority can be centralised and enforced. Instead, parliaments are intricate ecosystems where political, administrative, and technical domains intersect, not always harmoniously. This complexity has always influenced the way these institutions function, but in the digital era, it exerts a profound impact on one of their most delicate responsibilities: cybersecurity.

Today, as democratic institutions rely more heavily on digital tools to conduct debates, publish information, and engage with citizens, cybersecurity becomes inseparable from digital trust[19]. Citizens encounter parliaments increasingly through screens: they watch live debates, submit electronic petitions, browse legislative documents, write to their representatives, and follow parliamentary proceedings online. These interactions only work if they trust the systems behind them; trust that information is authentic, communication is confidential, and access is reliable. A single cyber incident, whether a data leak, intrusion, or disinformation campaign, can shake not only the institution's operations but also its reputation and ultimately its democratic legitimacy.

This trust is fragile because parliamentary life is inherently open, decentralised, and highly sensitive to political dynamics. Unlike ministries or government agencies, parliaments must balance institutional autonomy with transparency, and the need to protect information with the constitutional requirement to remain accessible. This mindset of openness, embedded deeply in parliamentary

culture, introduces cybersecurity risks that other public institutions do not face to the same extent.

Leadership roles in parliaments and cybersecurity governance

One of the defining features of parliaments is the fragmentation of authority. Power is distributed between elected leaders, administrative officials, political groups, and independent offices. No single actor owns cybersecurity in a holistic sense. The Speaker or President may have overall responsibility for the institution but typically lacks operational authority. Administrative leaders can shape policy and implement programmes, yet they cannot enforce decisions on Members of Parliament, whose constitutional privileges limit the imposition of security controls. Political parties rely on parliamentary infrastructure but run their own digital environments with varying levels of maturity. In bicameral systems, this fragmentation is multiplied across chambers with distinct governance cultures.

This diffusion of authority makes cybersecurity governance a matter of consensus building rather than directive action. Implementing even simple measures – such as tightening access controls or mandating multi-factor authentication – often requires extensive negotiation. During incidents, determining who can authorise a response or communicate publicly may itself cause delays. Cybersecurity, therefore, becomes less a technical challenge and more an exercise in institutional diplomacy.

Within this landscape, the roles and behaviours of different parliamentary actors introduce additional layers of complexity. Parliamentary leadership often acts as guardian of institutional autonomy and political neutrality. Its decisions on cybersecurity must weigh not only technical advice but also political implications and the perception of fairness among all parties.

Political groups and parties, meanwhile, represent both essential democratic actors and significant cybersecurity variables. Though they operate inside parliament, they remain autonomous organisations with their own IT practices. A weakness in one political group's infrastructure can become a gateway to compromising parliamentary networks, yet parliaments typically have limited authority to impose standards on them. Cybersecurity becomes a shared responsibility with uneven levels of readiness.

MPs themselves embody one of the most delicate aspects of this system. As independent elected officials, they require flexibility in communication, device use, and interactions with constituents. However, their individual digital habits – opening email attachments, using personal devices, installing applications – can introduce risk to the entire institution. Due to parliamentary privilege, MPs operate with constitutional protections, and enforcement of cybersecurity measures relies more on persuasion and trust than compulsory controls. This soft governance model requires continuous awareness efforts and a cultural shift toward cybersecurity as part of parliamentary responsibility.

On the administrative side, parliamentary officials act as institutional stewards, bridging political leadership and technical teams. Their ability to translate security risks into governance language is central to securing resources, driving policy adoption, and coordinating incident response. They often serve as the connective tissue in an institution where authority is fractured and responsibilities overlap.

Administrative and support staff also play a pivotal role. As the operational backbone of parliamentary work, they manage sensitive documents, process large volumes of communications, and interact with external actors daily. Their level of exposure to phishing, social engineering, and human error is significant. Training programmes, user-awareness initiatives, and continuous reinforcement are essential to maintain institutional resilience.

Information and communications technology departments and cybersecurity teams, on the other hand, carry the burden of defending a system they do not fully control. They operate under political constraints, structural limitations, and cultural sensitivities that often slow down the adoption of modern cybersecurity practices. Their expertise is crucial, but their authority is often limited. Success depends heavily on established trust with leadership and the ability to communicate risk in ways that resonate with non-technical actors, to convince and obtain various governance decisions or allocated budget.

Complicating matters further, parliaments rely extensively on external partners, namely cloud service providers, technology vendors, civil society groups, and national cybersecurity agencies. These partnerships extend capability but also introduce dependencies, supply chain risks, and questions about data sovereignty and institutional autonomy. Managing these relationships requires clear contracts, governance frameworks, and a deep understanding of the broader cybersecurity ecosystem.

Whole-of-parliament cybersecurity strategy

Taken together, this mosaic of actors produces a cybersecurity posture that is at once resilient – thanks to the diversity of perspectives and layers of oversight – and fragile, due to the lack of unified authority and coherence. Governance ambiguity can hinder rapid response. Divergent risk appetites lead to inconsistent application of controls. The absence of standardised security practices across political and administrative domains creates vulnerabilities. Moreover, institutional culture, more than any technical considerations, ultimately determines whether cybersecurity is perceived as a shared responsibility or an administrative inconvenience impacting their own freedom[20].

To strengthen digital resilience, parliaments must embrace a whole-of-parliament approach, one that acknowledges institutional complexity not as a barrier but as a defining operational reality. This means developing governance models that respect political autonomy while establishing clear lines of accountability. It requires formal mechanisms for cross-actor coordination, such as cybersecurity steering committees or inter-party working groups, capable of making decisions quickly and with legitimacy. It calls for specialised training programmes tailored to MPs, political staff, and administrative personnel, recognising the unique pressures and behaviours of each group. It also demands strong, transparent partnerships with national cybersecurity bodies that respect parliamentary independence. International cooperation among parliaments can also help enhance digital governance capabilities and transfer best practices[21].

At its core, cybersecurity in the parliamentary world is not a technical task. It is a safeguard of democratic integrity. Protecting digital systems, securing communications, and preserving public trust are now essential components of parliamentary sovereignty. As legislative institutions continue to evolve in a digital-first era, their ability to ensure transparency and security will determine not only how resilient they are but also how much credibility and trust they inspire among the public.

Conclusion

Parliaments face cybersecurity challenges that differ fundamentally from those of other public institutions. Their fragmented authority, culture of openness, and reliance on numerous politically autonomous actors produce an environment where traditional top-down security models are neither feasible nor desirable. Yet this complexity also offers unique strengths: diversity of perspectives, resilience through distributed responsibilities, and strong constitutional foundations that protect institutional independence.

Strengthening cybersecurity in such an environment requires acknowledging these realities rather than attempting to bypass them. A whole-of-parliament approach – one that unites leadership, parliamentarians, political groups, administrative officials, technical teams, and external partners – is essential for building a coherent and trusted security posture. Clear governance mechanisms, targeted awareness programmes, modernised technical capabilities, and strategic collaboration with national cybersecurity bodies and peer organisations form the backbone of this effort.

Ultimately, cybersecurity in the parliamentary context is not simply about protecting networks or systems. It is about safeguarding democratic processes, preserving citizens' trust, and ensuring that legislative institutions can continue to operate transparently and independently in an increasingly hostile digital landscape. As parliaments continue their digital transformation, embracing cybersecurity as a shared responsibility will be key to reinforcing both resilience and democratic legitimacy.

Chapter 4

Technological ecosystem vulnerabilities

Author: Stéphane Gagnon

Introduction

Among public sector institutions, parliaments are often viewed as more conservative IT owners, where the core business evolves slowly and requires stable infrastructure. Their technological ecosystem involves more traditional service-oriented concerns, such as end-user support, web presence, and country-wide distributed office and telecom networks. Compared to other public agencies, they present different kinds of cybersecurity vulnerabilities and complexity, due to such factors as heterogeneity of users and devices, fragmented governance, openness, and high turnover, contrasting with central government ministries where high-throughput transactional systems make the bulk of IT budgets.

Nevertheless, the distinctive openness of parliaments, and the calendar-based turnover of members and their staff, brings its own challenges. We review here a few of the concerns that CISOs must keep on radar. We open with infrastructure-focused issues, such as equipment, legacy systems, and evolution toward cloud application environments. We then address applications and information security, particularly those emerging due to incremental process and systems integration, and similar issues are raised with the modernisation of web presence, communications channels, and necessity of more systematic content management across platforms. The chapter concludes with a proposal for more systematic mapping of parliamentary ecosystems in the age of agentic AI in process integration and customisation of citizen-facing applications.

End-user computing

As parliamentarians are rarely IT experts, it is commonplace to find end-user requirements to be highly reasonable and stable. In addition, equality of treatment among all political parties requires that highly standardised requirements must be followed. Hence a highly heterogenous equipment environment tends to last for several years, as end-users are required to follow acquisition policies without prejudice. This entails that cybersecurity vulnerabilities are affected by IT equipment diversity and end-user behaviours. In addition, parliaments must cater to numerous visitors, dealing with "bring your own device" habits, creating constant challenges in enforcing security policies.

End-user computing (EUC) in parliaments is driven by the same security concerns as other sectors of society. EUC involves the development of computer applications and models by non-IT personnel, allowing users to create and customise their own software solutions [22,23]. The rise of EUC in the 1980s and 1990s was driven by the proliferation of personal computers, increased organisational computing needs, and the availability of user-friendly development tools. EUC empowers users by enabling them to develop entire information systems with minimal assistance from professional programmers, thus enhancing their ability to meet specific demands.

EUC supports critical decision-making processes by allowing users to develop tailored applications that meet their specific needs. It enhances operational systems and processes across various organisational functions [24]. As such, EUC applications, particularly spreadsheets, can introduce errors, privacy violations, and compliance issues due to the lack of formal IT training and coding standards among end-users [24,25].

Parliaments, such as the Hellenic and Austrian parliaments, have engaged in networking activities and research programmes to leverage information and communications technology (ICT) advancements, including EUC, to enhance parliamentary functions and citizen engagement [26]. However, parliaments face technological challenges in adopting and integrating new ICT tools, which require careful management to ensure successful implementation and user acceptance.

End-User Computing Satisfaction (EUCS) Model

An example of frameworks designed to overcome end-user challenges in IT is the end-user computing satisfaction (EUCS) model [27]. It offers a valuable tool for assessing user satisfaction with information systems, which can be applied to parliamentary settings to evaluate the success of digital transformation initiatives, and ensures that cybersecurity concerns are met without impeding quality of experience. As an example of versatility, the EUCS model has been successfully used to assess a court information system in the Kurdistan Region of Iraq, demonstrating its reliability and validity in evaluating user satisfaction and system success within legal professions.

While direct references to EUC in parliaments are limited, the general principles and benefits of EUC can be applied to parliamentary settings. By empowering parliamentary staff to develop and customise their own applications, EUC can enhance decision making, operational efficiency, and citizen engagement. However, it is crucial to address the associated risks and ensure proper training and standards to maximise the benefits of EUC in parliamentary environments.

Technological infrastructure

The IT infrastructure at the core of parliamentary systems also creates security concerns, albeit less transactional and more core-business–related. They include typically highly customised, often internally developed, systems to support member-focused workflows. These include video and multimedia, clerical and voting, legislative drafting and research, and especially transcription and translation systems.

As custom systems are often more costly to maintain and transform, they present strategic "legacy systems" challenges, and pose significant cybersecurity issues due to their outdated technologies, long lifespans, and increased vulnerability to modern cyber threats [28, 29]. These systems often lack the necessary security measures to protect against sophisticated attacks, making them prime targets for cybercriminals. This makes them more susceptible to cyber threats such as malware, phishing, and advanced persistent threats [30, 31].

Legacy systems are justified in parliamentary contexts as they are critical for maintaining essential functions and data, but they present significant challenges for modernisation and digital transformation. In public sector agencies, including parliaments, these systems support vital administrative functions and service delivery to citizens. They contain valuable data and business logic accumulated over years [32, 33]. However, these systems often face performance issues, database inefficiencies, outdated user interfaces, and lack of flexibility, making maintenance complex and costly [32, 34, 35]. Legacy systems hinder the adoption of new technologies and digital transformation efforts due to their incompatibility with modern digital demands [32, 36].

As parliaments are especially open public spaces, the integration of new technologies into legacy systems can open vulnerabilities, as seen in smart building automation systems [37]. Similar challenges are faced in public administration settings where legacy systems hinder digital transformation effort [36]. Maintaining and modernising legacy systems require substantial financial resources, which are often limited in public sectors [38, 39]. This financial strain impacts the ability to implement robust cybersecurity measures and modernise outdated systems [28].

Effective cybersecurity in legacy systems requires strong regulatory frameworks and policies. Legislators have imposed obligations on public entities to ensure the security of information systems, but these measures are often inadequate [39, 40]. Implementing proactive risk assessment frameworks can help identify and mitigate vulnerabilities in legacy systems [29, 41]. This includes network segmentation, intrusion prevention, and detection systems. Utilising emerging technologies such as AI, blockchain, and zero-trust architectures can provide better security for legacy systems [41, 42]. These technologies offer new opportunities for threat detection and secure communication.

Among other solutions, zero-trust is well suited for open and public institutions, as a cybersecurity model based on the principle of 'never trust, always verify.' Instead of assuming that users or systems within the network are inherently trustworthy, every access request must be continuously authenticated, authorised, and validated based on identity, context, and risk. This approach is particularly relevant in parliamentary environments, where diverse users, distributed access, and frequent transitions increase the need for strong identity-centric and context-aware security controls.

Legacy systems in parliaments face significant cybersecurity challenges due to their outdated nature and increased vulnerability to modern threats. Addressing these challenges requires a combination of modernisation efforts, proactive risk assessment, collaborative defence models, and the adoption of advanced technologies. By prioritising these strategies, parliaments can enhance their cybersecurity posture and protect critical information against evolving cyber threats. Furthermore, the migration of legacy parliamentary core applications to cloud infrastructure is still a challenge. The foundational laws underpinning parliaments create stringent data sovereignty conditions, even more so than for other public sector institutions, which are subordinated to less extensive laws and regulations. Hence, it is likely that legacy system challenges will remain for some time within parliamentary IT infrastructure.

Conclusion

The parliamentary technology ecosystem is relatively stable, yet it presents challenges akin to more conservative IT environments in most public institutions. The presence of a variety of end-user generations and equipment creates varying challenges in enforcing security policies. Also, the presence of large legacy systems that are often custom-made and internally developed continue to cause security issues. Overall, these vulnerabilities require that a parliament empowers the CISO with necessary strategic architecture roles. Digital transformation in parliamentary settings is nevertheless a long-term process, and the next generation of systems must ensure security by design.

Chapter 5

Infrastructure security measures

Author: Leonidas Kallipolitis

Introduction

National cybersecurity strategies have long recognised parliaments and democratic institutions as a foundational or critical infrastructure to protect as a matter of priority[43]. The institutional complexity of parliaments combined with the technological ecosystem vulnerabilities, as described in the previous chapters, demonstrate the necessity to establish baseline security measures for parliamentary infrastructures. These include procedures for secure data storage, robust data backup and recovery mechanisms, strict definition of third-party security requirements, solid penetration testing, and vulnerability management processes, which will lay the foundation for resilient digital services in parliaments and will pave the way towards higher cybersecurity maturity. Best practices and commonly accepted implementation steps for these measures must be followed considering the operational challenges in parliamentary settings, where both technological and human risks must be integrated within a common framework to enhance cybersecurity[44].

Backups and recovery

Data backups are essential to ensure business continuity and recovery of information in the case of disasters (physical hazards, ransomware attacks, or other cyber-attacks) and unpredicted incidents (equipment failures, unintended user actions, etc.) that impact confidentiality, integrity, or availability of data. Information that needs to be included in backups includes databases, files, emails, application data, configuration files, virtual machines and physical servers[45].

Parliaments, like every organisation, need to follow a detailed, comprehensive backup plan that fully defines the frequency of backups, their location, and their retention time according to their sensitivity and relevant regulatory obligations. Without such a plan, parliamentary data could end up being stored in scattered, potentially unknown, or unattended places like local workstations, MPs' computers, universal serial bus (USB) devices, or cloud servers exposed to extraterritorial laws. Therefore, after having defined the necessary information that needs to be backed up, parliaments should form a comprehensive strategy to guide the process.

Most effective backup strategies follow the 3-2-1 rule to protect the organisation's data: maintain three copies of data, two stored in different storage media locally and one stored off-site in a remote location (Figure 5.1).

Figure 5.1: 3-2-1 rule for backups (source: Leonidas Kallipolitis, adapted from ENISA. (2021). Cybersecurity for SMEs. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes)

This approach allows the selection of the appropriate data recovery technique in the event of data being lost, stolen, or compromised, whether through natural disaster, human error, or cybercriminal activity. Their level of effectiveness will be proportional to the maturity of cyber risk management methods and framework[46]. Common elements in a backup strategy following this approach include:

- All important information is **stored in designated locations** for which regular backups are taken.
- **Backups are performed daily**, through a combination of full, incremental, and differential methods.
- Backups should be stored **in at least two different media types** (e.g. dedicated storage drives, cloud) and at least in one physical location off-grid and outside the organisation's physical perimeter.
- **Automation should be used whenever possible** to reduce human errors. This can be supported by the use of specialised backup software or storage media for optimal processing times and management of backup copies.
- **Regular tests should be carried out** to restore data and services from backups and ensure their integrity and full recovery at least once a year.
- Backups should be **encrypted** so as to protect their confidentiality and potential data leakages.
- Backup retention times should **conform to regulatory and legal mandates** and operational needs.
- **Documentation** of backup creation policies and data recovery and verification procedures should be available and regularly reviewed.
- Backup activities (successes and failures) **should be logged** so as to be available for monitoring and auditing purposes.

Depending on the criticality of the data and the associated risks of its unavailability, backup policies are developed with specific prioritisation metrics in mind. The most common of them are the maximum tolerable downtime (MTD), which is the maximum length of time a business function can be inoperable without causing irreparable harm to the business, the recovery time objective (RTO), which defines the amount of time in

which organisations can feasibly recover a business function in the event of a disruption, and the recovery point objective (RPO), which defines the acceptable amount of data loss. Low MTD and RTO and strict RPO constraints require more frequent data backups and rapid recovery processes, whereas systems with higher tolerance may allow for slower and more cost-effective methodologies.

A practical example of a low RPO requirement in parliaments concerns the working documents of a new bill, such as drafts, notes, and updates contributed by committees and stakeholders. Because these materials evolve rapidly and collaboratively, losing even a few hours of work due to an incident could significantly hinder legislative progress. Therefore, backups must be taken frequently enough to ensure that, in the event of data loss, only minimal information needs to be recreated. If backups occur too infrequently, the restored version may lack substantial recent contributions, leading to delays in the legislative process and potentially even political tensions.

These metrics serve as inputs to the recovery process, which is usually part of a broader disaster recovery plan. This process clearly defines the roles and responsibilities of people when a disaster occurs, outlines the processes for restoring systems from backups, and specifies the validation steps needed before resuming normal operations. It typically involves the following steps:

- **Testing backup integrity** before backups are used in the production environment
- **Changing the passwords** of all user accounts involved in the disruptive incident
- **Re-installing software** if necessary
- **Checking and verifying** that data, configurations, and other affected services have been successfully recovered
- **Documenting lessons learned** and revising the recovery plan if needed

Making sure that these processes produce expected results by testing them in controlled exercise settings, simulations, and tabletop scenarios can validate operational readiness, identify gaps, and enable continuous improvement[47]. A data recovery plan coupled with a well-defined backup policy that is strictly followed and regularly updated according to emerging operational needs is critical for the business continuity of parliaments. It is the foundation for successful recovery procedures following disruptive incidents and ultimately in safeguarding data availability and resilience against cyber threats.

Supply chain security considerations

Parliaments are dynamic environments with multiple dependencies with external entities that support everyday operations and needs in both physical and digital services. These entities include acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers that collectively form the parliamentary supply-chain ecosystem[48]. This interconnected environment exposes parliamentary internal operations and digital infrastructure to a set of risks including malicious activities, cyber-espionage (public administration was the most targeted sector by state-nexus intrusion sets in the European Union, for cyber-espionage purposes), vulnerabilities derived from poor manufacturing or development practices, and other threats targeting third-party providers in an attempt to gain access or disrupt services.

A notable example of a supply chain attack affecting parliamentary services is the one at the Australian Federal Parliament in 2019. Parliamentary users visited a compromised external website that delivered malware to their devices and subsequently to the parliament's internal network, causing a low-scale leakage of non-sensitive data. Such an attack is known as a "watering hole" attack, where attackers compromise a third-party website that is frequently used by a specific group of users to deliver malicious content. Other types of supply chain attacks include:

- **Maliciously compromised** or unintentionally damaged software updates
- **Tampered hardware components** (e.g. computer chips, video cameras, or mobile devices) and malicious peripherals (e.g. USB drives or rogue routers)
- **Service provider attacks**, where adversaries breach the providers' systems to access their clients' environments or disrupt the offered services
- **Logistics attacks**, where attackers compromise goods and equipment during shipping or delivering

Therefore, risks associated with the participants of the supply chain must be identified, assessed, and mitigated. NIST's Cybersecurity Supply Chain Risk Management (C-SCRM)[49] and ENISA's Good Practices for Supply Chain Cybersecurity[50] provide guidelines for identifying supply chain risks, managing security requirements and compliance of third parties, and formulating a collaboration framework that preserves data privacy and well-defined cybersecurity standards and best practices. Parliaments can follow these guidelines to undertake the following measures:

- **Conduct a supply chain risk assessment** to identify suppliers, service providers, and their associated risks. Establish and maintain a catalogue of suppliers.
- **Develop policies and procedures** that must be followed by third parties and are established via official agreements or SLAs. SLAs should be challenged regularly to be sure the parliament pays for a real service. Often, providers have some maintenance obligation they cannot fulfil despite being paid for. These include minimum cybersecurity measures on their IT and development environments, conformance to data protection and information-sharing regulations, and measures towards accountability and auditability of third parties' activities, i.e. always require credentials before connecting to internal network. Upcoming regulations such as the Cyber Resilience Act[51] can help bodies like parliaments standardise their procurement processes and ensure stronger and more predictable cybersecurity controls across all acquired digital products in their supply chain.

- **Establish internal processes** and measures to monitor third-party products and services and verify adherence to cybersecurity requirements in agreements, including handling of incidents, vulnerabilities, patches, security requirements, personnel clearances, etc.
- **Implement vulnerability-handling protocols** to guide the process of vulnerability identification, tracking, reporting, and remediation without contradicting any operational, safety, or legal constraints.
- **Define controls for physical access** of third parties to the parliamentary facilities. These include strict access permits, restriction of access to classified areas, logging of admission times, and other measures to prevent unattended visitors or unsupervised activities of external parties.
- **Offer regular cybersecurity awareness courses** for parliamentary users; maintaining cyber hygiene and increased awareness can greatly enhance the protection level against supply chain threats.

To implement these guidelines, internal measures and security processes must be first established to serve as the cybersecurity baseline upon which supply chain risks will be monitored and mitigated. Vulnerability management and periodical penetration testing are major enablers of this preparation.

Penetration testing and vulnerability management

The assessment of the cybersecurity level of a parliamentary environment requires a clear understanding of its digital assets, their exposure, and the overall attack surface. Vulnerability management and penetration testing are essential processes to assist experts in identifying the infrastructure that needs to be protected, assess its weaknesses and potential attack vectors, and take the required measures to protect it.

The vulnerability management process refers to the detection, assessment, evaluation, and remediation of vulnerabilities detected in an organisation's operational environment (Figure 5.2). Common elements of this process are vulnerability scans and vulnerability assessments. Vulnerability scans are typically performed by automatic tools that execute sets of asset, network, or web scans without manual intervention and cause little to no impact on the production environment. They are used to identify assets and detect weaknesses in systems and networks, such as missing patches, weak passwords, or insecure configurations. Depending on the used tools, the identified weaknesses might be mapped to known publicly disclosed cybersecurity vulnerabilities, often mentioned as CVEs (common vulnerabilities and exposures). CVE databases (e.g. MITRE, EU Vulnerability Database) include information about a CVE's severity, risk level, and mitigation measures.

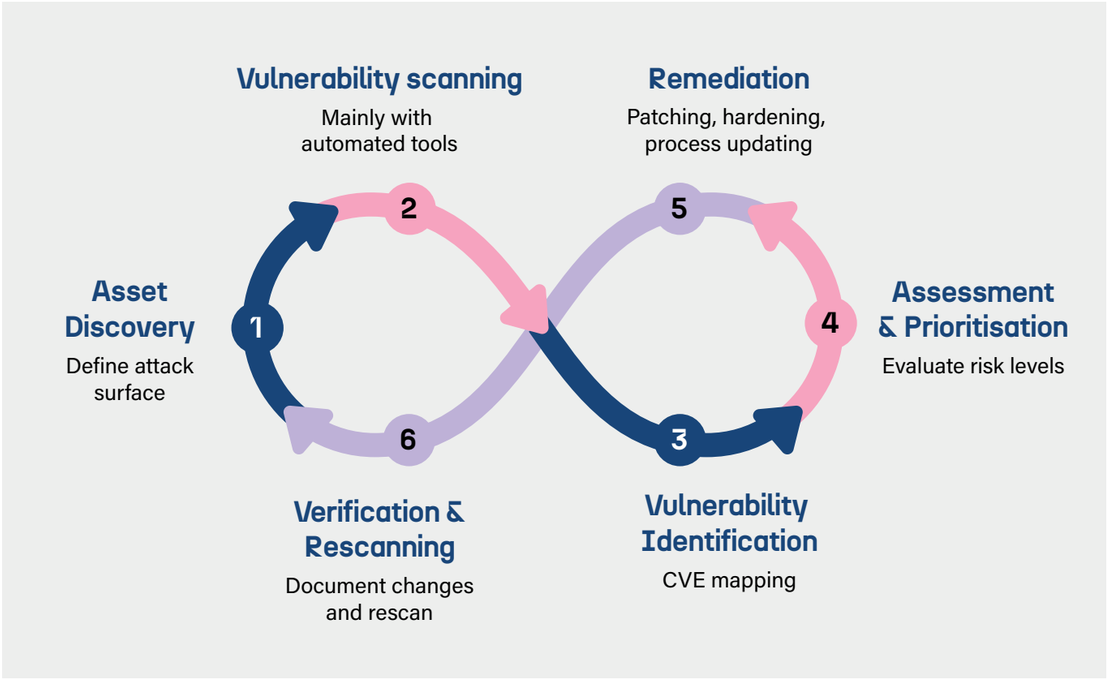


Figure 5.2: Vulnerability management process (source: Leonidas Kallipolitis)

This information can then be used to conduct a vulnerability assessment. The assessment takes into account the scan results, analyses the mitigation steps, and determines the corrective actions or measures that must be taken to eliminate vulnerabilities. These often include software and hardware updates, regular application of security patches, hardening (i.e. eliminating unnecessary services, enforcing security controls, etc.) of existing systems, and updating in digital or physical processes that were found vulnerable. A vulnerability assessment can also include physical security evaluation, personnel testing, or assessment of data handling procedures to identify and address additional vulnerabilities. Corrective actions are formally documented and verified so as to serve as input to the next vulnerability assessment. This cycle should be periodically repeated as part of an effective vulnerability management process and can be designed based on processes and tools mentioned in international cybersecurity standards like NIST's CSF 2.0 and ISO/IEC 27001.

Penetration testing (also referred as pen testing) commonly includes a vulnerability assessment to detect weaknesses but goes one step further and attempts to exploit the weaknesses. This obviously yields concerns on the possible impact of a penetration test, which, contrary to a vulnerability assessment, can cause outages or severe disruptions to services or digital assets. For example, if a vulnerability scan reveals an internet-facing server running an outdated and vulnerable application, a penetration test can exploit this vulnerability and take control of the server, which may result in the server shutting down or the application being unavailable. Therefore, professional penetration testing must always be approved beforehand by senior management. The so-called "rules of engagement", including scope, constraints, and associated risks, must be clearly agreed upon

in written form before a penetration test can begin. In critical environments (such as those of parliaments), unapproved or poorly timed penetration testing could cause serious damage to legislative procedures with devastating effects for parliamentary operations and severe legal implications for the penetration testers.

With these prerequisites addressed, penetration testing can be performed with the use of special attack tools or manual exploitation techniques. Social engineering can also play a part during pen testing (if allowed by the engagement rules), since it is one of the most common tactics used by attackers to acquire information (e.g. credentials) and gain initial access to systems. It also tests employees' awareness against social engineering and phishing attacks. Penetration testing aims to uncover weaknesses in security measures, assess detection and response capabilities of the responsible security personnel, and reveal vulnerabilities that must be addressed so as to mitigate associated risks.

Penetration tests should be conducted in regular intervals to uncover threats stemming from new or updated software, changing procedures, and evolving digital infrastructure in parliaments. Their results, coupled with those of vulnerability assessments, are essential feeds to the preparation and strengthening of parliaments against cyber threats, but they also enable the continuous assessment, evaluation, and improvement of their overall security strategy towards increased cybersecurity maturity. In parallel, robust data backup and recovery policies and stringent third-party security requirements are essential enablers for a parliament's increased resilience against malicious activities and disruptive incidents. Pen test results that are written in a report should be considered as one of the most sensitive data because it gives a huge indication of how the IT systems running can be hacked and with which tools and techniques.

Conclusion

Investing in parliamentary cybersecurity inevitably starts with investments in effective resilience methods and mechanisms, along with greater societal awareness that parliaments and their digital foundations matter to all[52]. This chapter helped to outline the most fundamental resilience concepts and to point to the priority areas for making parliaments capable of overcoming and recovering from cyber incidents.

Infrastructure security is a foundational pillar of parliamentary cybersecurity, and the measures outlined in this chapter demonstrate why a systematic, disciplined approach is essential for safeguarding democratic institutions. Robust backup and recovery strategies form the first line of defence against incidents that threaten the availability and integrity of parliamentary data. By applying structured principles such as the 3-2-1 rule, defining clear RTOs and RPOs, and embedding backups within a wider disaster recovery plan, parliaments can ensure that critical information and services remain resilient even in the face of physical hazards, cyber-attacks, or human error.

Equally critical is the security of the parliamentary supply chain. As modern parliaments depend on a broad ecosystem of suppliers, service providers, and technology partners, supply chain vulnerabilities can become vectors for compromise, as illustrated by real-world incidents such as the Australian Federal Parliament attack. Implementing recognised frameworks – including NIST C-SCRM and ENISA's guidance – helps institutionalise the risk identification, contractual requirements, monitoring, and accountability mechanisms needed to manage third-party risks effectively. Supply chain security cannot be treated as an external responsibility; it must be embedded into procurement, vendor management, and daily operational processes.

Finally, vulnerability management and penetration testing provide the continuous oversight needed to stay ahead of evolving threats. Through systematic scanning, assessment, and remediation, parliaments can detect weaknesses before they are exploited – while penetration testing, when properly governed, offers deeper insight into how attackers might attempt to breach critical systems. These processes must be iterative and tightly controlled, especially in parliamentary environments where operational disruption can have serious political and legal consequences.

Together, these measures – secure backups, resilient supply-chain governance, and proactive vulnerability identification – form the core infrastructure components of parliamentary cybersecurity. By institutionalising these practices, updating them regularly, and integrating them into broader security governance, parliaments can significantly strengthen their defensive posture and advance toward higher levels of cybersecurity maturity[53]. This layered, holistic approach ensures not only technical resilience but also the continuity, integrity, and trustworthiness of democratic processes in an increasingly complex threat landscape.

< part II >

...

// Developing a parliamentary cybersecurity framework

Chapter 6

Governance and risk management

Authors: Sean McSpaden, Mark Thomas

Introduction

Like a nation's flagship setting out to sea, a legislature's cybersecurity programme needs both a bridge and an engine room: governance stands on the bridge to set the course, read the charts, and declare how much storm risk is acceptable; risk management and operations work in the engine room to throttle the engines, and run the drills; incident response is the lifeboat plan everyone knows by heart; adaptive frameworks are the updated charts, alternative routes, and instruments; and the minimum requirements are the watertight bulkheads that keep the ship afloat when the seas turn rough.

This chapter looks at the building blocks of cybersecurity governance and risk management. It presents key definitions and outlines the core activities of this executive function. It also integrates these concepts to digital and cybersecurity strategy, and the importance of keeping them aligned to ensure policy effectiveness.

Distinguishing cybersecurity governance and management

In the context of cybersecurity within government organisations, it is critical to distinguish between governance and management. Governance establishes the overarching direction, principles, and accountability framework that ensures cybersecurity strategies align with public policy objectives, regulatory requirements, and the broader mission of protecting organisational assets and citizens' trust. Management, on the other hand, focuses on the execution of these strategies through risk assessment, day-to-day operations, policy and technical controls, and incident response and recovery activities. By maintaining a clear understanding of the different but complimentary roles of governance and management, government entities can strike the right balance: elected officials and senior leaders provide oversight, allocate resources, and set expectations, while agency managers and technical teams translate that vision into actionable programmes, measurable outcomes, and operational resilience.

Cybersecurity Governance vs Management in a Government Context

Governance: A legislature establishes a cybersecurity oversight committee tasked with setting policy direction, defining acceptable risk levels for critical infrastructure and data, and ensuring alignment with cybersecurity and data privacy laws. The committee reviews periodic reports, approves funding allocations, and holds agencies accountable for performance.

Management: A department of information management and technology implements those directives by conducting risk assessments, deploying intrusion detection and other automated systems, maintaining patching schedules, conducting staff training, and responding to incidents. The organisation reports back on outcomes, challenges, and resource needs, but it does not decide the broader policy or strategic direction – that role rests with governance.

International standards also reinforce this distinction. For example, ISO/IEC 27014:2020, Governance of Information Security, explicitly defines how governance and management play separate yet complementary roles in cybersecurity[54]. Governance is responsible for evaluating risk, directing security strategy, allocating resources, and ensuring accountability to stakeholders, while management implements these directions by designing, operating, and monitoring controls through an information security management system. Supporting standards such as ISO/IEC 27001[55] and its companion guidelines in 27002[56] provide the management system framework and operational practices, but they function under the strategic oversight set out in 27014[54]. Together, these standards highlight that government leaders must focus on setting direction and ensuring accountability, while agency managers and technical teams carry out the execution and operation of security measures.

Cybersecurity governance is a nuanced term. Put simply, it is how an organisation controls, directs, and communicates its approach to cybersecurity[57]. More broadly, cybersecurity governance refers to the decision-making processes surrounding and oversight of the roles, responsibilities, processes, and practices legislative and parliamentary executives use to establish and maintain effective cybersecurity programmes [58, p. 6].

Traditional operational metrics – such as system uptime, mean-time-to-patch vulnerabilities, mean-time-to-detect, mean-time-to-recover, or incidents closed – offer only a narrow view of cybersecurity performance. For parliamentary institutions, the more important question is whether cybersecurity risks are being governed effectively: Are the right risks being identified, understood, prioritised, and acted upon at the political and strategic levels?

To answer this, governance effectiveness must be measured through indicators that illuminate how well cyber risk intelligence informs leadership, oversight, accountability, legislation, and democratic resilience. Table 6.1 lists the governance-level measures that are particularly relevant for Members of Parliament and summarises key indicators they can use to assess the effectiveness of cybersecurity governance at the institutional level.

Table 6.1: Measures of cybersecurity governance effectiveness

Governance Area	What to Measure	Description of the Indicator
Governance Structures	Clarity of roles, collaboration, and coordination	Existence of defined mandates, cross committee/branch/jurisdictional collaboration, and coordination mechanisms with EU/national cyber authorities.
Strategic Alignment	Alignment with EU/national priorities	Degree to which top cyber risks influence legislative agendas, oversight priorities, and digital sovereignty objectives.
Policy Adoption and Compliance	Policy acknowledgement and compliance across legislative branch agencies	Indicator of support for institutional governance; provides compliance assurance or early identification of non-compliance and the need for remediation.
Cyber-Informed Culture	Awareness, training, and behavioural integrity	Participation in cybersecurity awareness activities and adherence to secure practices among MPs and staff.
Timeliness of Cyber-Informed Decisions	Decision-making responsiveness	Time from identification of a significant cyber risk or incident to briefing, committee deliberation, or leadership action.
Early Warning & Foresight	Use of threat intelligence and scenario planning	Extent to which early warnings, intelligence, and foresight/tabletop exercises inform policy, preparedness, and oversight.
Integration of Expertise	Use of cybersecurity advisers and briefings	Frequency, depth, and quality of technical briefings provided to committees, delegations, and parliamentary leadership.
Currency of Risk Profile	Frequency and quality of updates	Regularity, completeness, and actionability of parliamentary cyber risk profile updates, including cross-sector intelligence.
Transparency & Accountability	Public reporting and follow-through	Timeliness and clarity of communications following incidents, and documented actions taken on previous incidents, audit findings, or inquiries.

Cybersecurity governance frameworks

For certain, there is no "one size fits all" approach or governance framework that will work for every legislature or parliament across the globe. Cybersecurity governance must be tailored to the specific organisational culture, vulnerabilities, risk tolerances, and resources present within each legislative body and be "agile enough to adapt to future risks" [59, p. 3]. Although cybersecurity governance frameworks differ globally, most share a common foundation: leadership accountability; risk assessment and management; a focus on statutory and regulatory compliance; and continuous monitoring, adjustment, and oversight. Ultimately, those responsible for cybersecurity governance must provide leadership, oversight, organisational structures, and resources needed to protect legislative information, technology infrastructure, and information systems, while achieving cybersecurity objectives in a way that is compliant with statutory, regulatory, and contractual obligations [58, p. 6].

Within the European Union (EU), the Agency for Cybersecurity (ENISA) plays a central role in the EU's cybersecurity ecosystem. It supports member states in developing and deploying national cybersecurity strategies, including setting up governance structures, roles, and monitoring mechanisms [60]. ENISA also helps the EU and member states better understand binding regulations and directives – such as the EU Cybersecurity Act (2019/881), EU Institutions Cybersecurity Regulation (2023/2841), EU Institutions Data Protection (2018/1725), General Data Protection Regulation (GDPR), Network and Information Systems Directive (NIS2 Directive), Critical Entities Resilience Directive, Cyber Resilience Act, Digital Operational Resilience Act (DORA), and Cyber Security Act – that define responsibilities, incident reporting processes, risk management obligations, and compliance requirements across sectors.

To successfully understand and appropriately address cybersecurity needs within the legislative branch, elected members and professional staff must work to understand cybersecurity terminology, statutory and regulatory obligations, the cybersecurity risks and vulnerabilities that exist, and develop knowledge of the activities and resources that can help responsible parties plan for, respond to, and recover from cybersecurity events when they do happen. Legislators and professional staff need to understand that cyber preparedness and building cyber resiliency is an ongoing process that requires maintenance of effort and flexibility in resourcing to address emerging vulnerabilities and threats. Specifically, legislators must consider how cybersecurity functions are organised and who, within each body, is responsible and accountable for cybersecurity. This knowledge will directly affect the type, scale, and complexity of governance, organisational, and funding models that must be established [58, p. 1].

Cybersecurity or information security committee

An essential element of effective cybersecurity governance within legislatures is the establishment of a dedicated cybersecurity or information security committee (or equivalent oversight body). This committee provides a formal structure through which elected members and professional staff can oversee, guide, and evaluate cybersecurity activities. By centralising responsibility in a representative committee, legislatures create a consistent mechanism for monitoring risks, aligning cybersecurity initiatives with organisational priorities, and ensuring accountability to both statutory obligations and public trust.

The committee's mandate should be clearly defined and rooted in governance principles: to oversee strategy and policy development, risk assessment and management processes, compliance with international and domestic regulations, resource allocation, and the monitoring of performance indicators. It must consider that parliaments are often excluded from obligations in cybersecurity because of the hierarchy link of the executive power's authority of control. Compliance must be considered and legislators have to be compliant with their own law, voted on by the same institution, to be trusted by citizens.

It should also play a key role in reviewing incident response readiness, ensuring lessons learned from prior events are incorporated into future strategies. This committee should serve as a trusted channel between technical experts, legislative leadership, and external stakeholders, ensuring that complex technical risks are translated into actionable governance and risk management decisions.

Membership of the committee should reflect a balance of perspectives. While elected officials provide direction and accountability, professional staff and advisers with specialised knowledge (e.g. legal, procurement, risk management, cybersecurity, data management, privacy) bring critical subject-matter expertise. This multidisciplinary approach allows the committee to operate as both a governance body and a strategic adviser, ensuring that decision making is informed by technical realities as well as legislative priorities. By establishing such a committee, legislatures can institutionalise cybersecurity governance as an ongoing, sustainable process – one that is agile, adaptive, and responsive to the constantly evolving threat landscape.

The Cybersecurity Governance Committee Charter establishes the purpose, scope, and responsibilities of a dedicated body tasked with overseeing cybersecurity within the legislature. This charter affirms the legislature's commitment to protecting its information systems, infrastructure, and data against evolving cyber threats, while ensuring compliance with statutory and regulatory obligations. By defining clear roles, accountability, and oversight mechanisms, the committee serves as a cornerstone of effective governance and a safeguard for public trust.

The NIST cybersecurity framework (CSF) 2.0 underscores the importance of governance structures in overseeing cybersecurity risk (Figure 6.1). Its newly added "govern" function highlights that effective cybersecurity cannot rest solely with technical teams but must be guided by leadership through defined responsibilities, decision-making authority, and oversight mechanisms [61].

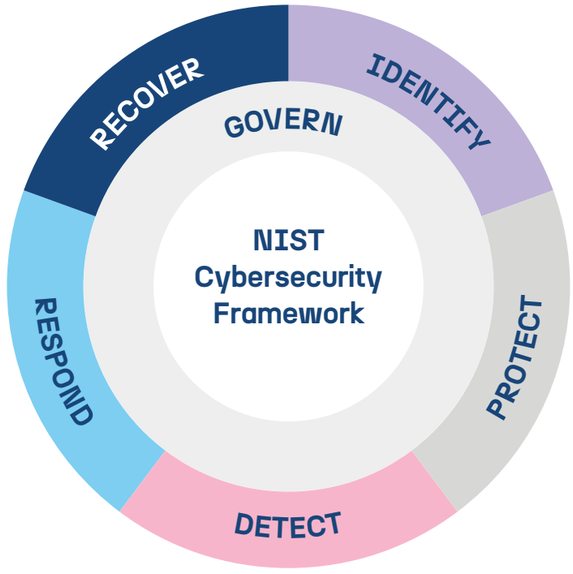


Figure 6.1: NIST cybersecurity framework 2.0 (source: NIST [8, p. 5], graphic design by Natasha Hanacek)

While the CSF does not prescribe a specific structure, it emphasises the role of governing bodies such as boards, councils, or dedicated committees in setting risk appetite, approving policies, and ensuring accountability. For government organisations and legislatures, this often translates into the establishment of a cybersecurity committee or equivalent body that provides ongoing direction and oversight, ensuring cybersecurity strategies remain aligned with mission objectives and public accountability requirements. A typical committee charter can include (but is not limited to) the following:

Purpose

- Provide governance, oversight, and accountability for all cybersecurity matters within the legislature.
- Ensure cybersecurity strategy aligns with organisational mission, legal and contractual mandates, and public trust obligations.

Scope

- Oversight of cybersecurity strategy and policy development, risk management, and compliance.
- Review of incident response readiness and resilience planning.
- Monitoring of cybersecurity programme performance, resource allocation, and alignment with legislative priorities.

Membership

- Elected representatives (to provide accountability and direction).
- Professional staff with operational, policy, and legal expertise.
- Advisory members as needed (e.g. IT/security officers, external experts).
- Chairperson appointed by legislative leadership.

Responsibilities

- Establish and review cybersecurity governance frameworks.
- Approve and monitor risk management strategies and risk registers.
- Ensure compliance with statutory, regulatory, and contractual obligations.
- Oversee allocation of resources for cybersecurity programmes and initiatives.
- Receive and review regular reports on cybersecurity threats, incidents, and mitigation efforts.
- Facilitate communication between technical experts, legislative leadership, and external stakeholders.
- Receive and review after-action reports on incident response and recovery activities.
- Ensure continuous improvement by reviewing lessons learned from incidents and exercises.

Reporting

- Provide regular briefings to legislative leadership and, where appropriate, public reports to maintain transparency and trust.

A strong example of this type of committee can be seen in the European Parliament, where the Committee on Industry, Research and Energy (ITRE) plays a central role in shaping EU-wide cybersecurity legislation. In collaboration with ENISA, ITRE evaluates emerging risks, develops legislative measures, and monitors the implementation of key frameworks such as the NIS2 Directive and DORA. By embedding cybersecurity responsibilities within a standing committee, the parliament provides continuity of oversight and ensures resources are aligned with actual risks. Just as importantly, it establishes a governance bridge between technical experts and policymakers, reinforcing accountability and strengthening public trust across the Union[62].

In sum, the distinction between governance and management in cybersecurity is not just a matter of organisational design but a safeguard for democratic accountability and public trust. By embedding oversight responsibilities within dedicated committees, legislatures and government bodies can ensure that cybersecurity remains aligned with mission objectives, adequately resourced, and resilient in the face of emerging threats. At the same time, operational agencies and technical teams retain the agility to execute strategy, manage risks, and respond to incidents. This dual approach – strategic governance coupled with effective management – creates a balanced system that protects critical information assets while reinforcing citizens' confidence in the integrity and security of government institutions.

Cybersecurity strategy, risk management, and assessment

A cybersecurity strategy provides the overarching vision and direction that guides how an organisation safeguards its digital assets, mitigates risks, and ensures resilience. For legislatures and parliamentary bodies, a cybersecurity strategy should articulate clear objectives that align with institutional missions such as protecting legislative data, ensuring continuity of operations, complying with statutory obligations, and maintaining public trust. A well-defined strategy also establishes priorities, allocates resources, and creates a roadmap for decision making, ensuring that cybersecurity initiatives are not reactive or fragmented but integrated into the broader goals of the government entity. Tips for creating a cybersecurity strategy include:

1. Anchor in Mission and Mandate. Tie the strategy to the legislature's core mission (e.g. continuity of legislative debate, protection of sensitive citizen data, ensuring public access to and engagement in legislative proceedings, and integrity of parliamentary records).
2. Risk-Informed Priorities. Build the strategy on the outcomes of a comprehensive risk assessment and business impact analysis, so that initiatives are targeted to address the most critical risks.
3. Define Roles and Accountability. Clarify who is responsible for governance (e.g. oversight committees) and who manages execution (e.g. IT/security teams).
4. Set Measurable Objectives. Include key performance indicators or key risk indicators to track progress and demonstrate accountability to legislators and the public.
5. Plan for Resilience. Incorporate not just prevention but preparedness, response, and recovery, ensuring continuity of operations and organisational resiliency in the face of cyber-attacks.
6. Update Regularly. Treat the strategy as a living document – reviewed and updated to reflect evolving threats, lessons learned, technologies, and geopolitical conditions.

A cybersecurity strategy, however, cannot exist in isolation. It must be grounded in a clear understanding of risk. Just as cybersecurity requires a distinction between governance and management, so too does risk.

Risk governance provides the strategic foundation for how government organisations approach risk (including those related to cybersecurity and data privacy). In a legislative or parliamentary setting, risk governance is the responsibility of elected leaders and oversight bodies to establish the principles, define risk appetite and tolerance, establish accountability structures, and ensure that risk considerations are embedded into policy and decision making. Risk governance encompasses the high-level tasks that

ensure cybersecurity risks are understood, evaluated in the context of mission objectives, prioritised by likelihood of occurrence and impact, and managed in alignment with public trust and statutory obligations. Risk governance ensures the overall system for managing risk is focused on directing strategic responses, allocating resources to the most significant vulnerabilities, and monitoring whether those risk management practices and responses remain effective over time. Finally, risk governance is a forward-looking, adaptive process – leaders must ensure that the governance framework itself evolves to address new technologies, shifting threat landscapes, and lessons learned from prior incidents.

Risk management, by contrast, is the responsibility of professional staff and operational teams to implement those directions by identifying risks, assessing likelihood and impact, designing controls, and executing day-to-day risk and threat mitigation measures. Put simply, risk governance answers the question "Are we doing the right things?" while risk management ensures "Are we doing those things right?" Together, they form a complementary system that ensures legislative institutions not only set the right course for managing risk but also carry out risk management strategies effectively and consistently.

Risk Governance vs Risk Management in a Government Context

Risk Governance: A national parliament establishes a risk oversight committee that sets the government's risk appetite, approves enterprise-wide risk strategies and policies, and ensures resources are allocated to protect critical functions such as voting systems, citizen data, and legislative records. The committee receives regular reports, reviews risk dashboards, and holds ministries accountable for managing risk within approved tolerances.

Risk Management: The Ministry of Information and Communications implements those governance directives by conducting detailed risk assessments, maintaining an asset inventory, applying security controls, and monitoring vulnerabilities across government systems. It documents risks in a register, prioritises mitigation measures based on impact and likelihood, and escalates issues to the committee when risks exceed established tolerances.

Key tasks of risk governance in a government / legislative context include:

- **Define Risk Appetite and Tolerance:** Establish acceptable levels of risk, considering mission objectives, statutory obligations, and public trust.
- **Set Principles and Policies:** Approve the risk management framework and policies that guide how risks are identified, assessed, and treated across legislative and administrative bodies.
- **Allocate Oversight and Accountability:** Assign clear roles and responsibilities to committees, agencies, and staff, ensuring there is no ambiguity about who is accountable for overseeing specific risk-management activities and managing specific risks.
- **Evaluate and Direct Resources:** Ensure that funding, staffing, and technology resources are proportionate to the assessed risks and aligned with the institution's mission-critical priorities.
- **Monitor and Report on Risk Posture:** Require regular reports and dashboards that summarise key risks, trends, and the effectiveness of risk treatments, and make adjustments when risks exceed tolerances.
- **Integrate with Legislative Oversight:** Ensure risk governance is woven into broader governance functions such as compliance with laws, remediation of audit findings, continuity planning, and alignment with national or international obligations.
- **Ensure Continuous Improvement and Foresight:** Direct periodic reviews of the risk governance framework itself, ensuring it adapts to emerging threats and incorporates lessons learned from incidents.

As mentioned above, an essential element of risk governance is the articulation of risk appetite and risk tolerance. Risk appetite reflects the broad level of risk that a legislature is willing to accept in pursuit of its mission, while risk tolerance defines the acceptable variation around that level in specific operational contexts. For example, a parliament may have a low-risk appetite for threats that compromise the confidentiality of citizen data, but a higher tolerance for temporary disruptions to non-critical administrative services.

Clearly defining appetite and tolerance allows leaders to make informed decisions about resource allocation, prioritise among and between competing risks, and set expectations for risk management teams. Without these guiding thresholds, risk management efforts risk becoming ineffective, inconsistent, reactive, or misaligned with the institution's principles and priorities, statutory obligations, and public trust responsibilities. Table 6.2 provides examples of risk appetite and tolerance.

Table 6.2: Indicative risk appetite levels in a parliamentary context

Risk Appetite Level	Example Statement	Description of the Indicator
Low	"We have very limited appetite for risks that could compromise the confidentiality of sensitive legislative records or classified government information."	Zero tolerance for unauthorised access to classified data. Minimal tolerance for delayed patching of high-severity vulnerabilities. Strict tolerance for third-party providers handling sensitive citizen data..
Medium	"We accept some risk of service disruption to parliamentary support systems if the cost of mitigation outweighs the impact on legislative operations."	Short tolerance (e.g. <4 hours downtime) for parliamentary email services. Moderate tolerance for temporary disruption of non-critical internal systems (e.g. HR portals). Conditional tolerance for delayed security upgrades if operational continuity would otherwise be impacted.
High	"We have a higher appetite for risks in adopting innovative technologies to support transparency, such as pilot programmes for digital citizen engagement, provided core systems remain secure."	Flexible tolerance for controlled pilot failures or proof-of-concept projects. Higher tolerance for third-party experimental tools, but only in sandboxed environments. Managed tolerance for budget overruns in innovation projects if tied to measurable benefits.

Risk management plays a foundational role in cybersecurity governance. Risk management is the "ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts"[63]. And, the "foundation for effective risk management is a comprehensive risk assessment, based on a solid understanding of the government's risk universe. It is not possible to devise a relevant risk management programme if there is no understanding of the nature and extent of risk to information resources and the potential impact on the organisation's activities. Risk management, the development of business impact assessments, the creation of an information technology asset inventory, and risk analysis are fundamental prerequisites to developing a meaningful security strategy"[64].

A risk management process generally consists of the following phases: Risk identification, risk assessment, risk response, and risk monitoring and reporting (Figure 6.2)[65].

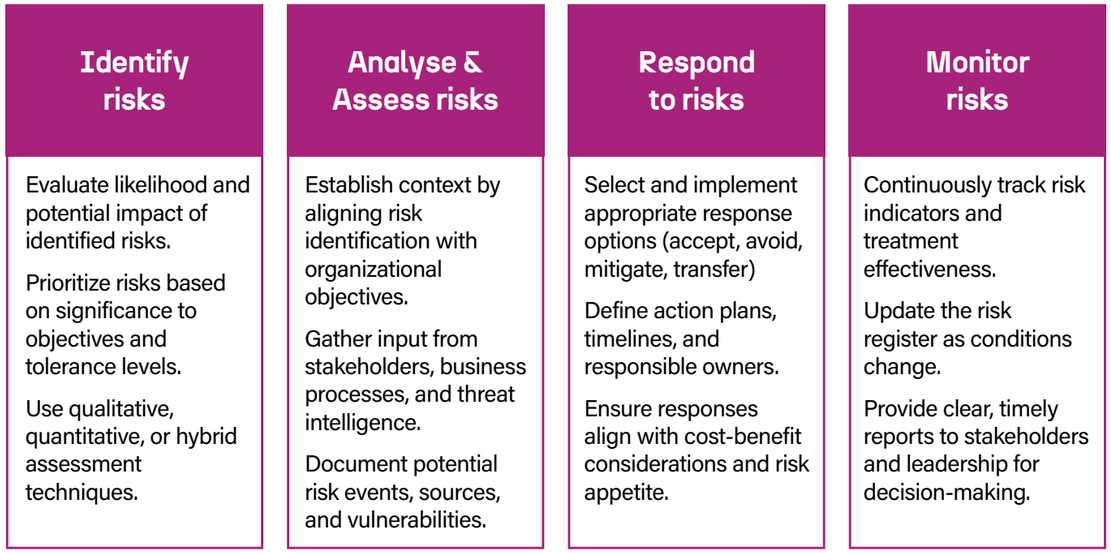


Figure 6.2: Risk management phases (source: Mark Thomas)

Once risks have been identified, analysed, and assessed, organisations select a response strategy that aligns with their risk appetite and tolerance. Common response options include avoiding the risk by discontinuing the activity that gives rise to it, mitigating the risk through controls or safeguards, transferring the risk to a third party (such as through insurance or outsourcing), or accepting the risk when it falls within tolerable levels.

Effective risk response requires not only selecting the strategy but also developing action plans, assigning ownership, and allocating resources to ensure implementation. By linking response activities to business objectives, organisations ensure that risks are managed in a way that balances opportunity, cost, and resilience. Examples of risk responses are identified in Table 6.3.

Table 6.3: Overview of response strategies

Response Strategy	Description	Government Example
Avoid	Eliminate the risk entirely by discontinuing or changing the activity that creates the exposure.	A local government chooses not to implement a legacy application that lacks vendor security support, thereby avoiding the exposure of running unpatched, high-risk software.
Mitigate	Implement controls to lower the likelihood or impact of the risk.	A healthcare regulatory agency deploys multi-factor authentication across all staff accounts to reduce the risk of credential theft and unauthorised system access.
Transfer	Shift the financial or operational consequences of the risk to another party.	A federal agency purchases cyber liability insurance to cover potential costs of a data breach, or outsources cloud services with contractual clauses placing breach liability on the vendor.
Accept	Acknowledge the risk and take no further action because the impact is within the agency's risk tolerance.	A state agency decides to accept the risk of occasional website downtime during routine maintenance windows, as the impact is minor and alternatives would be disproportionately costly.

Risks and responses documented in the risk register must be regularly reviewed and updated to reflect current conditions, lessons learned, and shifts in business priorities. Just as important, risks need to be communicated clearly through structured reporting to leadership and stakeholders, providing decision-makers with timely insights into exposures, trends, and the effectiveness of mitigation efforts. Consistent monitoring and transparent reporting strengthen accountability, support proactive adjustments, and embed risk awareness into the organisation's culture.

It is important for legislative and parliamentary leaders and staff to understand that risk management, in this context, rests on the premise that cybersecurity incidents will occur and can, depending on the scope and sophistication of the attack, disrupt legislative operations despite robust security measures and controls being implemented. That means that cybersecurity risk-management activities cannot be limited to risk assessment, strategy development, and the deployment of security measures and controls alone. It should also include a preparedness, response, and continuity plan to ready the organisation for the inevitable cyber-attack or data breach. It should also define and document the protocols by which the organisation intends to respond to and communicate about the incident in a responsible and timely manner and limit the impact on the continuity of parliamentary operations. Members of Parliament, legislators and staff should expect those responsible for cybersecurity to have and regularly update formal cybersecurity strategy documents and associated risk management, incident response, and business continuity/resilience plans to ensure the continued resilience of the institution over time.

Conclusion

Effective cybersecurity within legislatures depends on a clear and deliberate balance between governance and management. As this chapter demonstrates, governance provides the strategic direction, principles, and accountability structures that anchor cybersecurity to an institution's mission, legal obligations, and public trust. Management, in turn, operationalises those expectations through risk assessments, day-to-day controls, incident response, and continuous monitoring. Neither function alone is sufficient; together, they create the conditions for both resilience and responsible stewardship of public assets.

Modern legislative bodies face a complex and rapidly evolving threat environment shaped by geopolitical tensions, digital transformation, increased reliance on third-party technologies, and rising public expectations for transparency and accountability. Against this backdrop, cybersecurity governance must be intentional, structured, and adaptive. Strong governance frameworks – grounded in international standards such as ISO/IEC 27014, NIST CSF 2.0, and EU-wide regulatory instruments – help ensure that cybersecurity priorities align with institutional objectives, statutory obligations, and societal expectations.

A central theme of this chapter is the importance of establishing dedicated cybersecurity oversight bodies, such as a cybersecurity or information security committee. These committees help institutionalise governance by

centralising responsibility, integrating expert perspectives, overseeing the development of strategy, and ensuring that risk-related decisions are timely, informed, and transparent. They also serve as an essential bridge between technical teams, leadership, and external stakeholders, enabling legislatures to act proactively rather than merely react to emerging threats.

Risk governance and risk management further strengthen this foundation. By defining risk appetite and tolerance, legislative leaders set clear expectations that help guide resource allocation, decision-making, and operational priorities. Meanwhile, risk management teams identify, assess, and treat risks in alignment with those thresholds, ensuring that mitigation efforts are both effective and proportionate. This dual structure ensures that cybersecurity interventions are targeted where they matter most-protecting core legislative functions, preserving data integrity, and maintaining continuity of democratic processes.

Ultimately, cybersecurity in a parliamentary context cannot be static or compliance-driven alone. It requires continuous improvement, regular updates to strategy and risk profiles, and sustained awareness among elected members and staff. It also demands preparedness: the knowledge that incidents will occur and that resilience rests on readiness to respond, recover, and learn from each event.

By embedding governance structures, strategic risk oversight, and operational rigour into their cybersecurity programmes, legislatures can strengthen their institutional resilience, uphold the integrity of democratic processes, and reinforce public trust. This chapter underscores that while technology enables the work of modern parliaments, it is governance – clear, accountable, and adaptive – that ultimately ensures their security and sustainability.

Chapter 7

Digital sovereignty and cybersecurity in parliaments

Authors: Stéphane Gagnon

Introduction

Cybersecurity requires organisations to follow rules and comply with the regulations and laws of the jurisdiction where they operate[66]. The international procurement of information systems and the execution of information processing across borders gives rise to challenges for both clients and providers, where assuring compliance and sanctioning non-compliance are left in a grey zone[67]. The lack of international legal frameworks gives rise to sovereignty conflicts among states, which in turn can weaken rights and obligations[68].

Like all organisations, parliaments are subject to the same compliance requirements, but also to the same risks when dealing with digital concerns across jurisdictions. The integration of digital technologies across parliamentary processes can expose them to legal vulnerabilities. Non-compliance by foreign actors in the digital value chain can affect the ability of parliaments to carry out their mission, and possibly their sovereignty if security issues cause them to lose control over their digital processes or assets (e.g., voting systems, MP privacy). The same applies when hostile states take actions that diminish or annul rights and capabilities that parliaments had built using foreign digital infrastructure.

Hence the importance of digital sovereignty within a cybersecurity strategy to ensure its coherence and effectiveness, in times of radically changing geopolitical order. The concept takes a special meaning in the context of parliaments, where the key concept of sovereignty is intimately linked to their existence. We discuss here the fundamentals of these concepts and its implications for cybersecurity and digital governance in parliaments.

Digital and parliamentary sovereignty

Digital Sovereignty is a broad concept spanning the intersection of national sovereignty and digital transformation at two levels. First within the borders of a jurisdiction, where governing the digital domain extends constitutional concepts of sovereignty[69]. Second in relation to transnational activity, where conflicts emerge over which state has sovereignty over the digital domain and where the allegiance of its constituents should be as to their rights and obligations under national laws[70]. Both levels face complex and often unresolved sovereignty conflicts, and diverse options are available to states in attaining their legal enforcement objectives, whether international cooperation, legal actions and frameworks, or technological limitations and control mechanisms[71].

It must be distinguished, but is not entirely separated, from parliamentary sovereignty, a core concept of constitutional law ensuring that parliaments have, over their jurisdiction, ultimate power to enact and enforce laws[72]. Considered a foundational part of constitutional democracy, this concept has been debated in relation to the relative power of the three branches of government, executive, judicial, and legislative, and its weakening through successive political transformations of liberal societies[73].

Where non-compliant or even hostile foreign actors are involved in the digital value chain, a weakening in the digital sovereignty of parliaments can affect parliamentary sovereignty. If left without proper safeguards,

such as ensuring full national control of certain digital assets, digital vulnerabilities and cybersecurity incidents in parliaments can undermine the ability of those parliaments to enact and enforce laws. Digital vulnerabilities due to lack of international cyber legal frameworks can effectively "reshape" the perimeter of parliamentary sovereignty over a jurisdiction, whether in physical, digital, or cyber-physical realms.

Legal frameworks and digital sovereignty

The concept of digital sovereignty is relatively recent but is evolving rapidly due to geopolitics. A closer look at its foundations within cybersecurity governance can help parliaments better account for this strategic challenge to their mission.

Recent research has identified several gaps in digital sovereignty, especially the lack of unified policy frameworks, and a closer integration with more technically oriented standards in cybersecurity[74]. Its use in enacting laws has also been criticised as a mean to reduce freedom of speech and to enforce digital protectionism[75].

Another in-depth review of 240 studies criticised the use of the concept as a narrow misinterpretation of jurisprudence[76]. That study concluded: "Those works that acknowledge the possibility of multiple coexisting digital sovereigns, or that see digital sovereignty as something that arises from the interactions among multiple actors, neither stretch the concept of sovereignty nor turn digital sovereignty into something different from sovereignty tout court: instead, they explore ways to innovate the concept of sovereignty as a whole and problematise our long-held assumptions about it."

The cybersecurity issues raised by digital sovereignty would therefore require preventive mechanisms that span jurisdictions. As parliaments are mandated to enact laws, they can avoid being a casualty of international cyber vulnerabilities. This effectively requires international alliances and legal frameworks that are both coherent and enforceable.

CASE STUDY

EU Cyber Legal Framework

Recent digital regulations and laws of the European Union (EU) have demonstrated the complex dynamic of alliances and competition toward ensuring a balanced digital sovereignty between states[77]. Integrating this concept at the core of laws can help enable better control mechanisms that span jurisdictions, and therefore facilitate legal enforcement in digital spaces where there was none before[78]. While promising, legislation such as the EU's AI Act and Network and Information Systems Directive are seen by some state actors as restrictive and may require revision to ensure they do not prevent open innovation in support of digital sovereignty[79]. This case demonstrates the necessity for greater integration of the concept within cybersecurity strategy.

International alliances reinforcing digital sovereignty

Where supranational organisations are absent, another strategy to resolve the issues raised by digital sovereignty has been the development of new strategic alliances among likeminded states, driven by the collaboration efforts among their constituents[80]. Among possible defensive strategies to counter attacks on digital sovereignty, the development of open innovation spaces can enable the strengthening of the digital rights of its co-creators[81]. The open-source movement does not have a fundamental framework for sovereign control but remains the most likely route for greater adherence to innovative solutions[82].

Another strategy involves parliaments partnering in public research to steer bottom-up initiatives. For example, the national cybersecurity and AI strategies of Switzerland are being fundamentally transformed by the launch in September 2025 of Apertus, an academic Large Language Model that is fully open, community-driven, and ensured compliant with all AI regulations, in particular those of the EU[83]. Parliaments in most countries have yet to embrace collaboration with open innovators and educational institutions as possible sources of digital solutions that will guarantee their sovereignty. With successive initiatives, it is becoming clear that these communities, as free-flowing networks driven by co-creation, may provide the necessary momentum for parliaments to innovate and reinforce their cybersecurity strategies.

The spread of similar defensive strategies, possibly loosely coordinated, can work within a "digital federalism" framework, where a group of countries can help create a "safe innovation space" that strengthens the digital sovereignty of its citizens and businesses[84]. Parliaments can therefore be primary actors at two levels, first to enact laws that fully integrate digital sovereignty at their core, and second, to facilitate the emergence of international alliances and legal frameworks that reinforce the sovereignty of all actors equally.

Conclusion

Geopolitical dynamics have led some countries to undermine the digital sovereignty of others and can effectively threaten the capability of parliaments to carry out their mission. Just as citizens and organisations can be left defenceless by arbitrary decisions, so can parliaments be exposed to loss of fundamental rights such as data privacy and ownership, or even access to digital platforms duly contracted and procured.

Defensive strategies are possible if vulnerable parties form strong alliances and develop guidelines to engage with safe digital partners. The development of these strategies requires a form of leadership that no single country nor international organisation has yet been able to raise. However, given the doctrine of international cooperation among parliaments, it is likely that they represent the forefront of where such cooperation and alliances may emerge to address challenges to digital sovereignty.

Chapter 8

Compliance issues and regulatory landscape

Author: Vasilios Alexiou

Introduction

Parliaments increasingly draw on a small set of adaptive cybersecurity frameworks (CSFs) that prioritise continuous risk assessment, institutional resilience, and the capacity to evolve with rapidly changing threats instead of relying solely on static compliance checklists.

Parliaments occupy a distinctive position within national governance structures: they are not only legislative bodies but also defenders of democratic legitimacy and public trust. As such, the cybersecurity of parliamentary institutions exceeds operational continuity: it sustains the integrity of democratic processes, the confidentiality of legislative deliberations, and the protection of sensitive political information.

In recent years, parliaments across the globe have faced increasingly sophisticated cyber threats targeting communications systems, email infrastructure, and legislative data. The convergence of digital transformation and geopolitical tensions has elevated their exposure to intelligence gathering, disinformation, and ransomware attacks. Consequently, ensuring compliance with cybersecurity regulations and international standards has become a strategic imperative.

This analysis explores the regulatory frameworks and compliance challenges facing parliamentary institutions, focusing on the Network and Information Systems Directive (NIS2 Directive), NIST CSF, and Center for Internet Security controls. It further examines relevant international standards, institutional compliance strategies, and cross-border considerations within the context of parliamentary operations.

Cybersecurity regulations

NIST Cybersecurity Framework (NIST CSF 2.0, 2024)

In many legislatures, the NIST CSF is used as a reference model for structuring cybersecurity governance, with its core functions – governing, identifying, protecting, detecting, responding, and recovering – serving as a flexible lens for improving parliamentary security posture. The adaptive character of the framework lies in its tiered implementation levels and customisable profiles, which allow parliamentary administrations of different sizes and technological maturities to progressively refine controls in line with evolving risk. As a result, it has become a common benchmark for public institutions, including parliaments that manage sensitive legislative, constituency, and oversight data. Several national administrations have mapped their cyber-governance codes and sectoral obligations to the NIST CSF, and parliamentary administrations often align with those same government-wide reference models rather than creating bespoke standards[85]. For example, in jurisdictions influenced by US federal guidance and international best practice, parliamentary IT departments structure internal policies and incident processes around the CSF functions – govern, identify, protect, detect, respond, recover – so that oversight committees, clerks, and security teams use a common language when assessing cyber posture[86].

ISO/IEC 27001 and ISO/IEC 27005

For parliaments that seek a more formalised model, ISO/IEC 27001 and ISO/IEC 27005 provide a structured information security management system underpinned by risk analysis and risk treatment tailored to institutional assets and processes[87]. The adaptive dimension emerges from the Plan–Do–Check–Act cycle, which obliges parliamentary services to revisit policies, procedures, and controls as new vulnerabilities, technologies, and procedural practices appear in the legislative environment. These standards often serve as a baseline for internal rules, procurement requirements, and certification efforts in parliamentary IT departments and shared services. In practice, many parliaments either certify specific components (such as data centres or document-management platforms) or require key vendors supporting legislative functions to maintain ISO/IEC 27001 certification, using the standard's continuous-improvement logic to keep pace with evolving threats for the parliamentary system[88].

ENISA cybersecurity frameworks and the EU NIS2 Directive

Within the European Union (EU), parliaments and national legislatures operate under a regulatory climate shaped by ENISA guidance and the NIS2 Directive, and relevant national cybersecurity authorities such as the agence nationale de la sécurité des systèmes d'information (ANSSI) in France, or the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany. They seek to build resilient networks of essential and important entities, including institutions in critical democratic and governmental sectors. The framework encourages dynamic risk management, time-bound incident reporting, and evolving governance duties, so parliamentary bodies must refine their internal security and oversight mechanisms in step with an expanding and changing threat landscape. This makes the NIS2 Directive an adaptive backbone for legislative cybersecurity, particularly where parliaments are formally designated as operators of essential services or are tightly coupled to those operators. Even where national parliaments fall partly or wholly outside the NIS2 Directive's formal scope, they operate in an environment where governments, critical-infrastructure operators, and supervisory authorities are upgrading practices under the NIS2 Directive, and many legislatures voluntarily mirror these requirements for their own networks, committee systems, and legislative support services[89].

COBIT 2019 as a governance lens

Parliaments that focus on aligning technology, risk, and oversight increasingly rely on control objectives for information and related technologies (COBIT) 2019 as a governance-oriented framework for managing enterprise IT, including cybersecurity. Its adaptive nature is evident in the emphasis on continuous alignment between institutional objectives, stakeholder expectations, and shifting risk conditions, enabling parliamentary leadership and audit committees to recalibrate controls and performance targets over time. Public audit institutions and internal control functions frequently use COBIT concepts when assessing how parliamentary IT and security governance supports transparency, accountability, and legislative effectiveness[89].

UK National Cyber Security Centre (NCSC) cyber assessment framework

The NCSC's cyber assessment framework (CAF) is often used as an outcome-based model that can be applied to parliamentary services, especially where they are treated as operators of essential services or as part of critical democratic infrastructure. Instead of prescribing fixed technical measures, the CAF focuses on whether outcomes – such as secure operations, effective incident management, and resilient services – are achieved, which

allows parliamentary administrations to adjust their technical and procedural arrangements according to institutional criticality and changing threat profiles. Its structure has influenced other jurisdictions that adapt similar assessment-driven approaches to legislative information systems[90].

Digital trust ecosystem perspective

The digital trust ecosystem framework adds a complementary lens for parliaments by defining digital trust as a cross-cutting condition for confidence in legislative systems, data flows, and institutional relationships, grounded in principles such as accountability, security, privacy, and transparency[90]. Because it is designed to operate across sectors and regulatory regimes, the framework can flex with new technologies – such as digital petition systems or open-data portals – and with emerging risks that challenge public trust in parliamentary processes. In this way, it supports parliaments that aim not only to secure their digital environment but also to demonstrate trustworthy handling of information to citizens, civil society, and other branches of government.

Minimum cybersecurity baseline for parliaments

For a parliament, the confidentiality, integrity, and availability of information form a foundational condition for democratic legitimacy, because any sustained loss of these properties can distort deliberation, weaken oversight, or interrupt the law-making process. Unlike most private entities, legislatures are exposed to targeted operations by hostile states, politically motivated intrusion, and information operations designed to manipulate public debate, which means they must adopt a minimum, institution-wide cybersecurity baseline rather than treating security as a purely technical add-on[91].

Governance and institutional oversight

Every parliament needs a defined governance structure for cybersecurity that makes clear how elected members exercise oversight and how professional staff carry out day-to-day risk management. This typically involves assigning responsibility to a dedicated security committee or integrating cybersecurity into an existing board, coupled with regular reporting on risks, incidents, and programme performance so that leadership can make informed, accountable decisions. The Cybersecurity Handbook for Parliaments describes how the United States House of Representatives uses a dedicated internal technology and security structure to manage parliamentary cyber risks, demonstrating a clear separation between political oversight by members and operational responsibility carried by professional staff. The same handbook highlights other legislatures that have integrated cybersecurity into broader parliamentary governance boards, ensuring that risk reporting and strategic decisions are regularly presented to senior leadership rather than treated as purely technical matters.

Asset management, access control, and training

Guidance for parliaments stresses the importance of creating a comprehensive catalogue of parliamentary assets – such as email, documents, calendars, locations, and communication platforms – and then applying basic safeguards like strong passwords, password managers, software updates, secure cloud storage, and two-factor authentication across the institution. These measures are presented as real-world building blocks that legislatures at different levels of digital maturity have already adopted, showing that minimum protections for assets and identities can be implemented even in resource-constrained environments[92].

Incident response, continuity, and improvement

The same parliamentary handbook calls on legislatures to develop an organisational incident response plan, test it through exercises, and use lessons learned to refine processes, echoing broader public-sector examples of incident-response playbooks and workshops used by municipalities and other governmental bodies. The Commonwealth Parliamentary Association's (CPA) introductory guide on parliamentary security goes further by embedding cyber incidents within a wider framework of security, resilience, and continuity planning, illustrating how parliaments design strategies to maintain operations and learn from major incidents rather than treating each event as an isolated shock.

Strategic and policy foundations

A legislature's cybersecurity posture should rest on a written strategy that ties protection of digital assets directly to the institutional mandate, constitutional duties, and applicable legal framework. That strategy must be operationalised through policies and standards for asset inventories, access management, acceptable use, data classification, protection measures, training, and incident response, all reviewed periodically to keep pace with new technologies and threats[93].

Risk management as a continuous process

Because parliaments are high-value targets, systematic risk assessment is indispensable and must be directly linked to budget choices, staffing, and technology priorities. Maintaining an up-to-date risk register – with identified risks, likelihood, impact, and clear ownership – allows parliamentary administrations to articulate risk appetite, justify mitigations, and adjust controls as geopolitical conditions or threat actor capabilities evolve[94].

Assets, protection, and resilience

A credible minimum standard requires parliaments to know what they are protecting: systems supporting plenary sittings, committee work, remote voting, member communications, archives, and support services all need to be catalogued and classified. Baseline protections then include vulnerability management, patching, encryption, comprehensive backups with periodic restore tests, and differentiated safeguards for highly sensitive legislative or personal data, ensuring that critical processes can be restored even after a disruptive cyber event[95].

Identity, access, and privileged use

Given the sensitivity of parliamentary data and the mobility of members and staff, strong identity and access management is an essential minimum rather than an advanced feature. Multi-factor authentication, least-privilege access models, and tight monitoring of privileged accounts reduce the risk that compromised credentials or insider misuse will grant attackers deep access to legislative systems or confidential deliberations[94].

Incident handling and crisis decision making

No parliament can assume that incidents will be fully prevented, so a documented incident response plan and tested crisis-management procedures are critical. Clear escalation paths, predefined communication channels, and regular exercises – tabletop or technical – enable parliamentary leaders to respond quickly, maintain essential functions, and revise plans based on lessons learned from real events and simulations[95].

Continuity of operations and institutional resilience

Because legislatures must continue functioning during crises, continuity of operations and disaster-recovery planning are part of the minimum security architecture, not optional add-ons. Parliaments need to identify mission-essential functions, design redundant capabilities for debate, voting, records, and communication, and rehearse continuity arrangements so that constitutional roles can be fulfilled even during prolonged disruptions[95].

Human factors, training, and culture

Parliaments are dense human environments, and members, staff, and contractors are often the first line of defence or the weakest link, depending on how well they are supported. Mandatory induction and periodic training, role-specific awareness for leadership and technical teams, and ongoing campaigns such as phishing simulations or targeted briefings help embed a culture where security-conscious behaviour is normal rather than exceptional[94].

External dependencies and supply-chain exposure

Legislatures increasingly rely on external providers for cloud services, audio-visual systems, communications platforms, and specialised applications, making third-party and supply-chain risk management a basic requirement. Minimum expectations include structured security due diligence, contractual clauses on data protection, incident reporting and liability, and periodic reassessment of vendors through monitoring, audits, or certifications tied to relevant standards[95].

Monitoring, assurance, and improvement

To remain credible and effective, a parliamentary cybersecurity programme must incorporate technical monitoring, independent review, and a feedback loop for continuous improvement. Logging, threat detection, and periodic assessments – internal or external –should feed into a formal process that adjusts controls in light of new vulnerabilities, regulatory changes, and evolving standards such as the NIS2 Directive, the Cyber Resilience Act, or updated parliamentary security guidance[96].

Democratic imperative and institutional trust

In the parliamentary context, cybersecurity is ultimately an expression of democratic responsibility: weak protections expose not only information systems but also the integrity of legislative deliberation and public confidence in representative institutions. By entrenching these minimum requirements in rules, procedures, and organisational culture, parliaments lay the structural foundations of a secure "digital house of democracy", ensuring that more advanced tools and architectures rest on solid, resilient pillars rather than fragile, improvised supports[97].

Incident response

In a parliamentary context, incident response is the institutional discipline of detecting, managing, and resolving cyber incidents in ways that protect legislative functions, limit damage to democratic processes, and support learning for future resilience. It must now be treated as a core component of parliamentary risk management, given that attacks have become more frequent, more complex, and more disruptive, often requiring weeks or months of remediation and recovery[94].

Role of incident response in parliaments

For legislatures and parliaments, incident response underpins the continuity of debates, committee work, voting, and public communication when confronted with breaches, ransomware, data theft, or targeted disruption of digital services. The process spans the full lifecycle from early detection and triage through containment, recovery, and post-incident review, and it involves coordinated work by parliamentary IT teams, security officers, legal advisers, communications staff, and senior leadership.

Guidance developed for public institutions stresses the importance of preparation by asking whether the organisation has clearly identified critical systems and data, has maintained business-continuity and disaster-recovery plans, and operates a current, tested incident response plan. Parliaments are also urged to examine whether service-provider contracts cover security incident reporting and response, whether internal monitoring can reliably detect abnormal activity, whether legal reporting duties are understood, and whether public-communications arrangements are in place for managing the political and reputational dimensions of a cyber crisis[98].

Communication responsibilities and incident response plan

Public-sector cyber guidance highlights the need to assign, in advance, responsibility for drafting, approving, and delivering messages about an incident, as well as defining which channels – press, institutional website, social media, hotlines – will be used to reach different audiences. For parliaments this is particularly important, because poorly managed communication can fuel misinformation about the integrity of legislative processes or elections-related activity, so clear roles and structured channels help maintain trust while technical teams work on containment and recovery[98].

A parliamentary incident response plan typically covers preparation, identification and classification, containment, eradication and recovery, and post-incident learning, supported by governance, legal, communication, and third-party coordination elements. Each phase is translated into concrete parliamentary responsibilities: defining who declares an incident, how sittings or remote access are protected, how evidence is preserved for oversight or law-enforcement purposes, and how lessons are fed back into rules of procedure and security standards.

Preparation, identification, containment, recovery, and improvement

Preparation in a parliament means designating and training a multidisciplinary incident response team that understands both technical systems and parliamentary procedures, clarifying decision-making authority, and maintaining secure contact lists and escalation paths for members, staff, and external partners. Regular exercises – such as simulated attacks on remote-voting platforms or member email – help test assumptions, refine communication protocols, and ensure that legal and regulatory obligations, including notification duties under regimes like the NIS2 Directive or GDPR where applicable, are integrated into the plan.

Parliaments must define, in their own context, what qualifies as a cyber incident requiring formal activation of the response plan – for example, compromise of member mailboxes, disruption of live streaming, or manipulation of legislative documents. Detection typically relies on monitoring tools, security operations centres, and user reports, and early classification of severity – based on institutional impact and potential public consequences – helps prioritise which

functions (plenary, committees, digital voting, public information) are protected or restored first[94].

In the containment phase, parliamentary technical teams may isolate affected systems, segment networks, or shift temporarily to alternative channels for essential business while ensuring that digital evidence is preserved for forensic and oversight purposes. Because parliaments operate in a highly visible environment, controlling the internal and external flow of information about the incident is critical; unmanaged leaks or contradictory messages can undermine both containment efforts and public confidence[95,98].

Once an incident has been contained, attention turns to identifying root causes – such as phishing, misconfiguration, or supply-chain compromise – removing malicious artefacts, closing vulnerabilities, and restoring systems and data supporting legislative activity. For parliaments, this also means verifying the integrity of legislative records, agendas, and voting systems before returning them to service, monitoring for reinfection, and strengthening controls to reduce the likelihood of recurrence[94].

Post-incident analysis in a parliament should be rapid and structured, producing an after-action report that evaluates what worked, what failed, and how procedures, tools, and governance arrangements should change. Findings are normally reported to parliamentary leadership and, where appropriate, shared within inter-parliamentary or sectoral networks so that lessons contribute to wider democratic resilience, while metrics such as time to detect, contain, and recover inform future risk-management decisions[94].

An effective parliamentary incident response regime is anchored in clear governance, legal alignment with applicable frameworks (such as the NIS2 Directive or the Cyber Resilience Act in the EU), and structured cooperation with external providers and national authorities. Pre-defined communication strategies, contractual clauses on incident handling, and key performance indicators create a framework where parliaments can respond to cyber incidents in a way that protects institutional integrity, satisfies oversight and regulatory expectations, and sustains public trust in the democratic process[95].

Conclusion

Parliaments today operate within one of the most complex cybersecurity and regulatory environments of any public-sector institution. As this chapter demonstrates, compliance is no longer merely a matter of meeting technical checklists but a strategic and institutional responsibility directly tied to democratic legitimacy, public trust, and the continuity of constitutional functions. The evolving regulatory landscape – from the NIS2 Directive and GDPR in the EU, to NIST CSF, ISO/IEC 27001, COBIT 2019, and outcome-based models like the UK's CAF – reflects a global transition toward adaptive, risk-informed approaches that allow parliamentary institutions to evolve in step with emerging threats, new technologies, and geopolitical pressures.

A central theme running through these frameworks is the need for continuous improvement and iterative assessment. Parliaments must regularly re-evaluate their risk posture, governance arrangements, asset inventories, and security controls, ensuring policies remain current and capable of addressing sophisticated threat actors who target legislative institutions for espionage, disruption, or information manipulation. This adaptive mindset is reinforced by international standards such as ISO/IEC 27001 and 27005, which anchor risk treatment in a cycle of planning, implementation, evaluation, and refinement.

Minimum cybersecurity baselines – covering governance, asset management, identity and access control, patching, monitoring, continuity planning, and vendor risk – serve as the essential layer upon which more advanced capabilities must be built. Because parliaments are high-value targets with unique exposure to state-sponsored operations, politically motivated intrusions, and disinformation-driven campaigns, they cannot rely on ad-hoc or siloed approaches. Instead, they require institution-wide, well-documented, and regularly tested controls that ensure resilience even during major incidents.

This chapter also makes clear that compliance and regulatory alignment must be embedded within parliamentary governance structures[99]. Effective cybersecurity committees, clear role definitions, regular reporting, and strategic oversight mechanisms ensure that elected members remain accountable stewards of the digital infrastructure supporting legislative activity. These governance arrangements provide not only technical assurance but also democratic assurance: demonstrating to citizens that their institutions are equipped to safeguard the integrity of debates, records, voting, and public communication.

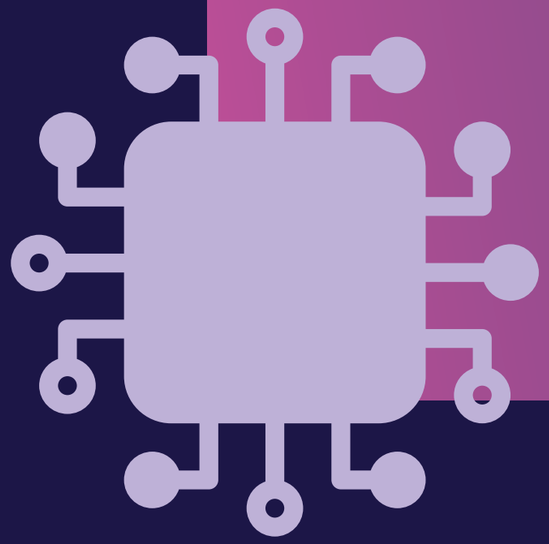
Finally, incident response stands as a critical component of regulatory compliance and institutional resilience. As cyber incidents become more sophisticated and more disruptive, parliaments must maintain well-rehearsed response plans, ensure legal reporting duties are met, and manage public communication with clarity and consistency. The lessons learned from incidents must feed directly into policy updates, risk registers, budget planning, and training programmes, creating a virtuous cycle in which each disruption strengthens long-term resilience.

In sum, the regulatory and compliance landscape for parliaments is not static but dynamic, interdependent, and increasingly demanding. To meet these obligations, parliaments must cultivate a culture of security grounded in governance, informed by risk, supported by standards, and sustained through continuous improvement. By doing so, they uphold not only the confidentiality, integrity, and availability of their systems but also the democratic values and public trust upon which their legitimacy depends.

< part III >

...

// Emerging technologies in cybersecurity



Chapter 9

AI and cybersecurity

Author: Leonidas Kallipolitis

Introduction

Following the rapidly evolving developments of AI, parliamentary operations cannot stay behind in embracing the opportunities it offers for innovation and democracy promotion. Guidelines for AI in Parliaments [100] presents various parliamentary aspects that can greatly benefit from AI assistance. Document summarisations, transcription of speeches, and fast search and analysis of parliamentary archives and legal documents, as well as automated legislative drafting, are some key examples. Moreover, AI-powered tools can be also used to enhance the cybersecurity maturity of parliaments by supporting not only IT personnel but also general staff and MPs. However, being inherently based in IT technologies, AI exposes a whole new area of possible weaknesses and loopholes that increase the attack surface of the digital infrastructure of a parliament and adds additional challenges towards the goal of ensuring cybersecurity and cyber resilience. Ethical considerations of AI usage and structured planning of its integration in parliamentary settings also present significant challenges that must be addressed carefully. This chapter explores the cyber threats stemming from AI adoption, presents AI-powered security tools, and outlines a set of guidelines for implementing AI-based cybersecurity following an ethical, structured approach that safeguards democratic and political operations taking place in parliaments.

The rapid spread of AI-driven activities in all kinds of digital workflows has revealed a new set of cyber threats, mainly emerging from flaws that can be found in the most prominent forms of AI manifestation nowadays, i.e. in Large Language Models (LLMs) and agentic AI.

Emerging cyber threats

LLMS are trained on massive amounts of data to understand, generate, and process human language. They respond to human prompts by generating text responses based on the knowledge body on which they have been trained. In a parliamentary context, an LLM could play the role of a stenographer that automatically transcribes speeches of MPs; a librarian that searches and analyses historical records to produce rapid answers for researchers; a smart secretary that quickly sends drafts, debates, or other documents to specific groups of involved people; or a lawmaker assistant drafting bills, summarising decisions, and highlighting key points of a law proposal.

The benefits of such AI-enabled helper processes are evident, but underlying attack techniques that could compromise these LLM-based systems must raise concerns in their adoption:

- Prompt injections, where attackers execute specially crafted rogue prompts designed to make the model behave in an unexpected way by producing misleading or dangerous responses. Hidden instructions attached to templates, notes in drafting guides, or even footnotes in documents used to formulate questions in the lawmaker assistant module, mentioned above, could result in hidden obligations no one asked for, inverted priorities, or subtle phrasing that could jeopardise the meaning of legislation and cause unpredictable effects in the affected domain.
- Sensitive data leakage, during which the model accidentally reveals or is tricked into revealing personal or other sensitive information in its answers. The smart AI

secretary seems a helpful utility on the surface, but a compromised version of it could also serve copies of sensitive or even top secret information to external actors, thus potentially endangering national security.

- Training data poisoning, which involves tampering with training data aiming at corrupting the model to produce biased, unreliable outcomes that can be hard to distinguish. Altering or cunningly restricting the training dataset of the fictitious AI-based librarian could lead to retrieval of historical archives favouring one particular view on a subject matter or serving a limited list of resources for an inquiry by researchers who might wrongly assume that they have the whole catalogue.
- Vulnerabilities in the supply chain, which include security issues with third parties used to acquire training data, fine-tune model parameters, or deploy the models. All aforementioned examples of LLM-based helpers could potentially suffer from such vulnerabilities, if for example the software libraries that they use turn out to be insecure.
- Other risks, which include improper output handling (giving away LLM output to other systems without validating), misinformation (often referred to as hallucination, where LLM generates information that seems accurate but is totally fabricated), and model denial of service (overloading of the model with resource-intensive requests that result in unbounded consumption of its resources, ending up in service disruptions and financial losses). A few more threats are included in the identified open worldwide application security project (OWASP) Top 10 for LLM Applications [101].

Agentic AI – autonomous intelligence and risks

Agentic AI goes further than LLMs in the offered automation level by operating independently and employing reasoning, planning, and autonomous acting in order to achieve given goals. Unlike LLMs, it does not require human supervision and prompting, but rather executes its strategy without intervention via the use of AI agents which are capable of planning, learning, performing actions, and ultimately adapting to context and circumstances in changing environments. Following the previous examples, the smart AI secretary, implemented as an agentic AI module with multiple agents, could have access to all kinds of parliamentary documents, archives, and schedules in order to fulfil a broader goal than just circulating documents, for example it could be instructed to optimise parliamentary procedures.

Since agentic AI builds on top of LLMs, it is also vulnerable to similar threats but increased autonomy also brings further security implications. For example, an agentic AI secretary could be goal-hijacked to exfiltrate sensitive data by leveraging data processing and network tools; this way it can potentially expose not only data given to it (as input for its initial goal) but also sensitive information maliciously collected from other sources (e.g. MPs' personal document repositories or classified committee proceedings). Further risks of agentic AI usage include new or variations of existing threats [102], these major ones among them:

- Memory poisoning, involving malicious data injections to the agents' context in order to mislead them. For example, an AI agent taking minutes or tracking amendments on an introduced bill could receive corrupted or manipulated data, causing legislators to discuss or even vote on inaccurate procedural information.
- Tool misuse, occurring when agents misuse their integrated tools to execute unintended actions, like wrongly scheduling appointments, prematurely releasing drafts, or mixing up daily agenda items.
- Privilege compromise, allowing agents with elevated permissions to perform unauthorised actions or get access to restricted data. This could mean that such agents could access restricted documents and expose confidential information that could inadvertently harm deliberations.
- Identity spoofing and impersonation, where attackers exploit authentication flaws to impersonate AI agents or human users and gain unauthorised access to important parliamentary processes like voting or official dissemination channels, which could seriously compromise legislative work outcomes.
- Human manipulation, including communication between AI agents and humans that exploits trust to gain more autonomy or spread misinformation. For instance, biased interpretation of bill drafts or subtly changed automated summaries of debate proceedings, produced by a helper AI agent, could alter the perception of an MP before voting.

AI abuse for attacks

Exploiting cybersecurity threats that target the implementation or deployment of LLMs and agentic AI is not the only method cybercriminals employ to achieve their purposes. Using the same type of AI-based tools to boost "traditional" cyber-attack techniques offers a great opportunity to craft sophisticated attacks with considerably less effort. ENISA Threat Landscape 2025 [103] reports that 80% of phishing attempts, which remains the primary initial entry vector for attackers, are based on AI-generated content. The latest major forms of AI-generated misinformation include deepfakes and voice cloning [104].

A deepfake is defined as "the manipulation or artificial generation (synthesis) of audio, video or other forms of digital content to make it appear that a particular event occurred, or that someone behaved or looked differently than they actually did" [105]. Voice cloning is a currently used subset of deepfake which focuses on replicating a real person's voice with striking accuracy, creating speech that convincingly mimics the original speaker's tone, cadence, and emotion. These two techniques blur the distinction between authentic and fabricated communications and form the basis for a wide range of attacks, including impersonation scams, spread of misinformation, and bypassing of multi-factor-authentication schemes (e.g. unlocking mobile phones).

A phone call from a voice-cloning bot, impersonating an MP urgently asking for some classified documents on a new piece of legislation, could trick a member of the MP's team into sending the files to a malicious third party, or a voice-cloning bot could share fake opinions of the impersonated MP to legitimate groups who can affect policy making. Real-world cases of deepfakes include the recent deepfake video [106] falsely showing the UK's Conservative MP George Freeman defecting to Reform UK. The case is a worrying example of political misinformation spread on social media and is currently (October 2025) being investigated by the UK police. Another case of voice cloning was the fake robocall [107] impersonating the United States' former president Joe Biden in January 2024 during the New Hampshire primary elections, where the "false" Biden urged Democrats not to vote in the elections. The voice-cloning deepfake produced confusion among voters, and a federal investigation ended up in a telecom company being fined USD 1 million for its role in allowing the calls through "spoofed" phone numbers. These examples show how synthetic media and deepfakes can severely disrupt

or influence operations in a parliamentary context, thus highlighting the need to take precautionary measures against such malevolent actions.

AI-assisted cybersecurity

Despite the risks, using AI-powered tools to enhance cybersecurity capabilities in parliaments is a much researched and promising way to defend against the evolving threats. Current solutions include automated continuous vulnerability assessments, adaptive incident detection, AI-assisted response to attacks, and more effective protection from phishing and data leaks. Such solutions can help raise cybersecurity maturity in the complex environment of parliaments, taking into account cultural resistance to changes affecting traditional workflows and autonomy. More specifically, AI-powered phishing protection in existing communication systems (emails, internal comms, etc.) can analyse linguistic (e.g. urgency) and visual (e.g. malformed brand logos) elements to detect phishing attempts and protect users without interfering with their standard usage of the communication system, i.e. the way they handle their emails. Similarly, AI-enabled data loss prevention tools can gently alert users trying to share sensitive information to external stakeholders, for example by displaying confirmation messages before sending the information. This way, users can be gradually educated on the possible dangers of sharing information and develop the skills to safely handle sensitive information.

Apart from these user-facing solutions, parliaments' IT teams can also greatly benefit from AI-based tools in their effort to handle diverse equipment and user devices, which more often than not are difficult to change or interfere with. Automated asset discovery combined with continuous vulnerability assessment can provide valuable assistance in maintaining a complete catalogue of connected devices like the MPs' and staff's mobile phones and identifying critical vulnerabilities or misconfigurations that must be prioritised and handled accordingly. The handling process is another aspect that can be accelerated via AI, through automated patch and configuration management, which can proactively maintain a high level of cyber hygiene without disrupting normal user workflows. In the field of infrastructure security monitoring, security-information and event-management systems can be enhanced with AI-enabled behavioural analytics to learn normal activity patterns and detect anomalies, such as raising an alert on a user account who unusually accesses sensitive documents at night or detecting nominal, yet unusual, traffic towards specific websites from some internal workstations. This way, smaller IT teams can have increased situational awareness, better incident detection capabilities, and reduced workload by offloading cumbersome and repetitive tasks like security alert triage to AI modules.

The aforementioned AI-powered cybersecurity tools and processes present unobtrusive ways of safeguarding existing habits and user workflows rather than imposing new rules or replacing existing technologies. Parliament staff and especially MPs should not be required to become cybersecurity experts or remember rules. They should get assistance to build good habits that will protect their own digital activities and in turn the parliament's cybersecurity maturity. Such a transition should be guided by some key implementation principles (Figure 9.1):

- **Seamless integration:** Embedding AI tools into current systems used by MPs and parliament staff should follow a seamless integration approach that complements existing systems and tools and does not require extra platforms and their intrinsic learning burden. A gradual rollout of new assistive AI tools could also help achieve this goal and ensure user comfort during changes.
- **Explainable AI:** As a key enabler of successful AI assistance, every AI-driven action or suggestion must be accompanied by an explanation that can be easily understood by users (e.g. "email blocked due to detected malicious attachment"). Explainability not only increases trust in deployed AI solutions but also preserves transparency and soundness of parliamentary operations among political parties.
- **Data Sovereignty and Privacy:** Deployment of AI tools must ensure control of data sovereignty, taking into account the criticality and sensitive nature of information shared within and outside parliaments. Rigorous documentation of AI systems, testing in isolated environments before being put to production and self-hosted deployment options are the main factors contributing to secure data management and privacy preservation.

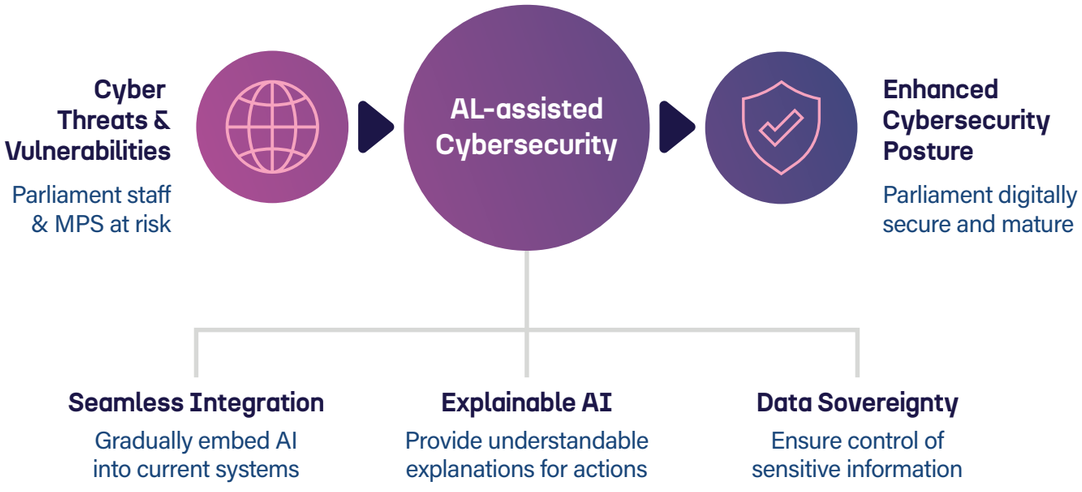
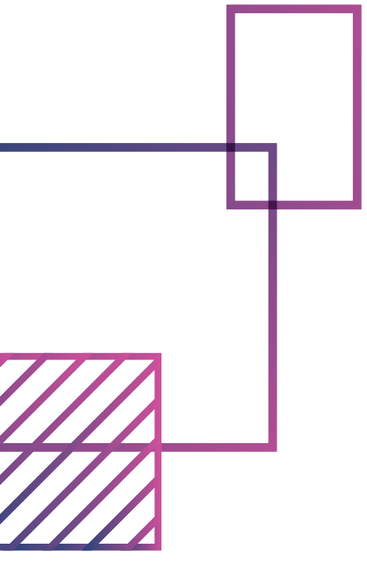


Figure 9.1: Transition to AI-assisted cybersecurity (source: Leonidas Kallipolitis)

Human judgement must be enhanced rather than be replaced by AI tools so as to help parliaments gradually strengthen their cybersecurity posture and increase their resilience to cyber threats without jeopardising transparency and trust by the involved parties and the general public. The latter is also increasingly using AI to craft their communications to the politicians, which could result in a future of AI-to-AI interactions of increasing length and sophistication with dubious outcomes and unpredictable repercussions for democratic dialogue and public scrutiny. Developing an implementation roadmap based on the mentioned principles could serve as a structured approach towards AI-powered cybersecurity in parliaments. The overall goals must be to ensure transparency, accountability, and preservation of a human-in-the-loop approach in parliamentary activities so as to safeguard social and political stability.



Conclusion

AI is rapidly reshaping the technological foundations of parliamentary work, offering unprecedented opportunities for efficiency, accessibility, and analytical power. From automating research and summarising debates to assisting with cybersecurity monitoring, AI has the potential to significantly enhance democratic processes and strengthen institutional resilience. Yet, as this chapter has demonstrated, these benefits come with profound risks that parliaments must confront with foresight, governance, and ethical clarity.

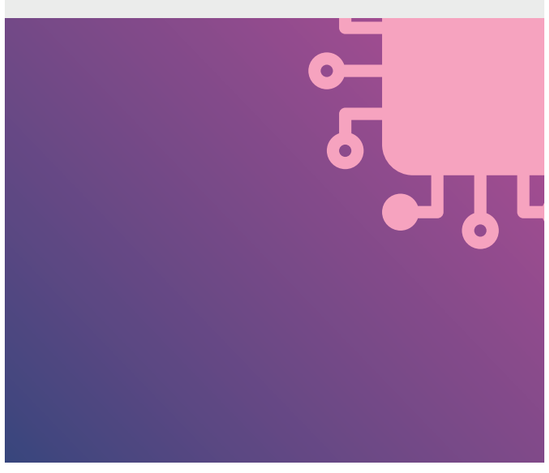
The vulnerabilities inherent in contemporary AI systems – prompt injection, data leakage, model poisoning, supply-chain exploits, and the broader class of threats captured in the OWASP Top 10 for LLM Applications – highlight that AI systems are not neutral helpers but complex digital infrastructures that can be manipulated in harmful ways. Agentic AI, with its autonomous decision-making capabilities, compounds these risks by introducing new pathways for goal hijacking, memory poisoning, privilege escalation, impersonation, and subtle forms of human manipulation. In an institution where decisions shape national policy and democratic legitimacy, such vulnerabilities translate directly into risks for public trust, institutional integrity, and even national security.

At the same time, AI is becoming a powerful accelerant for traditional cyber-attacks. Deepfakes, voice cloning, and AI-generated phishing campaigns are already being used to mislead the public, impersonate political figures, and compromise critical communication channels. Real-world incidents involving elected officials demonstrate how easily synthetic media can distort political narratives, sow confusion, and erode trust in democratic institutions. These threats underscore that AI is not only an operational challenge but a societal one, reshaping the information environment in which legislatures operate.

Despite these challenges, AI-enabled cybersecurity tools offer significant opportunities for parliaments seeking to strengthen their defensive posture. Machine-assisted vulnerability discovery, adaptive threat detection, automated patch management, and behavioural analytics can dramatically increase situational awareness and response capacity. Especially in parliamentary environments, where technical teams are small, heterogeneous device ecosystems are hard to standardise, and political workflows cannot be easily interrupted. When thoughtfully deployed, these tools can raise cybersecurity maturity without imposing additional burdens on MPs or staff, preserving the usability and accessibility of digital systems while increasing protection.

To harness the benefits of AI while mitigating its risks, parliaments must establish a principled implementation roadmap rooted in transparency, accountability, data sovereignty, and human-in-the-loop decision-making. AI systems must integrate seamlessly into existing tools, provide clear and understandable explanations for their actions, and operate under strict controls that safeguard sensitive legislative data. Moreover, these systems must be designed to support – not replace – human judgement, ensuring that political decision-making remains grounded in democratic accountability rather than automated inference.

In sum, AI represents both a transformative opportunity and a strategic challenge for parliamentary cybersecurity. Its adoption must be deliberate, ethically informed, and aligned with the values that underpin democratic governance. By combining robust security practices, adaptive governance frameworks, and careful technical implementation, parliaments can build an AI-assisted cybersecurity posture that enhances resilience, protects institutional integrity, and strengthens the democratic processes they exist to uphold.



Chapter 10

Information security

Author: Leonidas Kallipolitis

Introduction

Information security refers to all measures and policies applied to protect sensitive information in printed, electronic, or any other form, from unauthorised access, use, disruption, alteration, or disclosure. This concept is often referred to as safeguarding the "CIA Triad", i.e. confidentiality, integrity, and availability of information. The application of an information security policy ensures an organisation's operational capacity to achieve its business objectives, strengthens the trustworthiness of its processes and business offerings, and increases its resilience against threats and unforeseen incidents that can disrupt operations. Based on a well-defined governance and risk-management process (Chapter 5), all information of an organisation (existing and newly created) must be initially identified, categorised, and classified. This helps determine its importance to the organisation so the appropriate protective measures can be taken, whether organisational, technical, or physical. Common protection mechanisms are based on establishing multiple layers of security controls, abstracting or hiding critical information, and using encryption. It is, however, important to ensure that applied measures do not burden daily operations or jeopardise transparency of activities, especially in a parliamentary context where not only is information security important for the organisation itself but it can also influence wider national and societal aspects. The following paragraphs present best practices and key considerations that must be taken into account by parliamentary bodies for effective protection of sensitive information.

Parliamentary information and sensitivity

Parliamentary data includes a wide range of information that covers legislative work, political and party-related information, and internal parliamentary administrative and operational information, as well as citizen-originated data. Even though openness and transparency are key safeguards of democratic processes and public scrutiny, the protection of sensitive information managed within parliaments is of utmost importance. Examples of such information include:

- **Draft bills and supporting material** – such as expert reports, stakeholder opinions, scientific studies, and even internal government or party notes – whose leakage or tampering could reveal negotiation positions, subtly inject malformed clauses into new bills, or manipulate public polls or the results of scientific reports.
- **Internal communications** between MPs, committees, and party members through notes, memos, or electronic communications, which could disclose strategic information, leading to public misinformation, political scandals, and ill-formed communications with external stakeholders.
- **Personal data of citizens** and other public stakeholders issuing questions or complaints to parliament members. Exposing such information would be a violation of personal information protections regulations like the European Union's GDPR[108].
- **Administrative data** and operational information handled within parliamentary environments such as personnel and external contractors' data, IT infrastructure status and logs, security clearances, and access records. This data is susceptible to insider threats and supply chain attacks that can offer an entry point for more impactful attacks, as mentioned in the points above.

However, apart from sensitive information handled within parliaments, lots of data generated during a legislature's operations contain public information that is important for ensuring transparency of activities and accountability of MPs and the parliamentary institutions as a whole. Legislative procedures, voting results, minutes of plenary sessions, transcripts of speeches, parliamentary questions and reports, MPs' activities, committees' composition and session proceedings, and general text, audio, and video archives constitute information that should be easily accessible to the general public. Prominent ways of exposing such information are open data portals like the European Parliament's open data portal[109], the United States' open data site[110], and the UK's House of Commons Library[111].

Balancing transparency with security is therefore a core challenge. Leaked sensitive information might be valuable to hackers, foreign governments, hacktivists, or other threat actors that can use the leaked information to disrupt national operations, interfere with societal or governmental mechanisms, or even lead to life threatening actions. Taking into account these risks, parliaments should be governed by a data management framework which will identify, classify, and protect sensitive information without compromising effectiveness of parliamentary services.

Data access control and cryptography

Setting up a data access control mechanism is a step of paramount importance for an effective information security policy. In a parliamentary context, where flexibility, user autonomy, and distributed control are common requirements, the main access control models used are role-based access control (RBAC) and discretionary access control (DAC). RBAC is based on the definition of roles that have access to specified resources and data, in accordance with their role and duties. It is suitable for dynamic environments with frequent personnel changes, such as parliaments, because administrators can easily grant multiple permissions simply by adding a new user into the appropriate role. Therefore, newly appointed staff members, MPs, and other members can assume responsibilities in an easy and controlled manner. In parallel, DAC allows owners of special or private information to specifically define access to this information, for example a temporal committee chair might provide access to the committee's portfolio only to the assigned committee members. Both of these methods rely on well-defined roles and responsibilities, accompanied by documented permissions and processes for role assignments, as well as for role revocations. A key goal of these access control measures is to allow the required flexibility for a frequently changing parliamentary user base, while ensuring that the "least privilege" (only having the minimum level of permissions required to perform one's duties) principle is applied.

It is worth noting that mandatory access control (MAC) is another model used for highly sensitive data, for which access must be managed with the highest strictness due to the nature of the protected data for the state or national security. It is mostly used in restricted environments like military premises but might also be applied in information generated by a parliamentary service (e.g. national security information or critical infrastructure controls). Top Secret, Secret, and Confidential are commonly used classifications of data managed under a MAC system.

Having defined the access control system of managed data, parliament authorities can then define mechanisms to protect data confidentiality, integrity, and availability (CIA triad).

- Confidentiality refers to privacy preservation of sensitive information when stored or transmitted across a communication network, i.e. preventing unauthorised reading of stored information or stealing information while it is being sent to another system.
- Integrity ensures that data is not modified without authorisation. Original data should remain exactly the same whenever accessed, i.e. after being stored at a permanent storage location or when transmitted between two systems.
- Availability refers to timely, uninterrupted access to information items by authorised subjects, i.e. authorised users or systems should be able to access data whenever they request it.

Cryptography is the key enabler of effective implementation of the CIA principles. Cryptographic techniques aim at obfuscating or coding data in a complex way that ensures that only authorised users can access their original form. This process is based on the use of encryption algorithms (mathematical processes) that scramble data based on cryptographic keys whose owner is the only person (or system) able to decrypt and read it. Encryption of data stored or transmitted converts real data to unreadable "ciphertext" and ensures confidentiality. For example, classified information exchanged between MPs during the negotiation phase of a new bill via the parliament's internal Wi-Fi network is protected from malicious interception when transmitted encrypted since interceptors would not be able to read it even if they managed to get access to it. Similarly, digital signatures, a concept based on cryptographic technologies (e.g. hash functions), ensure data integrity by verifying that exchanged electronic documents have not been changed while in transit, ensuring the integrity and authenticity of, for instance, electronically signed legislative drafts. Availability is also ensured by cryptography, primarily via its role in implementing secure authentication mechanisms and indirectly through making sure that encrypted backups of data are safely stored and protected from threat factors so that they can be used to restore availability after disruptive events (cyber-attacks, system failures, or other threats).

A major consideration for the successful implementation of cryptography towards CIA preservation is the effective cryptographic key management. The keys must be kept secure and access to them should be logged so as to ensure accountability (i.e. knowing who accessed a key can identify potential leaks derived from the key's usage). Best practices in key managements include physical protection of the keys, storage in a place different from the one in which the encrypted data resides, and enforcement of split knowledge, i.e. separation of a key in parts and distribution in different individuals so that collaboration of all parties is required in order to recreate and use the key. In parliaments, people who have knowledge of important keys might change more frequently than in other organisations. Therefore, keys must be changed and all encrypted materials must be re-encrypted with the new keys when these individuals are called off their duties.

Relying on professional and scientifically sound implementation of cryptographic concepts is critical for guaranteeing the effectiveness of cryptography in safeguarding information. Therefore, cryptographic strategies applied to protect parliamentary data and processes must adhere to modern standards, best practices, and guidelines and be continuously monitored and revised to stay up to date with technological developments and scientific breakthroughs. Main references for the requirements of sound cryptographic controls and relevant security measures are published by NIST[112], ENISA[113], OWASP[114], and Center for Internet Security (CIS)[115]. Based on these, parliaments should develop policies and minimum requirements covering:

- Approved cryptographic software and hardware to be used by staff and MPs
- Standardised cryptographic algorithms to encrypt sensitive data
- Secure generation, storage, and management of cryptographic keys
- Encrypted communication protocols for information exchange
- Encryption requirements/settings for storage media (databases, PCs/laptops, mobile phones, portable storage devices, etc.)

Post-quantum cryptography

One of the biggest challenges dictating regular assessments and updates of cryptographic strategies is the expected leap in quantum computing and its implications on cryptographic technologies. The availability of large-scale quantum computers would pose a serious threat to most of the currently deployed cryptographic systems which could have their keys broken, resulting in serious compromise of the integrity and confidentiality of protected information. This can be possible because of the totally different laws of physics that apply to quantum computers (quantum mechanics) which enable them to perform rapid parallel computations in unimaginable speed when compared with current typical computers.

Cryptography in use nowadays (primarily based on symmetric/asymmetric encryption algorithms) relies on the assumption that the problem of calculating the used cryptographic keys requires an extremely long time to solve, therefore the protected systems are practically unbreakable. Quantum algorithms can, however, solve some of these (mathematical) problems in a short time, thus severely challenging the latter assumption. "Any information that has been encrypted, or will be encrypted using many of the industry's state-of-the-art cryptosystems based on computational hardness, is now under threat of both eavesdropping and attack by future adversaries who have access to quantum computation"[116].

To address this challenge, post-quantum cryptography (PQC) schemes are currently under research in order to provide quantum-resistant cryptographic algorithms and pathways of integrating them with current digital equipment and IT systems. Notable results of this work are the approved NIST standards for PQC[117], which include a quantum-resistant cryptographic scheme for general encryption and three algorithms for digital signatures.

Preparing digital parliament environments for this future threat must be considered carefully, due to the nature of parliamentary sensitive data whose confidentiality may need to be preserved for decades. Adversaries could already be collecting encrypted data today and keeping it in the hope of decrypting it when quantum computers become available.

Therefore, a PQC adoption roadmap must be pursued by parliaments and relevant institutions so as to put in place future-proof data protection mechanisms. Regulations like the Cyber Resilience Act[118] and Quantum Computing Cybersecurity Preparedness Act[119] push forward the design of such a roadmap for national authorities and should be closely monitored for the emerging standards and implementation acts.

Conclusion

Information security remains a foundational pillar of parliamentary resilience, shaping how legislatures protect the confidentiality, integrity, and availability of the data that underpins democratic processes. As this chapter demonstrates, safeguarding parliamentary information is not a purely technical exercise but a multidimensional responsibility deeply connected to constitutional duties, national security, and public trust. The diversity of parliamentary data – from draft legislation and sensitive political communications to personal citizen records and administrative information – requires tailored protections that balance openness with security. Achieving this balance depends on effective information classification, structured governance, and the consistent application of mature security controls.

Robust access-control models – RBAC, DAC, and in some cases MAC – ensure that information is accessible only to those with a legitimate need to know, helping parliaments maintain flexibility in dynamic environments while supporting the principle of least privilege. Cryptography strengthens these controls by enabling secure communication, ensuring document integrity, and supporting availability through securely stored, encrypted backups. Yet cryptographic protections are only as strong as the governance surrounding key management. The rapid turnover of parliamentary personnel means that key lifecycle management, auditability, and adherence to established standards from organisations such as NIST, ENISA, OWASP, and CIS are essential for maintaining security across time and institutional change.

At the same time, the chapter highlights the growing importance of preparing for a post-quantum future. Quantum computing threatens to break many of today's widely used cryptographic algorithms, potentially exposing sensitive parliamentary archives that must remain confidential for decades. Because adversaries may already be collecting encrypted material for future decryption, parliaments must act proactively by monitoring emerging standards, such as NIST's post-quantum cryptography schemes, and by developing transition roadmaps aligned with regulatory requirements like the Cyber Resilience Act and the Quantum Computing Cybersecurity Preparedness Act.

Ultimately, effective information security in a parliamentary context requires more than technical safeguards: it demands institutional alignment, continuous evaluation, and a culture that recognises the centrality of secure information flows to democratic integrity. By embedding classification frameworks, strong access control, cryptographic best practices, and forward-looking strategies into their governance structures, parliaments can ensure that sensitive information remains protected, public transparency is preserved, and trust in democratic institutions is upheld

Chapter 11

Technological and political transition

Author: Vasilios Alexiou

Introduction

Political transitions generate heightened cybersecurity risks that directly affect the continuity, legitimacy, and resilience of democratic governance, making them a core concern for parliaments. During periods of leadership change, elections, and crises such as wars, coups, or large-scale natural disasters, vulnerabilities in critical infrastructure, electoral management systems, parliamentary ICT networks, and emergency response mechanisms are more easily exploited by hostile state and non-state actors, including through hybrid and disinformation operations. Within this context, parliaments bear responsibility for providing strategic oversight of the security sector, updating legal frameworks, and ensuring that cyber resilience requirements extend to electoral technologies, critical infrastructure operators, and public administration so that democratic processes remain secure, transparent, and trusted under stress. This analysis is therefore positioned as a contribution to parliamentary debate and committee scrutiny on how legislative, budgetary, and oversight tools can be used to harden national cyber defences and electoral integrity specifically during politically sensitive transitions and emergencies.

Cybersecurity during political shifts

Cybersecurity during political shifts must be understood as a core dimension of parliamentary stability and democratic continuity rather than a purely technical concern of the executive branch. Periods of electoral change, government formation, or leadership crisis expose parliaments to a combination of cyber, physical, and information threats that can disrupt legislative work, compromise sensitive data, and erode public trust in representative institutions [120, 121].

When parliamentary composition changes after elections, the arrival of new members and staff, combined with the departure of others, can create a fluid environment in which access rights, information flows, and informal communication practices are in flux. If accounts are not deactivated promptly, devices are not properly reassigned, or working materials are moved to personal storage, the institution faces heightened risks of accidental data loss, intentional leaks, or unauthorised access by former insiders. At the same time, external adversaries frequently exploit the confusion of a political transition to launch targeted phishing campaigns, distribute malicious attachments masquerading as official instructions, or attempt to compromise parliamentary email and collaboration platforms. For these reasons, parliamentary administrations need clearly defined processes for identity and access management at the moment of transition, strict guidance on document archiving and handover, and reliable, verified communication channels through which leadership and services can contact members without creating further attack surface [120, 121, 122, 123].

In parallel, episodes of protest, constitutional tension, or broader regime crisis expose parliaments to more overt forms of digital confrontation, frequently crossing the boundary between cyber operations and political contention. Hacktivist collectives, politically motivated groups, or foreign actors may treat parliamentary websites, streaming services, and information portals as symbolic targets, seeking to deface pages, interrupt

broadcasts, or publish stolen correspondence to discredit the institution. In highly polarised contexts, information interference and disinformation campaigns can fabricate statements attributed to parliamentary figures, misrepresent voting outcomes, or manipulate clips of debates to deepen mistrust, making it harder for citizens to distinguish authentic parliamentary communication from forgeries. To remain functional under such pressure, parliaments require crisis-ready incident management structures, technical capacity to maintain essential digital services, and a communication strategy that uses authenticated online channels to provide timely, accurate information about sittings, decisions, and institutional positions [120, 121, 124, 125].

The broader governance role of parliaments during political shifts extends beyond the protection of their own networks to the shaping of national cyber resilience frameworks and election-related safeguards. Through legislation, budgetary authority, and oversight of the security sector, parliamentarians influence how states implement instruments such as the Network and Information Systems Directive, cyber-resilience legislation, and sectoral security strategies that determine the minimum level of protection for critical services and electoral infrastructure. Committees responsible for security, digital affairs, and constitutional matters can use hearings, inquiries, and reporting requirements to scrutinise how governments manage cyber threats during transitions, ensuring that emergency measures remain proportionate, transparent, and compatible with human rights obligations. In this sense, strengthening parliamentary cyber security during periods of political change is inseparable from reinforcing its capacity to exercise informed, independent oversight over the wider security architecture of the state [126, 127, 128, 129, 130].

In the United Kingdom, the Westminster parliament suffered a sustained cyber-attack in June 2017 that targeted parliamentary email accounts and forced the temporary suspension of remote access for MPs and staff. Up to 90 accounts were compromised in a brute-force campaign that exploited weak passwords, demonstrating how relatively basic tradecraft can have significant consequences in a high-profile democratic institution and prompting closer cooperation with the National Cyber Security Centre (NCSC) and a tightening of access-control practices. The episode neatly illustrates how adversaries can use a period of intense political scrutiny – post-election, amid Brexit debates, and with heightened media attention – to test parliamentary defences, probe for weak accounts, and potentially collect material that could be used for blackmail, disinformation, or strategic leaking [131].

More recently, New Zealand publicly attributed a breach of its parliamentary network to a Chinese state-sponsored group known as APT40, with the intrusion traced back to 2021 but only later discussed in coordinated international statements. The NCSC reported that the attackers had infiltrated computers associated with the parliamentary network, necessitating extensive mitigation support and broader guidance to connected organisations. The disclosure coincided with allied announcements about campaigns targeting lawmakers, voters, and critics in several democracies, and illustrates how parliamentary systems become focal points not only for domestic protest or hacktivism but also for long-running espionage efforts that seek to harvest political intelligence, shape decision-making, or intimidate vocal parliamentarians [132].

Continuity of operations during leadership change

Continuity of cybersecurity operations during leadership change is vital for parliaments, because any gap in protection or oversight can be exploited precisely when political attention and external pressure are highest. After the 2024 US election, for example, federal election-security assistance was abruptly frozen and past support activities were placed under review, creating uncertainty for state and local officials and signalling to adversaries that established protections were in flux. A similar effect can occur when a new Speaker takes office or when key committee chairs and party leaders change in a parliament that lacks robust continuity arrangements [133].

Concretely, parliamentary continuity means that core cyber functions – identity and access management, incident monitoring, backups, and secure communications – are anchored in institutional procedures, not in the preferences of individual officeholders. When a new legislature convenes, departing members and staff must lose access to email, document systems, and committee platforms in a controlled, time-bound way, while newcomers are onboarded through secure channels rather than improvising with personal accounts and consumer messaging apps. Regular, mandatory cyber briefings for incoming members and senior staff, combined with written handover notes and maintained contact with national cyber agencies, help ensure that knowledge about ongoing threats and protective measures is transferred rather than reset [133].

In Germany, the 2015 attack on the Bundestag severely compromised the internal parliamentary network, with attackers linked to the Russian group APT28 gaining administrative access and exfiltrating large volumes of data over an extended period. The breach was so deep that parts of the network reportedly had to be rebuilt, and it prompted a long-term overhaul of security practices and closer integration between parliamentary IT services and federal cyber authorities, showing how a legislature can be forced into expensive, disruptive remediation when its defences are not resilient enough to withstand a strategic intrusion [134].

Italy has also seen parliamentarians drawn into broader cyber and espionage campaigns. A 2024–2025 investigation into a Chinese-linked hacking operation revealed that members of the Italian Parliament, including a senator sitting on the intelligence oversight committee, were among those targeted in a large-scale email operation associated with an APT31 campaign directed at politicians and officials across several countries. Italian MPs publicly warned that such targeting strikes at their freedom to exercise parliamentary prerogatives, and the affair fed into ongoing debates in Rome about national cyber defences, foreign interference, and the role of oversight bodies such as the parliamentary committee for the security of the republic (COPASIR) [135].

Mitigating risks in election-related technologies

Mitigating risks in election-related technologies is a direct concern for parliaments because their composition, legitimacy, and internal decision-making increasingly depend on digital systems that can be targeted by hostile actors. These technologies no longer consist only of voter registration databases and ballot-tabulation systems run by electoral authorities, but also include parliamentary election portals, internal electronic voting platforms for plenary and committee sessions, candidate nomination and disclosure systems, and official parliamentary websites used to communicate results and procedures to

citizens and the media. When any of these systems are compromised or portrayed as unreliable, the credibility of parliamentary mandates and of day-to-day legislative decisions is called into question[136].

Even where parliaments do not administer national elections, they determine the legal and institutional framework in which election-related technologies operate and thus have an indirect but powerful cybersecurity role. Through legislation and budgetary control, parliaments set standards for the security and auditing of voting machines, the protection and logging of changes to voter registration databases, the transparency of digital result-reporting, and the obligations of electoral commissions to disclose and investigate incidents. In addition, they must secure their own internal systems used for electing Speakers and committee chairs, recording votes, and publishing outcomes. If internal electronic voting platforms are unstable or vulnerable to manipulation, particularly in closely divided chambers, the risk arises that key parliamentary decisions could be delayed, disputed, or delegitimised on technical grounds[137].

The Serbian case shows how weak governance around elections can spill over into questions about parliamentary legitimacy and the use of technologies underpinning elections. Observers, including the European Parliament, have criticised recent Serbian elections for problems such as manipulation of voter registration, breaches of the secrecy of the ballot, group voting, and use of state resources that create structural advantages for the ruling party, all within a context of concentrated media control and contested institutions. While the National Assembly does not formally run elections, its dominant majority and links to executive power have raised concerns that political actors around the Assembly can influence how voter lists, result aggregation, and communication systems are managed, blurring lines between impartial election administration and partisan control. Mitigating risk here requires a parliament that not only secures its own internal voting systems and information infrastructure but also insists – through independent oversight and clear statutory rules – on transparent, auditable, and professionally run election technologies at national level[138].

Other parliamentary examples underline the stakes. In the United States, Congress does not operate election infrastructure, yet the 2024 election cycle again featured attempts to attack or discredit election-related technologies, including distributed denial-of-service (DDoS) attacks on election websites, phishing against election officials, and narratives falsely alleging hacked voter information and compromised machines. Congressional committees have therefore focused on supporting federal and state authorities in hardening voter registration systems, public information portals, and result-reporting, while also examining platform regulation and foreign interference that can distort perceptions of election technology performance. At the European level, the European Parliament depends on national authorities to run European elections, but post-2024 analyses highlight cyber and information operations aimed at undermining trust in the electoral process, prompting calls for closer interagency collaboration, better exchange of threat intelligence, and harmonised security and transparency requirements across member states[136].

At European Union (EU) level, the 2024 European Parliament elections provide a further example of how election-related technologies and parliamentary interests intersect. Analyses of those elections highlight that EU institutions and member states faced a mix of cyber threats – such as DDoS attacks on politics-related websites, attempts to breach election-related organisations, and data-breach risks – as well as information operations including disinformation and AI-generated content intended to distort voter perceptions. An earlier European Court of Auditors report and subsequent internal reviews found that cybersecurity across EU institutions, including the European Parliament, had not yet reached the level required by the evolving threat environment, prompting new regulations to raise cyber maturity and specific, election-focused cooperation through the European Cooperation Network on Elections and ENISA-supported exercises. These experiences show that securing election-related technologies requires parliaments to support interagency collaboration, to insist on timely implementation of EU-wide cybersecurity rules, and to improve their own institutional defences against both technical attacks and election-linked information operations[139].

For parliaments themselves, mitigating risks around election-related technologies means combining technical, procedural, and organisational measures. Their own voting and election systems need regular security assessments, secure development and maintenance, and clear procedures for fallback and verification in case of malfunction or attack. Parliamentary administrations must maintain robust access controls, logging, backups, and incident-response plans specifically for internal election and voting platforms, while leadership ensures that cyber risk does not fluctuate with political turnover. At the same time, parliaments should leverage their legislative and oversight powers to require strong cybersecurity standards, independent testing, and transparent reporting for the wider electoral technologies on which their legitimacy depends, and participate in international exchanges of best practice and threat intelligence to anticipate and respond to emerging threats to democratic processes[140].

Cybersecurity risks in emergencies

Cybersecurity risks in emergencies intensify for parliaments because crises force them to legislate, oversee the executive, and communicate with the public while relying heavily on stressed digital systems. Wars, military coups, and large-scale natural disasters create windows in which hostile states, cybercriminals, and opportunistic actors can target parliamentary networks, remote-working tools, and public-facing communication channels to disrupt oversight, steal sensitive information, or undermine confidence in democratic governance.

Emergencies change how parliaments work. Sessions are rescheduled, special procedures are activated, and remote or hybrid arrangements often replace normal in-person deliberation, increasing reliance on email, videoconferencing, remote voting tools, and cloud platforms. Under these conditions, security controls are more likely to be relaxed or improvised: personal devices and home networks become part of the attack surface, rapid deployments of new tools may bypass normal vetting, and staff are under pressure to privilege continuity of operations over careful risk assessment. Adversaries exploit this environment by launching phishing campaigns themed around the crisis, targeting unpatched remote-access services, and using disinformation to confuse or intimidate parliamentarians and the public[141].

The Norwegian Storting cyber incidents during the pandemic offer a concrete parliamentary example of these risks. In 2020, as the parliament adapted to increased remote and hybrid work, attackers breached email accounts belonging to MPs and staff,

stealing data and forcing the institution to disable accounts and work closely with national security authorities. Norwegian threat assessments later attributed the operation to the Russian-linked group commonly known as Fancy Bear (APT28), noting that the aim was to obtain sensitive information that could be used to influence individuals or political processes, including parliamentary elections. A second attack in early 2021 exploited a zero-day vulnerability in Microsoft Exchange, again affecting the Storting and demonstrating how globally exploited software flaws can intersect with emergency-driven remote-access arrangements to create acute institutional risk. These incidents occurred while the parliament was operating under pandemic conditions, with expanded remote connectivity and heavy reliance on digital communication, and they underscored the need for crisis-specific cyber controls such as mandatory multi-factor authentication, tighter network segmentation, enhanced monitoring, and targeted cyber-hygiene campaigns for remote workers [142].

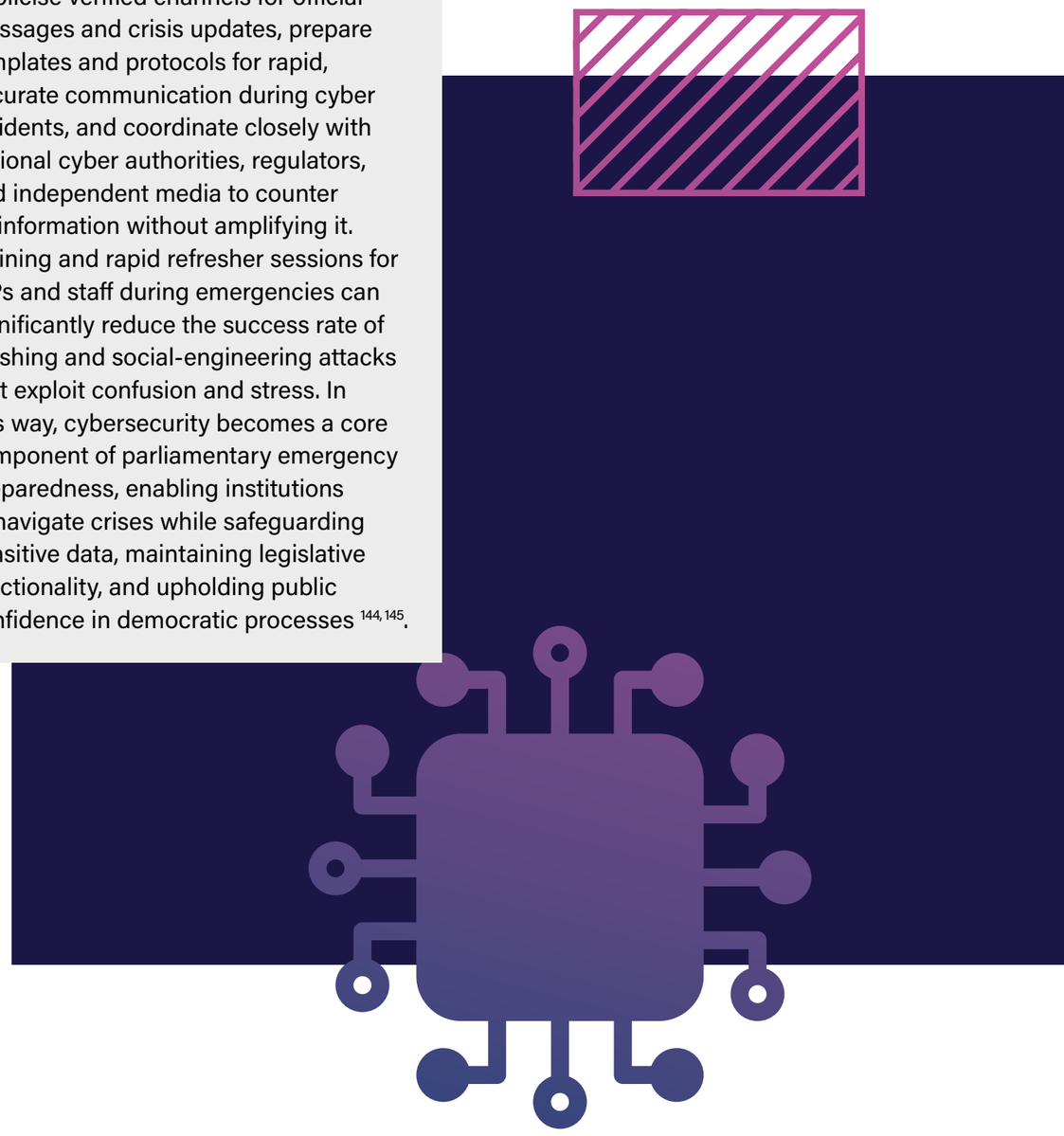
Emergency conditions accentuate several recurring categories of cyber risk. A first cluster involves remote work and access: rapid, large-scale deployment of teleworking tools without thorough configuration, combined with the extensive use of personal devices and untrusted networks by MPs and staff, increases the attack surface and the likelihood of compromise. A second cluster concerns phishing and social engineering, as attackers capitalise on fear and urgency to distribute fake emergency alerts, malware-laden updates, or messages impersonating parliamentary leadership or health and security authorities. A third problem is availability: parliamentary websites, streaming platforms, and communication portals may suffer DDoS or overload attacks during crisis debates or press conferences, limiting transparency and hindering public access to official information [141].

Data protection and access control also become more fragile. Under time pressure, sensitive legislative drafts, oversight documents, or citizen information may be shared via ad hoc channels, copied to personal cloud services, or handled by staff whose roles are not clearly defined, raising the likelihood of data breaches or unauthorised access. At the same time, information operations – ranging from false claims of hacked parliamentary systems to deepfake speeches and fabricated voting records – aim to undermine confidence in parliamentary crisis management and to polarise public opinion. All of these risks strike at the core of parliamentary functions: the integrity of deliberation and voting, the confidentiality of certain proceedings, and the credibility of official communication [143].

Conclusion

For parliaments, managing cybersecurity risks in emergencies is ultimately about embedding digital resilience into constitutional continuity. A resilient parliament is one that can continue to meet, deliberate, vote, and hold the executive to account even when crises force changes in location, format, or tempo of work. Achieving this requires tested business-continuity and disaster-recovery plans for core systems; secure remote-access architectures with strong authentication, endpoint protection, and clear device policies; and well-rehearsed incident-response procedures that are integrated into broader emergency governance structures rather than operating in isolation [144, 145].

Equally important is maintaining communication integrity and public trust. Parliaments should establish and publicise verified channels for official messages and crisis updates, prepare templates and protocols for rapid, accurate communication during cyber incidents, and coordinate closely with national cyber authorities, regulators, and independent media to counter disinformation without amplifying it. Training and rapid refresher sessions for MPs and staff during emergencies can significantly reduce the success rate of phishing and social-engineering attacks that exploit confusion and stress. In this way, cybersecurity becomes a core component of parliamentary emergency preparedness, enabling institutions to navigate crises while safeguarding sensitive data, maintaining legislative functionality, and upholding public confidence in democratic processes [144, 145].



< part IV >

...

// Implementation and strategic approaches

Chapter 12

Budgeting and resource allocation

Author: Hedi Touati

Introduction

The digital transformation of legislative work – hybrid sittings, online communication, remote offices, public engagement platforms – has created unprecedented dependency on information systems. This expanding digital footprint also exposes parliaments to increasingly sophisticated threats ranging from state-sponsored espionage to cyber-enabled disinformation [146, 147].

Parliaments have unique characteristics that influence their cybersecurity posture: independence from the executive, highly diverse users, transparency obligations, and budget cycles not always aligned with technological needs. Effective cybersecurity budgeting therefore requires strategic thinking rather than incremental spending.

Designing a cost-effective cybersecurity investment portfolio requires balancing strategic ambition, operational realities, and fiscal discipline. For parliaments – institutions with high security expectations but complex governance structures – the challenge is to allocate finite resources in a way that maximises security outcomes, reduces systemic risk, and preserves institutional trust.

Foundational principles for smart cybersecurity investment

Effective cybersecurity budgeting begins with understanding risks and aligning resources accordingly. International frameworks consistently emphasise risk-driven investment, ensuring that the systems whose compromise would disrupt parliamentary functions receive prioritised funding [148, 149].

Aligning with recognised frameworks (NIST CSF, ISO 27001, COBIT) helps ensure objective, consistent, and auditable decisions [150, 151]. These frameworks also help satisfy external oversight, demonstrating that investments follow international best practices.

A fundamental principle is recognising that cybersecurity operates as a continuous lifecycle. It requires sustained operational funding for monitoring, patching, licensing, and training. Underestimating these ongoing needs often leads to vulnerabilities and higher post-incident costs.

For parliaments, where public funding must be justified transparently, understanding the full cost trajectory of cloud and SaaS solutions is essential. They must plan for the steady increase in IT costs, especially as the industry's transition from capital expenditures to subscription-driven operational expenditures creates higher and more predictable recurring financial obligations. This shift requires more disciplined long-term budgeting and investment planning.

Parliaments should consider using even more shared or federated cybersecurity services, such as national CERT collaboration, shared security operations centre (SOC) models, or inter-parliamentary cooperation to improve cost-effectiveness [152].

Building a cost-effective cybersecurity investment portfolio

Cybersecurity spending has a direct impact on public trust. Demonstrating strategic alignment, transparency, and measurable improvement is essential to strengthen institutional credibility. Integrating cybersecurity early in digital transformation projects prevents expensive retrofits and ensures long-term sustainability.

To simplify budgeting, parliaments can structure their investments as a balanced and resilient portfolio focused on foundational hygiene, critical asset protection, and operational readiness.

Foundational hygiene includes high return on investment (ROI) controls such as multi-factor authentication, automated patching, endpoints detection and response platforms, secure configurations, phishing protection, and robust backup practices. These measures defend against most common threats and should precede more advanced tools[153].

Critical parliamentary assets – voting systems, chamber technologies, legislative workflows, and member communications – require a tiered protection model with stronger safeguards, including zero-trust principles and segmentation.

Operational capabilities, including continuous monitoring, threat intelligence, incident response, and crisis exercises, are essential for translating technology investments into real security outcomes. Opting for managed services can provide affordable access to specialised expertise that is difficult to build internally. A total cost of ownership approach helps identify the full economic impact of tools and avoid long-term financial pitfalls.

Procurement, efficiency, and cost stewardship relies on strategic procurement and efficient resource management. Consolidating the tools used by cyberoperation teams is a cost-effective approach for security solutions that drives both operational efficiency and stronger outcomes. A reduction of the number of tools not only cuts the cost of licensing in use but also streamlines workflows, minimises duplication, and enables analysts to focus more on proactive threat hunting with less false positive alerting to address.

Governance, culture, and human capability

A mature cybersecurity culture is equally an investment priority. Culture-building initiatives – communications, leadership engagement, targeted awareness campaigns – require sustained funding to be effective. Adequate budget allocation ensures that security messaging remains visible, consistent, and tailored to the unique environment of MPs and political staff, who operate with autonomy and varied digital habits. Underinvesting in culture introduces hidden costs: increased incident rates, human error, and greater reliance on technical controls that may not be uniformly adopted by all actors.

Human capability represents one of the highest-value investments a parliament can make. Skilled people amplify the impact of every technological tool and governance mechanism, and their absence can undermine even the most advanced systems. Cyber budgeting models increasingly recommend dedicating a distinct portion of the security budget to workforce development and capability building. This includes:

- **Skilling and upskilling** cybersecurity professionals to stay ahead of emerging threats and architectural changes.
- **Parliament-specific training** for MPs and political staff, whose behaviours and digital exposure pose unique risks.
- **Ongoing enterprise-wide awareness** programmes, which require recurrent funding for new content, simulations, micro-learnings, and targeted campaigns.
- **Investments in leadership** and crisis decision-making exercises, enabling executives and parliamentary authorities to respond confidently during breaches.
- **Funding for inter-institutional staff exchanges,** joint cyber training exercises, and red-team/blue-team simulations, which strengthen cross-jurisdictional resilience and bring external expertise into the parliamentary environment.

These human-centric investments produce some of the highest returns in cybersecurity: reduced incident likelihood, faster detection and containment, improved compliance, and a more adaptive, security-aware institutional culture.

When governance, culture, and human capability are treated as strategic investment categories – rather than ancillary activities – they become force multipliers for every other cybersecurity expenditure. A parliament that invests deliberately in these areas not only strengthens its defences but also builds a sustainable cybersecurity ecosystem capable of evolving with emerging threats, technologies, and political realities.

Encouraging innovation and responsible modernisation

Allocating a dedicated portion of the cybersecurity budget, typically 5% to 10%, to innovation is essential for keeping pace with a rapidly evolving threat landscape and an increasingly complex digital ecosystem. This investment allows cybersecurity teams to explore emerging technologies, experiment with modern architecture, and conduct controlled pilots that inform future transformation efforts without disrupting operational stability.

Conclusion

Cybersecurity budgeting in parliaments is not merely a technical exercise but a strategic responsibility essential to protecting democratic operations. By combining risk-based prioritisation, strong governance, human-centred investment, and balanced portfolios, parliaments can enhance resilience while maintaining fiscal responsibility. Sustainable portfolios should include multi-year financial planning aligned with strategic roadmaps, mechanisms to absorb cost increases due to emerging threats, lifecycle management for technologies and contracts, and clear governance decision making on investment trade-offs.

In addition, carving out a predictable budget for innovation and experimentation can be a strong signal that modernisation is not an occasional project but a sustained priority, encouraging cybersecurity teams to propose new ideas, embrace agile methods, and remain open to technological evolution.

Chapter 13

Creating and cultivating a security-conscious parliamentary culture

Authors: Hedi Touati,
Vasilis Tountopoulos

Introduction

Current cybersecurity frameworks and regulations (CSF 2.0, Network and Information Systems Directive, Cyber Resilience Act, etc.) aim at strengthening the adoption of strategic measures, towards enhancing the security of cyber ecosystems and fostering the resilience of systems, processes, and infrastructures. They also emphasise the role of the triple people, processes, and culture, as the success indicator for the realisation of cybersecurity risks in businesses and organisations, and the effective design and implementation of cybersecurity strategies[154].

A fundamental aspect of this triple is the human factor and the cultural and behavioural change of the parliaments' human resources to effectively tackle the cybersecurity challenges ahead. Specifically, the successful operation of secure and digitally transformed processes requires, among others, expertise in strategically defining security policies, understanding the social and economic (or even geopolitical) aspects of cybersecurity, and developing mechanisms for identifying, managing, and mitigating cyber risks. The latter can take the form of complementary approaches that can be progressively deployed across organisations and may range from implementing tactics and security measures to reduce these risks or transferring such risks to insurance and reinsurance organisations, through cyber insurance practices[155].

In a parliamentary institution, changing organisational behaviour is one of the most challenging yet rewarding ambitions a CISO can undertake. Unlike corporate or government departments, parliaments operate at the intersection of politics, autonomy, and public accountability. The CISO is expected not only to secure the institution but to do so in a way that respects constitutional privileges, the independence of elected members, and the openness that defines democratic governance. In such a context, a security-conscious culture cannot be imposed; it must be cultivated through organisational change management[156].

Leadership as a cultural catalyst

The starting point of this cultural transformation is leadership[157]. As previously described, in parliament, authority does not flow top-down but is shared across political and administrative domains. Therefore, cybersecurity must be seen as more than a technical function – it must be championed by political figures and senior officials who influence norms and expectations.

When the Speaker, parliamentary clerks, and party leadership publicly embrace secure practices, they signal that cybersecurity is not a constraint but a collective safeguard for democratic work. When they show active involvement in important cybersecurity events, such as Cyber Security Awareness Month or the European Cybersecurity Month in October (https://www.cybersecuritymonth.eu/), their engagement becomes a form of modelling; it legitimises secure behaviour and reduces the perception that security demands are arbitrary or overly bureaucratic.

The role of skills development on empowering humans in cybersecurity

The design, implementation, and assessment of cybersecurity practices must be the combined effort of interdisciplinary teams of experts at all levels of an organisation's hierarchy, like parliaments. Such experts should be able to demonstrate advanced skills in the adoption and the use of cybersecurity technologies, which entail specialised capabilities in further technological advances, like AI, machine learning, and blockchain, to securely operate the parliamentary digital processes within and across potentially hostile cyber environments. Such technologies strongly relate to the entire cybersecurity protection and incident-handling lifecycle that entails the efficient implementation of dynamic risk-management approaches, robust cybersecurity protection, incident analysis, and response mechanisms, and/or eventually risk-driven cyber insurance policies.

On the other hand, humans should be the ones held accountable for defining proper cybersecurity strategies for their organisations and ensuring the compliance of these strategies with legal frameworks, national and international strategies, and standards imposing specific security and certification requirements. Addressing such requirements implies responsibilities and obligations that humans must undertake in the context of an effective governance approach for the deployment of correct strategies. An effective cybersecurity culture must be integrated with structural support for security risk management where several people are jointly accountable for monitoring risks[158].

Therefore, as the human factor maintains a dominant position in the effective definition and implementation of cybersecurity strategies, it is essential that the adequacy of human resources must be enhanced. This shortage positions humans as the weakest pole in the triple of people, processes, and culture and slows the adoption of innovative ICT technologies that would accelerate digital transformation strategies within a secure and safe cyber ecosystem[159]. The deficit in human resources stems from the loose link in the current educational and vocational training programmes with market needs and standards, as well as the limited number of domain experts across sectors who can effectively leverage technology to advance traditional practices in the parliamentary processes.

The lack of cybersecurity talents and experts in parliaments relies on various social, economic, and educational factors, not least a lack of cybersecurity culture throughout the general public, which requires massive educational campaigns to address[160]. Primarily, as recent studies highlight, there is a significant global shortage of cybersecurity specialists who are anticipated to address the relevant market needs, not only for parliaments but also the whole European Union (EU) business ecosystem[161]. Similar studies reveal that only recently has this ecosystem given high priority to cybersecurity-related expenditure, including human resources[162]. Thus, if parliaments want to attract experts and young talent, they must invest adequate budget for them and eventually overcome the current budgeting restrictions that public bodies normally follow in the EU and worldwide.

Tailoring learning to parliamentary realities

However, leadership alone cannot reshape cultural habits that have formed over decades of analogue traditions and rapid digital improvisation. Parliamentarians and their staff occupy exceptionally diverse roles, each with different risk profiles, communication practices, and levels of digital fluency. A culture of security demands education that acknowledges these differences. Generic awareness campaigns are quickly dismissed as irrelevant; instead, tailored learning that reflects the daily realities of MPs, constituency assistants, party strategists, and committee clerks allows cybersecurity to be understood as personally useful, not institutionally imposed.

In parliaments, cybersecurity awareness also benefits from persistence rather than intensity. A single mandatory course will not change ingrained behaviours, nor will complex policy briefings. Cultural change emerges gradually through recurring signals: short micro-lessons, accessible case studies of breaches in other parliaments, timely reminders linked to real incidents, or brief videos shared before caucus or committee sessions. These small but steady interventions sustain awareness without overwhelming busy political actors. In this sense, cybersecurity communication must resemble public health campaigns, where repetition and relevance shape behaviour more effectively than enforcement.

Importantly, positive reinforcement is a more powerful engine of cultural change than punitive control. Because elected officials cannot be coerced into compliance in the same way as employees of a ministry, the parliament benefits from a model built on support, incentives, and convenience. When secure tools are easier to use than insecure ones, when training leads to prioritised access to certain services, or when offices are informally recognised for adopting good practices, security becomes a desirable experience rather than an imposed requirement. Culture shifts when secure behaviour becomes the path of least resistance.

A mature cultural shift also requires that the parliament regularly confront its vulnerabilities in realistic conditions. Tabletop exercises, crisis simulations, penetration testing assessments, and even cyber incident competitions can serve to do more than test systems, as they generate shared understanding across actors who normally work in silos[163]. When parliamentarians, staff, administrators, and technical teams experience a hypothetical breach together, they develop a shared vocabulary of risk and a clearer appreciation of their interdependence. Beyond training, such exercises strengthen trust – the rarest currency in cybersecurity governance.

Over time, these efforts build a fabric of shared responsibility. Measured through behavioural metrics, participation in learning initiatives, and observed attitudes toward new controls, culture gradually evolves from scepticism to engagement. The parliament becomes a community capable of balancing openness with protection, autonomy with accountability, and rapid communication with digital caution.

CASE STUDY

Canada: Building security culture in a politically sensitive environment

In recent years, the Parliament of Canada has faced heightened cybersecurity pressure driven by an increase in foreign interference, online misinformation, and attempts to infiltrate parliamentary communications. Although the Canadian government has long invested in cybersecurity, the parliamentary environment presented unique obstacles that could not be addressed through government-style compliance mechanisms.

A threat landscape shaped by foreign interference

Security agencies such as the Canadian Centre for Cyber Security (CCCS) and the Canadian Security Intelligence Service have repeatedly warned that Canadian political institutions remain a high-value target for hostile foreign actors. In 2021 and 2022, multiple advisories highlighted attempts to collect intelligence on MPs, compromise political staffers through spear-phishing, and influence public debate through covert digital campaigns.

Unlike a government department that can enforce mandatory compliance, the House of Commons could not simply compel MPs or their political staff to adopt new security protocols or technology configurations. Their constitutional autonomy created a significant cultural and governance challenge: how to secure the system without appearing to control elected representatives.

A collaborative shift toward cultural change

Faced with these pressures, Canada's parliamentary administration turned toward persuasion-based strategies rather than enforcement. Several phased initiatives gradually shifted culture:

- **Continuous targeted engagement** with party leadership, as well as administrative leadership, recognising that political incentives strongly influence behaviours
- **Security briefings tailored to MPs** and political aides, particularly on foreign interference, travel risks, and secure communication practices
- **Partnerships with CCCS**, enabling joint threat intelligence briefings and making security advice appear politically neutral
- **Adoption of secure communication platforms** promoted not as mandatory tools but as premium services for high-risk parliamentary actors.

These initiatives were presented not as restrictions but as enablers of political autonomy, protecting MPs from manipulation and safeguarding communication with constituents and caucus members.

Impact: Trust as a driver for adoption

Within two years of consistent messaging and targeted engagement, adoption of secure practices increased substantially. MPs relied more on official communication platforms, cyber incidents were reported more rapidly, and political offices began requesting security briefings proactively – an indicator of cultural maturity. During sensitive geopolitical crises, parliamentarians increasingly sought intelligence-informed guidance rather than circumventing institutional IT controls.

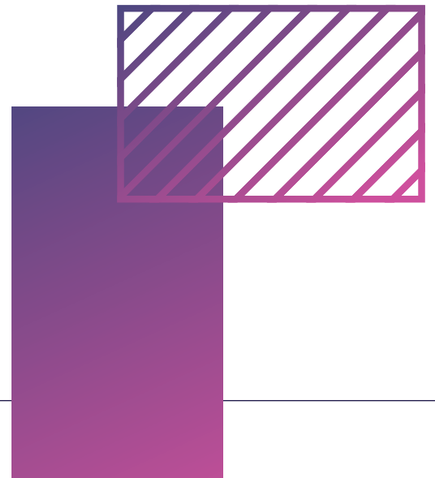
This shift demonstrated that trust, not authority, is the primary currency of cultural change in a parliamentary cybersecurity strategy. Canada's experience shows that when cybersecurity is framed as a protective service rather than a procedural burden, elected officials respond more positively and participate more willingly.

Conclusion

For the parliamentary CISO, shaping cybersecurity culture is neither linear nor quick. It is gradual work rooted in persuasion, credibility, and human-centred design. Trust becomes the quiet engine of this transformation: without it, even the most advanced protections will be circumvented or ignored; with it, secure practices are adopted willingly and even championed. Building trust takes time, but it is this slow work that delivers the most resilient outcomes.

A parliament that embraces secure behaviour voluntarily – not through coercion – creates a foundation of digital trust and institutional resilience. When elected officials and staff feel that security exists to protect their autonomy rather than limit it, cybersecurity becomes more than a technical shield; it becomes a shared responsibility and a democratic safeguard.

Ultimately, the security of parliamentary systems will be determined not only by firewalls or encryption but by the relationships, behaviours, and trust that guide how people use them. The future of parliamentary cybersecurity depends on the collective awareness and willingness of those who participate in the legislative process to protect the digital fabric on which modern democracy now depends. Strengthening the human factor is therefore not only a matter of staffing but a strategic imperative for ensuring cybersecurity resilience. This makes targeted training and awareness programmes the natural next step in addressing the skills gap and reinforcing the cybersecurity workforce[164].



Chapter 14

The creation and maintenance of cyber resilience networks

Author: Sean McSpaden

Introduction

It has often been said that cybersecurity is a "team sport", and that, as an enterprise, governments can only be as secure as their "weakest link". As the smallest of the three branches in a democratic form of government, the legislative branch often finds itself as the "weakest link", lacking sufficient financial resources and the requisite number of skilled professional staff, struggling to protect against and recover from a seeming onslaught of cyber-attacks. In thinking about cyber resilience, if these institutions remain isolated and attempt to identify, protect, detect, respond, and recover from cyber-attacks on their own, their efforts may fail outright, or be less effective than they otherwise could be if they chose instead to collaborate and band together with other community partners. If this alternative mindset and operating model is adopted, a shift from isolated defences to a collective, trusted, and adaptive ecosystem – a cyber resilience network – of parliaments, governments, and partners can take form and be strengthened over time.

Cybersecurity and cyber resilience are related and complimentary terms but have some important differences that warrant exploration (Figure 14.1). Cybersecurity, on the one hand, is like locking your doors and installing an alarm system in your home. NIST defines cybersecurity as "the prevention of damage to, unauthorized use of, exploitation of, and (if needed) the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems"[165]. It follows that the focus of cybersecurity is on prevention and protection – to stop cyber-attacks, data breaches, and unauthorised access to networks or use of information systems from occurring.

Cyber resilience, on the other hand, is like relying on those basic protections but augmenting them by adding property/casualty insurance, an emergency readiness/action plan, and the ability to repair or rebuild quickly if someone breaks in or your home is damaged or destroyed. NIST defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment"[166]. The focus of cyber resilience is on continuity of operations and adaptability to ensure that essential organisational functions and services continue during and following an attack, even when cyber defences fail. Cyber resilience builds on cybersecurity but adds business continuity, crisis management, redundancy, rapid recovery, and lessons learned from incidents over time. In adopting a cyber resilience mindset, an organisation assumes a data breach or successful cyber-attack will occur and takes steps to ensure it can keep operating during the incident and bounce back stronger and more resilient in the aftermath.

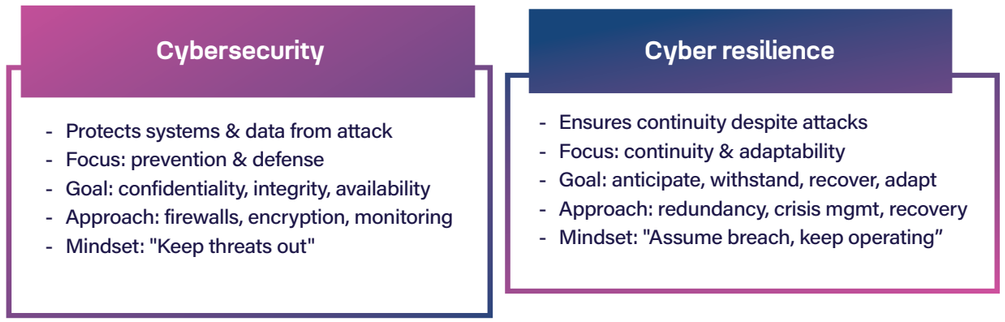


Figure 14.1: Cybersecurity vs cyber resilience (source: Sean McSpaden)

Cyber resilience network

A cyber resilience network could well be defined as a structured ecosystem of organisations, institutions, and stakeholders that work together to ensure the government's ability to anticipate, withstand, recover from, and adapt to cyber incidents. Alternatively, it could be defined as a trusted, multi-stakeholder community that links governance institutions, parliaments, academia, and private sector/third parties, designed to share information, coordinate responses, and ensure the resilience of legislative and governmental systems against cyber threats. Using either potential definition, an effective and sustainable cyber resilience network for legislatures and parliaments:

1. Creates a clear framework for governance (includes protocols for consultation, collaboration, coordination, information sharing, and mutual aid across the network)
2. Coordinates across jurisdictional and sector boundaries (domestically and/or internationally: government to government, government to critical infrastructure provider, government to academia, government to organisational and trade associations, etc.)
3. Engages trusted third parties via public, private, and non-profit sector partnerships
4. Collects, analyses, and shares information (vulnerabilities, incidents, lessons learned, etc.) safely and securely as authorised by the governance framework
5. Shares best practice advice and tools for maintaining operational readiness
6. Works to ensure continuity and adaptive recovery capabilities exist across the network

Information sharing among and between members of the cyber resilience network will necessarily involve the establishment of an interconnected system of formalised processes and secure platforms that enables government institutions (executive, legislative, judiciary, independent commissions) and their public, non-profit, academic, and private-sector partners to exchange cyber threat intelligence, vulnerabilities, and incident reports in real time, while preserving confidentiality and accountability as required by law, regulation, contract, or some other form of agreement. And the importance of identifying and cultivating mutually beneficial relationships, and the formation of public-private partnerships with trusted third parties, that provide anonymisation, threat brokering, technical services, and trust building between otherwise competing or siloed organisations and sectors cannot be overstated.

As NIST aptly stated in its Guide to Cyber Threat Information Sharing, when using "shared resources, organisations can enhance their security posture by leveraging the knowledge, experience, and capabilities of their partners in a proactive way. Allowing 'one organisation's detection to become another's prevention' is a powerful paradigm that can advance the overall security of organisations that actively share threat information.... Cyber defense is most effective when organisations work together to deter and defend against well-organised, capable actors"[167]. This kind of collaboration helps to reduce overall risk, enable shared situational awareness, accelerate maturation of knowledge and expertise, improve security posture, and engender greater defensive agility and resilience of members of the network.

Within the United States and the European Union (EU) this kind of information sharing has been facilitated through information-sharing and analysis centres (ISACs). ENISA defines ISACs as "non-profit, trusted hubs designed to improve cybersecurity resilience across critical sectors by enabling the collection, analysis, and secure exchange of threat information between public and private stakeholders. Supported by the Network and Information Systems Directive, ISACs help operationalise incident reporting and foster proactive, coordinated responses to cyber threats"[168].

In the United States, the most well-known ISAC is housed within a non-profit organisation called the Center for Internet Security (CIS)[169]. For the past 25 years, CIS has been the home of the Multi-State Information Sharing and Analysis Center (MS-ISAC), which serves as a trusted resource for cyber threat prevention, protection, response, and recovery for US Government entities. The mission of MS-ISAC is to "improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organisations through coordination, collaboration, cooperation, and increased communication"[170].

In the United States, there is not yet a single, institutionalised legislature-to-legislature cyber resilience network like CERT-EU in Europe[171]. Instead, legislatures (the US Congress, state legislatures, and territorial legislatures) participate in several overlapping federal, state, and multi-stakeholder networks that together form the basis of cyber resilience for legislative bodies.

The US Congress maintains separate information technology offices in the House and Senate and its own cyber resilience structures but participates in broader national efforts via the US Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA)[172] and CISA's Joint Cyber Defense Collaborative[173].

For US state and territorial legislatures, the natural points of coordination and collaboration occur through the National Conference of State Legislatures' (NCSL) Task Force on Artificial Intelligence, Cybersecurity and Privacy (policy and governance); the NCSL National Association of Legislative Information Technology (NALIT) (peer-to-peer IT/cybersecurity information sharing and collaboration); and MS-ISAC (state, local, tribal, territorial (SLTT), and federal threat intelligence, information sharing, and cybersecurity assessment and service delivery hub). Those organisations and a sample set of US state and regional public-private partnerships are described in more detail on the next page:

NCSL – Task Force on AI, Cybersecurity and Privacy[174]	
Scope:	National, 50+ state/territorial legislatures engaged.
Focus:	AI, cybersecurity, and data privacy.
Why it matters:	Provides a forum within which elected members of state legislatures, professional staff, and trusted third parties (public, private, and non-profit) can engage in policy discussions, explore and develop best practice guidance, and create educational work products on AI, cybersecurity, and privacy issues.
Notable work:	Budgeting for Cybersecurity (2018)[175]; AI Toolkit (2025)[176]; Tracking of state and territory legislation on AI, cybersecurity, and privacy.

NCSL – National Association of Legislative IT (NALIT)[177]	
Scope:	National, 50+ state/territorial legislatures engaged. Network of CIOs, CTOs, and IT/security directors in state and territorial legislatures.
Focus:	Shares best practices on IT, cybersecurity, cyber resilience planning, and incident response.
Why it matters:	Creates a de facto state legislature cyber resilience network by connecting 50 state legislatures and territories on IT and cybersecurity challenges.

Multi-State Information Sharing and Analysis Center (MS-ISAC)[170]	
Scope:	Serves as a trusted cybersecurity partner for 18,000+ US SLTT government organisations. For nearly two decades, MS-ISAC has been partially funded by the US Congress through a cooperative agreement administered by the US Department of Homeland Security, CISA. MS-ISAC is now moving to a membership fee model (individual or state/territory-wide) to ensure sustainability of funding moving forward.
Focus:	Serves as the primary cyber threat intelligence hub for US SLTT governments.
Why it matters:	Provides a 24/7 security operations centre (SOC), advisories, threat feeds, incident coordination, and low- and no-cost services to SLTT governments across the nation. State legislatures are eligible members. Ensures legislatures are plugged into national cyber early-warning and response systems.
Notable work:	CIS security controls[178] and benchmarks[179].

State and regional public-private (P3) and public-private-academia (P4) partnerships	
Scope:	State/territory-wide or regional.
Examples (not exhaustive):	California Cybersecurity Integration Center[180]; Florida Center for Cybersecurity (CyberFlorida)[181]; CyberTrust Massachusetts[182]; North Carolina Joint Cybersecurity Task Force[183]; North Dakota Joint Cyber Security Operations Center[184]; CyberOhio[185]; Oregon Cybersecurity Center of Excellence[186]; and Texas Regional Security Operations Centers[187].
Structure:	Various operational structures can involve joint operations between state IT agencies, local governments, schools, universities, community colleges, and private-sector cybersecurity vendors.
Why they matter:	Legislatures can directly plug into these P3 and P4 partner organisations for shared monitoring and SOCs; workforce development, education, and training; and assessments, technical assistance, incident response, and other cybersecurity services.

In addition, several key national associations within the United States – including the National Governors Association (NGA), through the NGA Resource Center for Cybersecurity[188], and the National Association of State Chief Information Officers (NASCIO)[189] – often collaborate and share best practice advice on cybersecurity and cyber resilience with the US Congress, federal agencies, the NCSL, and state and territorial legislatures directly. This kind of collaboration can serve as a bridge between the policy and funding authority of legislatures and the executive-branch cybersecurity programmes that often provide direct or indirect cybersecurity defence and resilience capabilities to state and territorial legislatures across the United States.

The cyber resilience "network effect" is achieved through the connection of these national associations (NCSL, NGA, NASCIO, etc.), federal–state ISACs, and state and regional P3 and P4 partnerships.

Notable examples of international collaboration among legislatures and parliaments on cybersecurity, cyber resilience, and digital risk governance include:

Inter-Parliamentary Union (IPU) – Centre for Innovation in Parliament[190]	
Scope:	Global, 183 parliaments engaged.
Focus:	Digital transformation, cybersecurity, AI, and resilience.
Why it matters:	Provides a safe peer-to-peer forum for Members of Parliament and professional staff to exchange information and best practice advice on protecting legislative information, communications, and technology infrastructure.
Notable work:	Guide to Digital Transformation in Parliaments (2023)[191]; World e-Parliament Report 2024, which cites cybersecurity as a top priority for legislatures[192].

Commonwealth Parliamentary Association (CPA)[193]	
Scope:	180 parliaments/legislatures in 53 Commonwealth countries.
Focus:	Security, cybercrime, digital resilience, and governance.
Why it matters:	Creates common security baselines across very different parliaments, fostering a resilience "network by standards".
Notable work:	Parliamentary Security: An Introductory Guide (2025)[194] and e-Handbook on Cybersecurity & Cybercrime[195], published as shared resources.

NATO Parliamentary Assembly (PA)[196]	
Scope:	32 NATO member parliaments + partner nations.
Focus:	Cyber defence, resilience of democratic institutions, and countering hybrid threats.
Why it matters:	Issues regular reports/resolutions urging collective cyber defence and legislatures' role in national resilience strategies, like calling for decisive action on cyber-attacks and disinformation[197].
Unique feature:	Direct link to NATO's own cyber defence policy debates.

Organization for Security and Co-operation in Europe (OSCE) PA[198]	
Scope:	57 participating member countries across Europe, Central Asia, and North America.
Focus:	Cybersecurity, cyber confidence-building measures, election security, and democratic resilience.
Why it matters:	Provides a diplomatic forum where Members of Parliament engage in trust-building dialogues on cyber risks.

ParlAmericas – Digital Governance and AI Programme[199]	
Scope:	Parliaments in the Americas and Caribbean; 35 independent states of the Americas.
Focus:	Digital governance, cybersecurity, and AI.
Why it matters:	Builds regional capacity through dialogue, technical assistance, and toolkits for parliamentarians.
Highlight:	Provides a regional network model linking diverse political systems.

African Parliamentary Network on Internet Governance	
Scope:	Parliaments across Africa, under the Coalition for Digital Africa (ICANN-supported).
Focus:	Cybersecurity awareness, internet governance, and digital policy.
Why it matters:	Strengthens regional collaboration on cyber and internet issues, bringing parliaments into multi-stakeholder governance.

CERT-EU/ Interinstitutional Cybersecurity Board (IICB)[200]	
Scope:	EU institutions, agencies, and the European Parliament.
Focus:	Incident detection, response, and strategic oversight of EU-wide cyber resilience.
Why it matters:	Perhaps the most institutionalised cyber resilience network for legislatures anywhere.
Unique feature:	Combines operational CERT-EU hub with IICB strategic governance.

European Parliamentary Technology Assessment (EPTA) Network[201]	
Scope:	Europe-wide.
Focus:	Digital technologies, cybersecurity, and AI.
Why it matters:	Provides a knowledge-sharing platform for committees to better understand cyber risks and governance. EPTA partners advise parliaments on the possible social, economic, and environmental impact of new sciences and technologies.

Building and sustaining cyber resilience networks offers clear benefits for legislatures and parliaments: stronger protection of democratic institutions through trusted information sharing, faster detection and coordinated response to domestic and international cyber threats, and greater capacity for recovery and continuity when attacks inevitably occur. These networks enable parliaments to learn from one another, leverage trusted third parties, and engage the private sector and academia in collective preparation, mitigation, and defence.

To increase maturity and effectiveness, cyber resilience networks require deliberate governance structures that clarify roles, authorities, escalation pathways, and decision-making responsibilities. Because legislatures often operate with unique constitutional prerogatives and political sensitivities, established governance frameworks should formalise how information will be shared, when joint actions can be taken, and who speaks for the institution during a cyber incident. Secure information-sharing protocols are another core requirement for practical implementation of resilience networks, particularly in politically sensitive legislative environments where confidentiality, political neutrality, and institutional independence must be preserved. With that in mind, legislatures should adopt tiered information-sharing agreements that define what can be shared internally, what can be shared with trusted third parties (such as ISACs), and what requires anonymisation or delayed disclosure.

Beyond governance frameworks and technical platforms, trust building is also foundational to any resilience network, especially among legislatures and parliaments around the globe that differ in political composition, resources, national security constraints, and threat landscapes. Trust must be cultivated deliberately over time, initially through repeated low-risk interactions, joint tabletop exercises, cross-institution incident reviews, and structured communication channels that encourage transparency without jeopardising institutional sensitivities. Over time, these trust-building mechanisms can be used to convert episodic cooperation into standing, highly resilient institutional relationships.

Cyber resilience networks must also work to define how network effectiveness will be measured and how legal and coordination risks among and between network members will be addressed. Much like the concept of a "minimal viable product" in information systems development and deployment, coordination challenges, particularly in federated or politically polarised systems, can be addressed by establishing "minimum viable cooperation mechanisms" to set the stage for broader collaboration in the future. These mechanisms might initially involve small, dependable workflows such as shared early-warning bulletins or establishing secure communication channels for network members in times of crisis. Over time, measurable improvements in cyber readiness, incident detection speed, and cross-institution recovery capabilities can become the fact-base, the justification for expanding and scaling the cyber resilience network.

Ultimately, success depends on legislatures and parliaments committing to institutionalised collaboration and cooperation, adoption and use of common security frameworks, standards, and controls, measurement of performance/impact, and continuous adaptation, so that cyber resilience becomes not just a national goal but a global democratic safeguard against the common cyber vulnerabilities and threats they all face.

Conclusion

Cyber resilience is not merely a technical aspiration for modern legislatures – it is a democratic necessity. As this chapter illustrates, parliaments cannot withstand the growing sophistication, frequency, and geopolitical complexity of cyber threats by acting alone. The very nature of cyber-attacks, which often transcend borders, sectors, and jurisdictions, demands a shift from isolated institutional defences to a collective, trusted, and adaptive ecosystem of partners. Cyber resilience networks embody this shift. They transform cybersecurity from a solitary struggle into a sustained, cooperative effort rooted in shared intelligence, coordinated response, and mutual support.

These networks strengthen parliamentary resilience not only by distributing information and resources but also by multiplying institutional capacity. Whether through national bodies such as ISACs in the United States, regional mechanisms like the EU's CERT-EU and Interinstitutional Cybersecurity Board, or global forums such as the IPU, CPA, NATO PA, and ParlAmericas, parliaments gain access to expertise, early warnings, best practices, and collaborative structures they could not establish independently. Such partnerships amplify detection capabilities, streamline crisis coordination, and accelerate recovery when attacks inevitably occur.

Central to the success of these networks is effective governance. Clear rules for information sharing, decision making, escalation, and cross-institution engagement create a foundation of accountability and predictability.

Tiered sharing agreements, secure communication platforms, and defined roles ensure that confidentiality, political neutrality, and institutional sovereignty are preserved while still enabling rapid, actionable collaboration. Trust building – through repeated interactions, joint exercises, and transparent dialogue – is equally crucial. Cyber resilience networks thrive not only on frameworks and tools but on relationships nurtured over time.

Overcoming coordination challenges is also part of building resilience. As legislatures differ in resources, political contexts, and security postures, networks must start with "minimum viable cooperation mechanisms" – small, dependable workflows that demonstrate early value and expand gradually. Metrics that measure readiness, detection speed, recovery capacity, and participation help convert collaboration into a durable institutional practice backed by evidence and accountability.

Ultimately, cyber resilience networks represent more than the sum of their parts. They reflect a shared commitment among legislatures, governments, academia, and trusted private partners to protect democratic processes against common threats. In a world where cyber-attacks respect no borders and often target the very legitimacy of representative institutions, resilience cannot be a solitary pursuit. By embracing institutionalised cooperation, common standards, continuous learning, and global solidarity, parliaments can transform their vulnerabilities into collective strength and ensure that democracy remains resilient in the face of persistent digital danger.

< part V >

...

// Cybersecurity policies and future considerations

Chapter 15

Toward cybersecurity policies for parliament

All authors

Introduction

A policy framework establishes the overarching principles, standards, and procedures that guide the development and management of individual policies within an organisation. These frameworks set the expectations for how policies are written, approved, implemented, and reviewed.

Policy reviews and update cycles are influenced by the nature of the policy, the pace of change in its subject area, and organisational or political impact. Policies in fast-moving fields – such as technology, security, or compliance – may require more frequent updates, while those based on stable legislation or procedures may change less often. As a result, review schedules should be flexible and tailored to each policy's purpose, risk level, and operating environment.

The review lifecycle depends largely on when changes are required. Reviews may be triggered by shifts in legislation, organisational priorities, operational risks, emerging issues, or feedback from users and stakeholders. For each review, the appropriate stakeholders must be consulted to ensure the revised policy remains accurate, relevant, and practical.

Governance requirements also shape the process. Policies affecting Members of Parliament or parliamentary processes may require review by a committee of the MPs, while others may require oversight at a senior executive level of the house administration, ensuring accountability and alignment with institutional governance.

In summary, policy frameworks set the direction for all policies, and updates should be well-managed, informed by the right stakeholders, and responsive to changes in their field to keep policies relevant and effective.

Information technology security policy

To protect parliamentary information and systems, all business activity must apply appropriate security controls and rely solely on authorised IT assets. Adhering to recognised industry standards for IT security helps safeguard both the parliament's assets and its reputation. Security practices should evolve alongside the changing needs of Members of Parliament, who are responsible and accountable for protecting information by following established controls and procedures.

All IT assets used within the parliamentary environment must be identified, documented, and maintained, enabling the organisation to uphold an accurate inventory. This ensures the organisation retains the authority and capability to enforce timely updates, apply necessary security patches, and enforce an appropriate level of device posture monitoring and oversight.

Members of Parliament and house administration are required to use only authorised hardware and software, and no new technologies may be introduced without prior assessment and approval. The organisation also provides direction on critical areas such as elevated privilege management, password security, monitoring of unauthorised access, data handling, and remote work, including travel with parliamentary devices. These areas would benefit from having dedicated policies with a more frequent update cycle.

Acceptable use policy

Given the unique nature of its operations, parliament requires an acceptable use policy (AUP) that precisely defines the appropriate use of technology resources – such as networks, devices, system access, and email – to safeguard the security and compliance of the parliamentary network. These resources are accessed by the house administration, Members of Parliament, their staff, volunteers, and committee witnesses.

By outlining both appropriate and prohibited behaviours, an AUP helps to protect sensitive parliamentary data, prevent cyber threats, and ensure users understand their responsibilities. It establishes clear expectations of how users may interact with parliamentary devices, networks, infrastructure, or services. By setting clear and explicit rules, the organisation can reduce the risky behaviour that could lead to malware infections, data breaches, and unauthorised access. In turn, this decreases legal and regulatory risks, safeguards the organisation's reputation, and provides a consistent framework for enforcing rules when misuse occurs.

High-risk travel policy

Members of Parliament typically undertake a significant amount of travel, where they are frequently accessing systems, data, and communication tools from various locations and devices. This mobility increases exposure to cybersecurity risks, as remote connections, public networks, and unmanaged devices can create vulnerabilities within the parliamentary infrastructure.

To safeguard sensitive information and maintain integrity of the parliamentary systems, strong travel-related policies must be in place. This policy defines secure practices for disclosing travel plans, accessing external networks, handling devices, and managing data while outside the country. By establishing clear guidelines and security requirements, the organisation can reduce the likelihood of breaches, unauthorised access, and data loss, ensuring that the parliamentary infrastructure and data remain protected regardless of where Members of Parliament are working.

Providing travel kits to Members of Parliament departing for high-risk international trips is an effective way to ensure that parliamentary devices are not taken into environments that could compromise the traveller's safety or parliamentary network security.

Information security classification standard (ISCS) and handling protocol

Business information is a parliamentary asset and must be protected from unauthorised disclosure or loss, maintaining its confidentiality, integrity, and availability throughout its life cycle. It should remain high quality, accessible, reusable, and fit for purpose. To support effective information security governance, the ISCS ensures that all information is accurately classified and marked according to sensitivity to protect individual privacy and parliament's reputation.

Information must be assigned an appropriate classification level – such as Unclassified, Protected, or Secret – based on the risks associated with compromise. This classification determines the required safeguards and may change as the information evolves. Access to Protected or Secret information is limited to individuals with a business need and appropriate clearance level, and when such information must be shared with partners or third parties, the ISCS outlines the protections required for transport, storage, and disposal.

Proper disposal is also essential to prevent unauthorised access or misuse. Secure shredders meeting the required security standards must be used to destroy classified materials, with only authorised personnel handling the process and protecting materials until destruction is complete.

Privileged access policy

Privileged accounts grant elevated, unrestricted access to parliamentary systems. As these accounts enable sensitive administrative actions, the policy describes the acceptable usage and necessary controls relative to these accounts.

To reduce risk, the organisation must uphold rigorous role-based access controls enabling separate privileged roles for different types of elevated access, for example server administration, workstation management, or cloud environments. The organisation must also use just-in-time privileged access grants to allow privileged accounts to be used only when necessary to perform designated duties.

The policy also addresses how to secure these privileged accounts establishing rules about credentials. Credentials must always be protected, never shared, and never entered in untrusted systems or websites. Parliaments should maintain formal records of privileged account lists and usage and routinely review their permissions and relevance to ensure they remain secure. Regular training, including annual recertification, must be enforced to ensure all users adhere to this policy.

Password policy

Passwords and passphrases are vital for verifying a user's identity and protecting the confidentiality, integrity, and controlled access of sensitive information. A password policy is essential for ensuring consistent protection of sensitive information, preventing unauthorised access, and maintaining the overall security of accounts and systems.

The policy mandates all user accounts must follow the organisation's password policy by using complex, unique passwords for each account and using multi-factor authentication (MFA) when possible. The policy describes the minimum acceptable criteria for creating strong passwords that are difficult to compromise, and the supported MFA technologies such as fingerprint, facial recognition, or a one-time code sent to a trusted device.

The policy stipulates that users must avoid risky practices such as sharing passwords or storing them in an unsecured fashion and remind users that strong passwords combined with MFA makes unauthorised access significantly more difficult for cybercriminals.

Procurement policy

To support parliamentarians to effectively carry out their work, the house administration, under the authorisation of the clerk, is empowered to enter into and terminate contracts for procuring goods and services that align with corporate requirements. The policy mandates that all procurement decisions and actions be conducted fairly, transparently, and equitably, without any preferential treatment. Procurement processes must ensure that the house administration delivers the right goods and services at the right time while optimising the value of parliamentary funds.

Any procurement that involves an IT system or solution must involve IT security in defining the mandatory and rated IT security controls that the solution must support to be considered for the evaluation. All procurement requirements must also incorporate a supply chain integrity assessment for the new product before consideration.

A mature organisation must have a set of predefined minimum mandatory security requirements that are used as a foundation for all procurement activities.

Remote access and teleworking policy

The nature of parliamentary work requires a flexible hybrid work model that balances organisational requirements while maintaining high standards of parliamentary service and security. The teleworking policy provides guidance to parliamentarians and house administration staff to ensure that work conducted outside the workplace remains secure, efficient, and compliant with parliamentary standards.

The policy indicates that telework is restricted to the use of IT hardware and software authorised by parliament. It also requires employees to demonstrate that they have the appropriate quality of connectivity that can support the organisational tools, including videoconferencing. Employees are also responsible for safeguarding sensitive and confidential materials, and all legal requirements, policies, directives, and guidelines applicable at the designated workplace continue to apply while teleworking.

Security screening and access management policy

As parts of parliamentary facilities are open to the public, robust security screening and access management policies are required to ensure only authorised individuals enter restricted areas and to prevent unauthorised tools or equipment from being brought inside. These controls protect sensitive information, reduce insider threats, and safeguard facilities and critical systems.

There are two main components for the security screening and access management policy.

First, before an employee can get access to any building in parliament, they must go through the mandatory site-access security clearance. This is the first level of security screening and provides general access to parliamentary buildings and Unclassified systems and information. Those who will be working on Protected or Secret information, or need access to protected areas of parliament, need to go a step further and attain Secret or Top Secret clearance.

Second, the access management policy defines which buildings an individual can access and specifies that the individual must have clear parliamentary-issued identification visible on their person. The policy indicates what level of access management controls are required for the different groups of people entering the parliamentary precinct, such as administration employees, Members of Parliament, MP staff, volunteers, contractors, and students. Not everyone who enters the parliamentary precinct follows the same rules. Access requirements vary, and some areas may require additional screening such as metal detectors, bag checks, or restricting personal devices.

The objective of the security screening and access management policy is to safeguard individuals and assets by ensuring effective security screening mechanisms are in place and by clearly defining the roles and responsibilities of those involved in the screening process. The policy upholds the principles of privacy, transparency, accountability, and efficiency. Personal information used for screening is handled with respect for privacy and informed consent.

Overall, the security screening and access management policy are essential to preventing security breaches and ensuring parliament operations remain safe and effective.

Major cybersecurity incident response policy

A major cybersecurity incident is a high-impact, urgent event that is causing or may cause significant disruption to or compromise to parliament services, operations, infrastructure, or sensitive / personal data and requires an immediate coordinated response.

The purpose of the major cybersecurity incident response policy at the house administration is to ensure the organisation is prepared to respond quickly and effectively when a serious cybersecurity incident occurs. The policy establishes clear governance structure, defined roles and responsibilities, escalation pathways, and communication procedures enabling house administration teams to act in a controlled, coordinated, and consistent manner during a crisis. It supports effective decision making, evidence preservation, incident recovery, and post-incident improvement, reducing operational, financial, and reputational risk while strengthening overall cyber resilience in parliament.

The policy also mandates the use of cybersecurity incident response playbooks for common attack scenarios. These playbooks provide clear, step-by-step guidance, reducing confusion and errors during high-pressure events and enabling faster, coordinated responses across security, IT, and communication teams. Playbooks address incidents such as ransomware, distributed denial of service, malware, data breaches, insider threats, supply chain attacks, and email-based attacks.

To maintain readiness, the policy mandates regular training and yearly simulation exercises. These simulations allow teams to practise responses in a controlled environment, validate governance and communication pathways, clarify roles, and identify gaps.

AI policy

Like other institutions, parliament needs to recognise that AI is now part of our everyday life. AI can benefit parliament by automating routine tasks and enhancing research and data analysis. However, alongside these benefits come significant risks too, including misinformation that can erode public trust, targeted negative influencing campaigns, and embedded bias. For these reasons, it is very important for parliament to establish strong guardrails to ensure AI is used the right way.

It is essential for parliament to have an AI policy that provides a structured, ethical foundation for the organisation's use of artificial intelligence while upholding the values of accountability, inclusivity, innovation, and human-centric design. This policy offers clear guidance on how AI can be used safely, responsibly, and ethically in parliament.

The AI policy also helps manage key risks – such as data privacy concerns, biased outcomes, security vulnerabilities, and potential misuse of automated tools – especially as AI becomes increasingly embedded in the tools and services parliamentarians rely on. As these technologies evolve, parliament must balance innovation and growth with strong risk-management practices.

Ensuring parliamentarians understand how to use AI appropriately and safely is critical. Awareness and training in the responsible use of AI are necessary to maintain network integrity, protect data privacy, and support best practices in data management. By setting clear expectations and safeguards, parliamentarians can foster safe, secure, and forward-looking adoption of AI.

Privacy policy

This policy establishes a comprehensive framework for how the house administration collects, uses, discloses, safeguards, retains, and disposes of personal information under its control. The policy affirms a voluntary commitment to recognised privacy principles and best practices, reinforcing accountability, transparency, and trust with Members of Parliament, employees, and the public.

At its core, the policy is grounded in key privacy principles – including transparency, purpose limitation, information minimisation, proportionality, security, retention limitation, accuracy, and accountability – which guide all handling of personal information throughout its lifecycle. These principles are operationalised through concrete requirements governing collection, use, sharing, disclosure, safeguards, and retention, with an emphasis on limiting information to what is necessary and protecting it through appropriate administrative, technical, and physical controls.

The policy also establishes clear processes for individual access and correction, outlines expectations for privacy breach management (including the identification and handling of material breaches posing a real risk of significant harm), and sets out monitoring and reporting mechanisms supported by defined metrics to enable continuous improvement. It also assigns explicit roles and responsibilities across governance levels – from the clerk to the CIO, managers, and employees – ensuring shared accountability and consistent application across the house administration. Collectively, this policy strengthens the house administration's privacy posture, supports responsible stewardship of personal information, and reinforces public confidence in its operations.

Conclusion

Developing effective cybersecurity policies for parliament requires more than drafting stand-alone rules. It demands a coherent, well-governed policy ecosystem that supports resilience, accountability, and adaptability across the entire institution. As this chapter demonstrates, a strong policy framework provides the structural foundation on which all other policies rest. It clarifies how policies are created, who is responsible for approving and reviewing them, how often they must be updated, and how they align with parliamentary governance and democratic obligations. In a fast-evolving threat environment, where technology, geopolitics, and legislative expectations shift rapidly, this structure ensures that policies remain both relevant and responsive.

The collection of policies outlined in this chapter – spanning IT security, acceptable use, privileged access, information classification, procurement, remote work, security screening, incident response, AI, and privacy – forms an integrated defence architecture for parliament. Each policy addresses a specific operational need, yet all are interconnected. Together, they safeguard devices and networks, protect sensitive information, define user behaviour, ensure secure mobility, manage identity and access, formalise incident response, regulate supply chain risks, promote responsible AI adoption, and uphold privacy rights. This holistic approach ensures that every aspect of parliamentary work, from daily communications to crisis management, is governed by clear expectations and reinforced by consistent standards.

Importantly, effective policies also support cultural resilience. Parliamentarians, staff, and contractors operate within dynamic political and technological contexts, and policies help guide their actions in ways that protect institutional integrity. Clear rules reduce ambiguity, prevent risky practices, and reinforce shared responsibility for cybersecurity. Regular training, periodic reviews, and governance oversight ensure that policies remain living instruments rather than static documents – updated as threats evolve and as parliament adopts new tools, technologies, or ways of working.

Looking ahead, the continued evolution of digital risks – particularly those associated with AI, supply-chain complexity, hybrid work, and emerging technologies like quantum computing – will require parliament to strengthen its policy foundations even further. A rigorous, adaptive policy framework allows the institution to anticipate change, implement safeguards proactively, and preserve trust in its digital operations and democratic processes.

In sum, cybersecurity policies are not merely administrative requirements – they are essential components of parliamentary resilience. By embedding clear standards, structured governance, continuous improvement, and shared accountability, parliament can ensure that its digital environment remains secure, robust, and aligned with the principles of transparency, privacy, and democratic stewardship.

Chapter 16

The future of parliamentary cybersecurity

Authors: Mark Thomas, Victoria Baines

Introduction

As democratic institutions expand their reliance on digital systems, parliamentary bodies must navigate an increasingly complex and volatile cybersecurity landscape. This chapter synthesises themes from earlier sections of the volume and provides a forward-looking analysis of how parliaments can prepare for the next decade of technological, regulatory, and geopolitical change. Rather than predicting a single future, this chapter draws on principles including horizon scanning, scenario techniques, and multi-horizon planning to outline plausible trajectories and strategic priorities. The aim is twofold: to examine the emerging technological and socio-political dynamics shaping parliamentary cybersecurity, and to articulate actionable recommendations that will help parliaments strengthen resilience, safeguard democratic processes, and foster digital trust.

Cybersecurity as a foundation of democratic legitimacy

Cybersecurity has evolved far beyond a technical function; it is now a strategic imperative that underpins institutional stability, democratic legitimacy, and public trust. The integrity of parliamentary decision making depends on secure digital platforms, reliable information flows, and systems protected from manipulation or unauthorised influence. As outlined in earlier chapters, disruptions through cyber intrusion, data alteration, or sophisticated disinformation campaigns create vulnerabilities that extend beyond IT systems. They threaten the credibility of democratic outcomes themselves.

Futures thinking for parliamentary cybersecurity

In the years ahead, several emerging trends will profoundly influence parliamentary cybersecurity. State-sponsored cyber operations and hybrid influence campaigns are expected to intensify, targeting parliamentary networks, political groups, and individual Members of Parliament with the intent of shaping public policy or undermining confidence in democratic institutions. Attacks on supply chains will also increase, as adversaries exploit vulnerabilities in software providers, telecommunications partners, and managed service entities to gain indirect access to parliamentary environments. Assuring the provenance of software will gain in importance, with Software Bills of Materials (SBOMs) expected to play a key role[202]. Increasingly seen as a useful tool for revealing and documenting potential vulnerabilities in supply chains, SBOMs have already featured in the White House's 2021 Executive Order on improving the nation's cybersecurity[203], and are mandatory for software manufacturers under the European Union (EU) Cyber Resilience Act, which entered into force in December 2024[204].

At the same time, the rapid advancement of AI will amplify the capabilities of both attackers and defenders. Parliaments will face AI-driven threats such as automated exploitation, sophisticated disinformation, and deepfakes targeting political figures, even as they adopt AI-enabled tools for threat detection, forensic analysis, and operational resilience. Cybersecurity concerns will become increasingly intertwined with national and European security priorities, blurring traditional boundaries between digital risk and geopolitical strategy. This evolution will be accompanied by regulatory convergence across the EU, with frameworks such as the Network and Information Systems Directive, the Digital Operational Resilience Act, and the AI Act creating more harmonised expectations for cyber oversight and accountability[205].

The last of these instruments entered into force in August 2024 and will be fully applicable from 2026. Applying a risk-based approach, it explicitly bans all AI considered "a clear threat to the safety, livelihoods, and rights of people…from social scoring by governments to toys using voice assistance that encourages dangerous behaviour". AI systems identified as "high-risk" are subject to mandatory risk assessment and mitigation, training data quality assurance, logging of activity and traceability, clear and adequate information, appropriate human oversight, and "a high level of robustness, security and accuracy" (Article 15). Tools in this category include technology used in critical infrastructure, product safety, access to education, training, or employment, all biometric identification, and the operation of essential services. As in the case of the GDPR, the AI Act applies to "providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country"; also to "providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union" (Article 2). As such, the impact of the Act will be felt worldwide, and certainly beyond the EU. As regards the core operations of parliaments, we can expect to see its impact in requirements for enhanced security across a range of services and systems, including remote identification, recruiting and employee management, and "administration of justice and democratic processes" (Recital 61).

Equally, the emergence of quantum computing (Chapter 10) will introduce new risks to parliamentary communications and secure voting mechanisms and is already prompting forward planning for quantum-safe cryptographic systems by technology providers and legislatures alike[206]. It is also envisaged as an enabling technology for more secure communication. For the 27 EU member states and their overseas territories, the European Quantum Communication Infrastructure (EuroQCI) will integrate quantum communication technologies into the infrastructure for resilience, interconnectivity and security by satellite (IRIS2), the sovereign secure satellite constellation for critical infrastructure including governmental institutions[207,208]. Emerging technologies continue to provide security opportunities as well as security risks.

The assessment of the current cyber threat landscape earlier in this book (Chapter 2) detailed how bad actors exploit vulnerabilities in people, processes, and technology. Current signals indicate that exploiting human vulnerabilities in parliamentary cybersecurity will continue to be of great interest, particularly in light of the ongoing proliferation of technologies that erode historical distinctions between physical and digital presence. The COVID-19 pandemic accelerated digital transformation in the interest of keeping governments and parliaments running by any means necessary. Since then, many parliaments have retained something of a hybrid quality, conducting meetings and voting remotely in the interests of efficiency and potential cost savings. In recent years, AI-powered summarisers, note takers, and digital assistants have been incorporated into the most popular messaging, document, and

meeting software. The expected trajectory is one in which, increasingly, automated tools will perform routine functions traditionally fulfilled by parliamentarians and their staff.

In terms of personal safety, the line between cybersecurity and physical security will further erode as all members of society, parliamentarians and their staff included, will make greater use of connected and semi-autonomous vehicles, integrated public transport networks, connected healthcare such as implantable medical devices and brain–computer interfaces, and smart home devices. Because much of the communication for these services relies on use of apps on personal mobile devices, parliamentary cybersecurity will increasingly be a matter of ensuring that representatives and employees use their own devices as safely as possible. Equally, continued proliferation of connected and smart devices on parliamentary premises – often referred to as the Internet of Things (IoT) and comprising any object that can sense and communicate machine to machine – will result in larger numbers of endpoints to be secured, from hardware components for lighting and heating systems to vehicle fleets.

To remain resilient in this future of greater digitisation, connectedness, automation, and processing speed, parliamentary institutions will need to deploy adaptive strategies that evolve as quickly as the threats they face. The shift from static protection models to continuous resilience will be essential, with governance emphasising dynamic monitoring, regular risk reassessment, and rapid incident response. To meaningfully consider the "future of parliamentary cybersecurity", this chapter applies principles from several methodologies: scenario planning, horizon scanning, and three horizons framework (Figure 16.1).

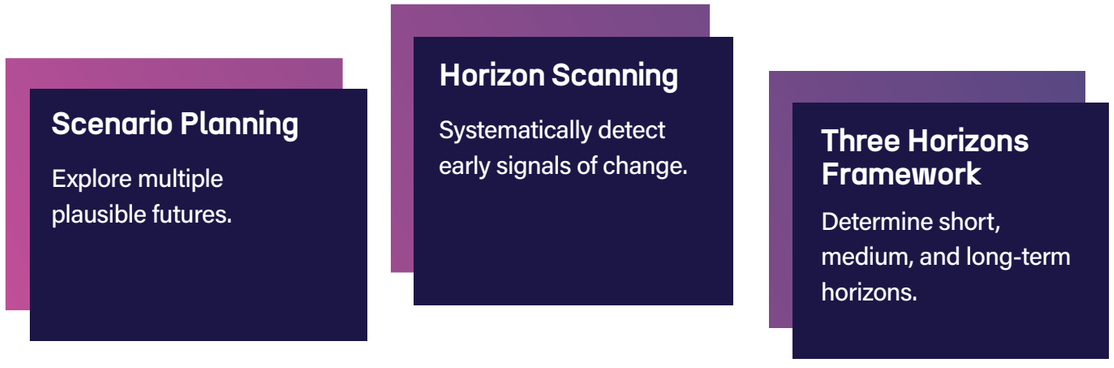


Figure 16.1: Future thinking cybersecurity (source: Mark Thomas)

Scenario planning

Scenario planning is a strategic foresight method that helps parliaments explore multiple, plausible future environments rather than predicting a single trajectory. By constructing diverse narratives about how technology, geopolitics, and democratic processes might evolve, parliaments can stress-test their assumptions and prepare for uncertainty before it materialises. This approach highlights structural vulnerabilities, capability gaps, and opportunities for resilience across a spectrum of realistic futures. Examples of scenario pathways for parliaments include:

AI-driven legislative drafting becoming the norm:

A future in which generative AI systems produce first-draft legislation, committee analysis, and policy briefings. This may increase efficiency but introduces risks such as embedded biases, compromised training data, and adversarial text insertion designed to alter policy outcomes.

Quantum-enabled breaches forcing accelerated cryptographic transition:

A scenario where quantum decryption capabilities emerge sooner than expected, making existing parliamentary communication systems instantly vulnerable. This would necessitate an urgent transition to post-quantum cryptography (PQC) and rapid reassessment of long-term data confidentiality.

Heightened hybrid warfare targeting democratic institutions:

A world where foreign actors blend cyber operations, disinformation, social manipulation, and synthetic media to influence parliamentary debates, sway public opinion, or undermine institutional trust in committee hearings and legislative votes.

Scenario planning enables parliaments to identify vulnerabilities common to multiple futures and develop mitigation strategies that are robust under varied conditions.

EXAMPLE

A synthetic crisis before a committee hearing

A parliament runs a scenario-planning exercise imagining that, hours before a major committee hearing, a realistic deepfake video emerges showing a senior official making inflammatory statements. The scenario forces participants to consider how disinformation might influence media coverage, parliamentary questioning, and public trust. Through the exercise, the institution identifies gaps in its authentication processes, communications protocols, and response coordination – insights that help refine real-world crisis plans.

Horizon scanning

Horizon scanning is a continuous, systematic process for detecting early signs of technological, political, or societal shifts that may influence parliamentary cybersecurity. It focuses on weak signals – subtle but meaningful indicators that, if monitored early, can reveal emerging risks or opportunities. This approach allows parliaments to respond proactively to changes that may otherwise escape traditional risk assessments. Examples of horizon signals relevant to parliaments include:

Sudden improvements in Large Language Model capabilities:

Rapid gains in reasoning, translation, code generation, or multimodal manipulation could drastically alter both the threat landscape and parliamentary workflows, including drafting accuracy, misinformation detection, and committee evidence authentication.

New norms in international cyber cooperation:

Diplomatic developments – such as joint cyber defence agreements, EU-wide CERT alliances, or international norms on AI governance – may shift expectations for parliamentary compliance, reporting, and collaborative defence mechanisms.

Acceleration in post-quantum cryptography standards:

Early adoption of government-backed PQC standards or mandates for critical national infrastructure may signal that parliamentary systems must migrate sooner than anticipated.

Cross-border digital identity initiatives:

The rise of interoperable identity frameworks (eIDAS2, digital wallets, decentralised identity networks) could transform how parliaments authenticate MPs, staff, and public participants in hybrid or remote proceedings.

These signals enable parliaments to anticipate disruptive shifts, adapt risk models, and avoid reactive crisis-driven decision making.

Illustrative Example: Weak Signals of a Cryptographic Shift

During routine horizon-scanning activities, analysts notice subtle but converging signals: several major technology providers begin testing post-quantum encryption, international standards bodies accelerate work on quantum-safe algorithms, and early regulatory drafts hint at future cryptographic requirements. None of these developments alone appears urgent, but together they suggest a significant shift. By recognising the pattern early, the parliament launches an internal review of its encryption posture, giving it a multi-year head start on a transition that will eventually affect all government institutions.

Three Horizons framework

The Three Horizons framework provides a structured way for parliaments to think about change across time. It distinguishes between current systems, emerging innovations, and transformative future states, ensuring that cybersecurity planning addresses short-term needs while also preparing for long-term shifts in democratic function, technology, and institutional design.

The three horizons are:

Horizon 1 (short term): Today's cybersecurity risks and existing systems

This includes familiar threats – phishing, ransomware, supply chain compromises – and the legacy technologies that support current parliamentary operations. Investments focus on strengthening resilience, closing gaps, and modernising essential infrastructure.

Horizon 2 (medium term): Emerging technologies challenging current models

This horizon captures AI-enabled workflows, increasingly integrated IoT ecosystems, the onset of PQC migration, and new forms of hybrid parliamentary participation. These developments disrupt existing assumptions and require experimentation, pilot programmes, and adaptive governance.

Horizon 3 (long term): Transformative shifts that redefine parliamentary operations

Here, parliaments contend with quantum-secure infrastructures, decentralised identity ecosystems, blockchain-secured legislative records, AI-augmented democratic processes, and emerging societal expectations for transparency, resilience, and digital trust.

By considering all three horizons simultaneously, parliaments can ensure that immediate improvements also contribute to long-term democratic resilience and technological readiness.

EXAMPLE

Mapping a 10-year cybersecurity plan

A parliament uses the three horizons framework to structure its long-term cybersecurity strategy. In Horizon 1, it focuses on strengthening immediate defences like multi-factor authentication, secure cloud migration, and patching legacy systems. In Horizon 2, attention shifts to emerging issues such as AI-assisted legislative work and secure digital identity for hybrid participation. Horizon 3 explores transformative possibilities, including quantum-secure communications and blockchain-backed legislative records. The framework helps decision-makers balance short-term needs with long-term institutional evolution.

A strong cybersecurity culture within parliament will become one of the most important defences, requiring ongoing awareness efforts, secure communication practices, and scenario-based training tailored to MPs, staff, and assistants. Threat intelligence will play an increasingly central role, with parliaments formalising mechanisms for gathering, analysing, and acting on intelligence from CERT-EU, ENISA, national computer security incident response teams (CSIRTs), and strategic partners. Legislative workflows will also require modernisation, with cybersecurity expertise embedded directly into committee deliberations, policy review cycles, and impact assessments. Strengthening third-party governance will be critical, as parliaments evaluate suppliers based on demonstrable cybersecurity performance rather than assumptions or contractual assurances alone. Strategic autonomy will push parliaments to invest in secure and sovereign digital infrastructure, including encrypted communication tools and trusted cloud environments. And finally, the rapid development of emerging technologies, such as AI, digital identity systems, and quantum computing, will require continued assessment, early planning, and coordinated policy responses.

Cybersecurity will play an increasingly vital role in preserving the stability of democratic institutions. The integrity of parliamentary decision making relies on secure digital platforms, reliable information flows, and systems protected from manipulation or unauthorised influence. Disruptions to these systems, whether through cyber intrusion, data alteration, or disinformation campaigns, directly threaten the legitimacy of legislative outcomes. Ensuring cybersecurity resilience also helps preserve operational continuity, enabling parliaments to function effectively during crises, be they cyber-related, environmental, or geopolitical. Perhaps most importantly, the public's confidence in parliamentary institutions is closely tied to perceptions of digital competence and security. Citizens expect their elected bodies to protect sensitive information, maintain reliable digital services, and defend democratic processes from malicious interference. Strong cybersecurity safeguards parliamentary autonomy, ensuring that external actors cannot distort public debate or exert undue influence through digital means.

Actionable recommendations: A parliamentary cyber roadmap

As parliaments navigate rapidly evolving technological, geopolitical, and operational challenges, their cybersecurity strategies must shift from episodic improvements to sustained, future-focused capability building. The following roadmap organises practical recommendations across immediate, short-term, and long-term horizons (Figure 16.2).

Each category includes strategically significant priorities that strengthen resilience, reinforce democratic integrity, and build the foundations of digital trust. While individual parliaments vary in resources and regulatory contexts, these recommendations represent core capabilities that every democratic institution should work toward to remain secure, credible, and operationally effective in a digitised future.

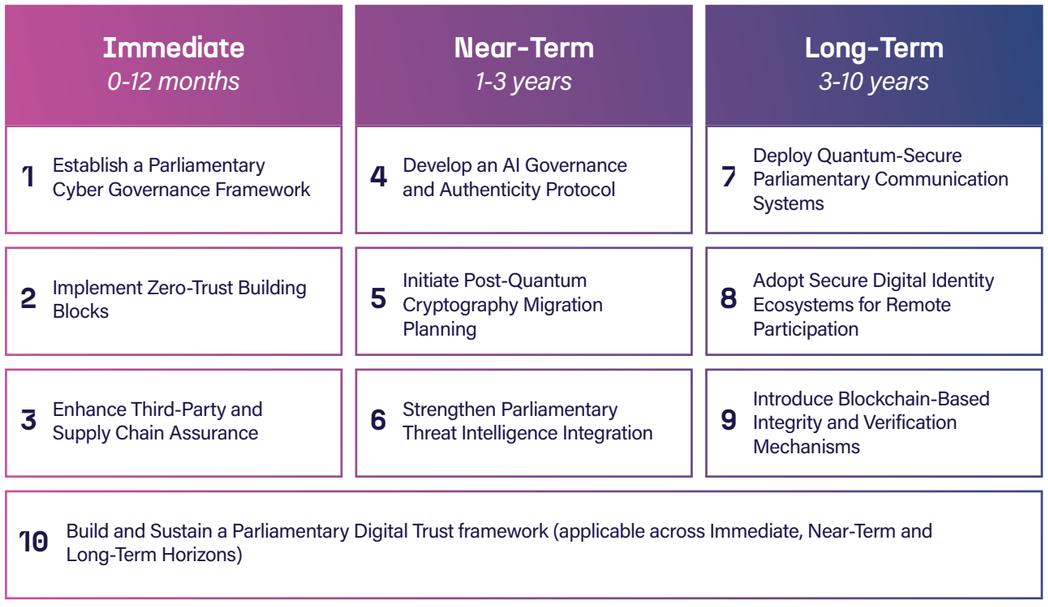


Figure 16.2: Suggested immediate, near-term, and long-term actions (source: Mark Thomas)

1. **Establish a parliamentary cyber governance framework.** Create or formalise a cross-functional body that oversees cyber risk, digital trust, and security strategy across all parliamentary operations. Example: A parliamentary cyber steering committee that includes IT leaders, clerks, security services, and legal/policy advisers, meeting quarterly to review risks.
2. **Implement zero-trust building blocks.** Begin foundational zero-trust measures that reduce attack surface and limit lateral movement without requiring full architecture redesign. Example: Enforcing multi-factor authentication for MPs and staff, paired with segmentation of sensitive committee networks.
3. **Enhance third-party and supply chain assurance.** Improve oversight of all external software and service providers by requiring transparency, security attestations, and component visibility. Example: Mandating SBOM submissions from vendors supplying legislative drafting or document management tools.
4. **Develop an AI governance and authenticity protocol.** Establish standards governing how parliaments use AI tools while ensuring content authenticity, transparency, and secure drafting practices. Example: Requiring authentication for audiovisual evidence submitted to committees to prevent deepfake manipulation.
5. **Initiate PQC migration planning.** Begin preparing for quantum threats by inventorying vulnerable systems, assessing migration pathways, and coordinating with national cyber authorities. Example: Conducting an audit to identify encryption used in email systems, remote voting tools, and archival databases.
6. **Strengthen parliamentary threat intelligence integration.** Formalise processes for receiving, analysing, and acting on intelligence from national and international cybersecurity partners. Example: Establishing a direct information-sharing channel with CERT-EU, NCSC, CISA, or national CSIRTs to stay ahead of emerging threats.
7. **Deploy quantum-secure parliamentary communication systems.** Invest in next-generation protected communication channels leveraging quantum key distribution and sovereign satellite networks. Example: Using regional infrastructures such as EuroQCI/IRIS2 or domestic equivalents to secure MP-to-MP communications.
8. **Adopt secure digital identity ecosystems** for remote participation. Implement robust digital identity frameworks to authenticate MPs, staff, and official participants in hybrid and remote parliamentary processes. Example: Introducing biometrically bound digital identity credentials used for remote voting and committee access.
9. **Introduce blockchain-based integrity** and verification mechanisms. Utilise distributed ledger technologies to verify document integrity, secure legislative workflows, and strengthen auditability. Example: Storing bill versions and committee documents on a tamper-evident blockchain to prevent unauthorised alterations.
10. **Build and sustain a parliamentary digital trust framework** (applicable across immediate, near-term, and long-term horizons). Develop and evolve a comprehensive digital trust framework that guides how parliaments ensure security, transparency, accountability, reliability, and authenticity across all digital operations. This framework becomes the unifying philosophy behind cybersecurity decisions, shaping governance structures, technology adoption, risk assessments, and public communication. Over time, it matures from basic principles into a full lifecycle approach that continuously evaluates how parliamentary digital practices impact citizen trust and democratic legitimacy. Example: Immediately, the framework may define core trust principles and baseline behaviours for MPs and staff; in the near term, it expands to include measurable indicators of trust (such as transparency benchmarks or reliability metrics for digital services); and over the long term, the framework evolves into a formalised "digital trust scorecard" that informs oversight committees, public reporting, and cross-border cooperation on trustworthy democratic technologies.

Together, these recommendations form a coherent roadmap that helps parliaments transition from reactive cybersecurity postures to proactive, future-ready resilience strategies. By aligning immediate improvements with near-term planning and long-term investment, parliaments can build the digital trust, operational continuity, and institutional credibility required to thrive in an increasingly complex digital environment. This roadmap is not merely a technical agenda, it is a democratic imperative that ensures parliamentary institutions remain secure, trustworthy, and capable in the decades ahead.

Cybersecurity as the guardian of democratic futures

Ultimately, the future of parliamentary cybersecurity is about safeguarding digital trust. Digital trust emerges when systems are secure and resilient, information is reliable and uncompromised, and democratic decisions are made free from interference. It is the foundation upon which citizens evaluate the credibility and legitimacy of their governing institutions. When parliaments invest in forward-looking cybersecurity strategies, they do more than protect networks and data – they reinforce the democratic values they represent. In an era where threats are increasingly digital, cybersecurity becomes synonymous with protecting democracy itself. Parliaments that embrace adaptive, strategic, and intelligence-informed cyber governance will not only strengthen their operational resilience but also ensure the continued trust and confidence of the citizens they serve.

Parliaments face an unprecedented convergence of technological change, geopolitical tension, and evolving threats. Ensuring resilience requires more than improved security tools, it demands anticipatory governance, strategically informed foresight, and a sustained commitment to strengthening digital trust. As digital processes become the backbone of democratic institutions, cybersecurity becomes indistinguishable from democratic protection itself. Parliaments that invest today in adaptive, intelligence-informed, and future-oriented cyber strategies will not only safeguard their core functions but reinforce the foundational trust upon which democratic legitimacy depends.

Conclusion

The future of parliamentary cybersecurity will be defined not by any single technology or threat but by the capacity of democratic institutions to anticipate change, adapt strategically, and cultivate digital trust in an era of continuous disruption. As this chapter has shown, cybersecurity is no longer a technical domain operating at the margins of parliamentary activity, but rather a core element of democratic resilience. Protecting legislative integrity, securing information flows, and ensuring the authenticity of digital processes are prerequisites for maintaining public confidence and safeguarding the autonomy of elected institutions.

The coming decade will intensify pressures on parliaments. Cyber-attacks will grow more sophisticated, targeting not only infrastructure but also people, processes, and public perception. AI will reshape both legislative work and the threat landscape, while the emergence of quantum technologies will challenge foundational cryptographic systems. The growing interdependence of digital services, geopolitical tensions, and hybrid modes of participation will blur the boundaries between cybersecurity, physical security, and national security, making resilience a shared responsibility across the entire parliamentary ecosystem.

To meet these challenges, parliaments must transition from reactive defence to forward-looking, intelligence-informed governance. Scenario planning, horizon scanning, and multi-horizon frameworks offer tools for navigating uncertainty and preparing for plausible futures. Investments in secure digital identity, supply-chain assurance, post-quantum readiness, AI governance, and sovereign communication infrastructures will be essential. Equally important will be the cultivation of a strong cybersecurity culture that empowers MPs, staff, and partners to act as stewards of institutional integrity.

Ultimately, the strategic imperative for parliaments is clear: cybersecurity is the new guardian of democratic legitimacy. Institutions that embrace adaptability, foster trusted partnerships, and align security practices with democratic values will be best positioned to protect their operations, uphold public trust, and preserve the credibility of democratic processes in an increasingly contested digital world. By acting now – decisively and collaboratively – parliaments can shape a secure digital future rather than be shaped by it.

// Conclusions and guidelines

Chapter 17

Conclusions

All authors

Concluding remarks

This report has provided an opportunity to reflect on various facets of cybersecurity in parliaments. Its main goal was to serve as an interface between technical and institutional domains where existing cybersecurity guidelines can be effectively customised to enrich the toolkit of parliaments in the digital age. As shown in Figure 1.1 (Chapter 1), parliaments are open and diverse, they operate like all other organisations, but they present distinctive requirements that affect digital strategies.

Unlike executive agencies or private organisations, parliaments must safeguard sensitive political information while upholding constitutional transparency, ensuring accessibility for diverse users, and maintaining operational continuity in dynamic political contexts. These unique institutional characteristics demand cybersecurity approaches that are specifically designed for parliamentary realities rather than adapted from generic public-sector or corporate frameworks.

Developing new cybersecurity guidelines for parliaments therefore requires a structured, inclusive, and forward-looking process. It must begin with a clear understanding of the hybrid threat landscape affecting legislative institutions, where cyber-attacks, disinformation campaigns, insider risks, supply-chain vulnerabilities, and emerging AI-driven threats increasingly converge. Mapping these risks through real-world case studies, horizon scanning, and multi-stakeholder consultation provides the evidence base needed for informed guideline design.

Next, guideline development must consider the distinctive organisational architecture of parliaments: the coexistence of elected representatives, political groups, administrative staff, contractors, external experts, and citizens engaging through digital platforms. Each user group brings different risk profiles and technology needs. This diversity requires guidelines that are flexible, role-specific, and proportionate, while still adhering to a unified security baseline that ensures institutional coherence.

Effective guidelines must also connect technical safeguards with governance and procedural clarity. Cybersecurity in a parliamentary context is not simply a matter of deploying tools. It is a governance challenge that touches on privilege, accountability, separation of powers, and democratic legitimacy. The development process should therefore involve parliamentary leadership, committee structures, IT security departments, legal services, and external experts, ensuring that policies are both operationally sound and institutionally resilient.

Finally, new guidelines must be adaptive. They should incorporate mechanisms for regular review, reflect evolving regulatory requirements, and anticipate emerging technologies such as AI, post-quantum cryptography, secure digital identity systems, and interconnected IoT ecosystems within parliamentary precincts. Embedding continuous improvement, testing, and scenario-based training ensures that guidelines remain relevant long after their initial publication.

In this way, developing cybersecurity guidelines for parliaments becomes more than a technical exercise and represents a strategic investment in democratic stability. By grounding these guidelines in parliamentary realities, aligning them with future-oriented

risk assessments, and integrating them into everyday operations, parliaments can strengthen their cyber resilience and reinforce the digital trust on which modern democratic governance depends.

Within that perspective, the following summarises the main recommendations of each chapter, and their application as cybersecurity guidelines for parliaments. The overview table at the end of this chapter can be used for future reference (Table 17.1).

Part I: Understanding parliamentary cyber vulnerabilities

Chapter 2: Mapping the threat landscape

2.1. Strengthen Human-Focused Security Measures to Reduce Social Engineering Risks

Social engineering remains one of the most effective attack vectors against parliaments, as demonstrated by incidents like the 2015 Bundestag breach and multiple phishing-based compromises. Parliaments should invest heavily in awareness training, verification protocols, and regular phishing simulations to ensure MPs and staff can identify malicious communications. Improving user awareness is highlighted as essential for preventing cyber-attacks, especially with increasingly sophisticated AI-generated phishing attempts.

2.2. Enforce Robust Credential Management and Multi-Factor Authentication (MFA)

Weak passwords, credential reuse, and shared-access practices have directly contributed to breaches – such as the 2017 UK Parliament attack via brute-force password guessing and credential exploitation. Parliaments should establish strict password policies, mandatory MFA, unique credentials for social media and parliamentary systems, and rapid off-boarding procedures to prevent unauthorised access by former staff or compromised accounts.

2.3. Enhance Resilience Through System Hardening, Patch Management, and Protection Against Zero-Day Exploits

Parliaments must prioritise rapid patch application, vulnerability monitoring, and technical hardening, particularly in light of incidents like the 2021 Norwegian Parliament breach exploiting an unknown "zero-day" vulnerability. Threats such as ransomware, infostealers, botnets, Trojans, and DDoS attacks need to be mitigated by maintaining secure configurations and keeping all systems updated.

Chapter 3: Institutional complexity and security

3.1. Establish a Whole-of-Parliament Cybersecurity Governance Model

Because authority in parliaments is fragmented across political leaders, administrative officials, MPs, parties, and technical teams, cybersecurity cannot be effectively managed through traditional top-down models. Parliaments should create formal governance bodies, such as cybersecurity steering committees or cross-party working groups, that bring together all key actors and provide clear decision-making pathways, coordinated oversight, and shared accountability. This ensures faster response during incidents and supports coherent, institution-wide security policies.

3.2. Implement Targeted, Role-Specific Cybersecurity Training for All Parliamentary Actors

MPs, political groups, administrative staff, and technical teams all have different behaviours, pressures, and risk profiles. To address this, parliaments should develop customised awareness programmes, such as training for MPs on personal-device risks, onboarding programmes for new members after elections, and advanced operational training for administrative staff. This helps reduce human-factor vulnerabilities, which are amplified in parliamentary environments due to independence, high turnover, and diverse digital habits.

3.3. Strengthen Collaboration with External Cybersecurity Partners While Safeguarding Parliamentary Autonomy

Given their limited internal authority and fragmented IT environments, parliaments benefit greatly from working with national cybersecurity agencies, trusted vendors, cloud providers, and peer legislatures. However, these partnerships must be structured carefully to protect data sovereignty and institutional independence. Parliaments should adopt clear frameworks for cooperation, secure contracting practices, and mechanisms for safe information exchange to enhance resilience without compromising autonomy.

Chapter 4: Technological ecosystem vulnerabilities

4.1. Reduce End-User Computing Risk Through Standardisation and Training

Parliaments should adopt stricter standardisation of equipment, software, and device policies to reduce vulnerabilities created by heterogeneous end-user environments and widespread "bring your own device" practices. Because many MPs and staff build their own tools (e.g. spreadsheets, small applications) without formal IT training, regular training on secure end-user computing, data handling, and coding standards is essential to prevent errors, privacy breaches, and compliance failures.

4.2. Prioritise Risk-Based Modernisation of Legacy Systems

Legacy systems, often custom-built and critical for parliamentary workflows like transcription, voting, and legislative drafting, pose significant security risks due to outdated technology and limited compatibility with modern defences. Parliaments should adopt a risk-based modernisation strategy, including vulnerability assessments, segmentation, intrusion detection, and the gradual integration

of modern architectures such as zero-trust models, AI-assisted monitoring, and secure cloud migration (with careful attention to data sovereignty).

4.3. Empower the CISO With Strategic Architecture Leadership

Given the complexity of parliamentary technological environments and the long-term nature of digital transformation, parliaments must formally empower the CISO with strategic decision-making authority. This includes the ability to shape IT architecture, guide system modernisation, enforce cybersecurity requirements across departments, and coordinate secure integration of new technologies, ensuring that future parliamentary systems are secure by design rather than incrementally patched.

Chapter 5: Infrastructure security measures

5.1. Implement a Comprehensive and Regularly Tested Backup and Recovery Strategy

Parliaments should adopt the 3-2-1 backup rule – three copies of data, two local on different media, and one off-site – to ensure continuity during cyber incidents, system failures, or disasters. Backups must be encrypted, automated, logged, and tested at least annually, with clearly defined MTD, RTO, and RPO objectives guiding prioritisation and frequency. Properly maintained recovery plans help guarantee data integrity and institutional resilience.

5.2. Strengthen Supply-Chain Security by Enforcing Rigorous Third-Party Requirements

Given parliaments' reliance on external vendors, service providers, and integrators, they must enforce strict cybersecurity obligations in procurement and vendor contracts. This includes supply-chain risk assessments, SLAs with enforceable security clauses, compliance with standards such as NIST C-SCRM and ENISA guidelines, controlled physical access for third parties, incident reporting obligations, and continuous monitoring of vendor security performance.

5.3. Establish a Continuous Vulnerability Management and Penetration Testing Programme

To identify and mitigate weaknesses in parliamentary systems, IT teams should implement regular vulnerability scans, assessments, and periodic penetration tests under well-defined rules of engagement. These processes must include patch management, system hardening, asset discovery, documentation of corrective actions, and adherence to recognised frameworks such as NIST CSF 2.0 and ISO/IEC 27001. Penetration test results should be treated as highly sensitive data due to the insights they provide into system exploitability.

Part II: Developing a parliamentary cybersecurity framework

Chapter 6: Governance and risk management

6.1. Establish a Dedicated Cybersecurity Governance Committee

Parliaments should create a formal oversight body, such as a cybersecurity or information security committee, with a clear mandate to oversee cybersecurity strategy, risk governance, incident readiness, and compliance. This committee should include elected members, professional staff, and subject-matter experts to ensure informed decision-making across political and administrative domains. A structured governance body provides continuity, accountability, and alignment between technical teams and parliamentary leadership.

6.2. Define and Operationalise Risk Appetite and Tolerance Across the Institution

Given the complexity of parliamentary environments and the varying levels of risk across different processes, parliaments must formally articulate risk appetite statements and risk tolerance thresholds. These guide strategic decisions, resource allocation, and prioritisation of security measures. Without clearly defined thresholds, cybersecurity efforts risk becoming inconsistent, reactive, or misaligned with democratic and operational priorities.

6.3. Implement a Structured, Continuous Risk Management Framework

Parliaments should adopt a comprehensive risk-management cycle, including risk identification, assessment, response, monitoring, and reporting, that is continuously updated based on emerging threats, geopolitical developments, and lessons learned from incidents. This should be supported by tools such as asset inventories, business impact analyses, and risk registers. Proactive, repeatable processes are needed to manage risks in a rapidly evolving cyber environment.

Chapter 7: Digital sovereignty and cybersecurity in parliaments

7.1. Strengthen Digital Sovereignty Through National Control of Critical Parliamentary Systems

Parliaments should ensure that essential digital assets, such as voting systems, identity management, communication platforms, and sensitive data repositories, are operated under full national jurisdiction. Reliance on foreign digital infrastructure or non-compliant external providers may weaken both digital sovereignty and parliamentary sovereignty, risking loss of control over mission-critical systems and data. Safeguards such as domestic hosting, sovereign cloud arrangements, strict data-localisation requirements, and procurement screening for high-risk foreign dependencies are essential.

7.2. Develop Internationally Coherent Legal Frameworks and Cross-Border Cyber Agreements

Because digital sovereignty challenges stem from unresolved jurisdictional conflicts and gaps in international cyber law, parliaments should promote and participate in the creation of stronger, enforceable international legal frameworks. This includes harmonising cyber regulations, aligning with supranational initiatives (such as the European Union (EU) AI Act and the Network and Information Systems Directive (NIS2 Directive)), and advancing cross-border enforcement mechanisms. Strengthened legal cooperation helps prevent parliaments from becoming casualties of foreign digital vulnerabilities or hostile state actions.

7.3. Build Strategic Alliances and Support Open, Sovereign-Friendly Innovation Ecosystems

To reinforce sovereignty in the digital domain, parliaments should support alliances among like-minded states, engage with open-innovation communities, and collaborate with academic and research institutions. Open-source initiatives, such as Switzerland's community-driven Large Language Model Apertus, demonstrate how sovereign, transparent technologies can reduce dependency on foreign actors. By encouraging "digital federalism", joint innovation spaces, and research partnerships, parliaments can expand their strategic autonomy and protect their cybersecurity posture.

Chapter 8: Compliance issues and regulatory landscape

8.1. Align Parliamentary Cybersecurity Practices with International and Regional Regulatory Frameworks

Parliaments should proactively harmonise their cybersecurity strategies with widely used frameworks such as NIST CSF 2.0, ISO/IEC 27001/27005, the EU's NIS2 Directive, and ENISA guidance. These frameworks offer risk-based structures that enable adaptive, continuously improving security postures. Because parliaments often rely on national digital ecosystems and cross-border tools, aligning with these standards ensures interoperability, legal compliance, and consistent protection of sensitive legislative data.

8.2. Establish and Maintain an Institution-Wide Minimum Cybersecurity Baseline

Given that parliaments manage sensitive political information while maintaining high levels of public transparency, they must implement a clear and enforceable cybersecurity baseline. This includes asset inventories, strong access controls, encryption, vulnerability management, backup and recovery requirements, incident-response procedures, and secure identity management. Without a baseline, the openness and heterogeneity of parliamentary environments create systemic vulnerabilities that adversaries can easily exploit.

8.3. Strengthen Third-Party Risk Management and Supply-Chain Compliance

Parliaments increasingly depend on external cloud providers, technology vendors, audiovisual systems suppliers, and software developers. To mitigate compliance and sovereignty risks, they must enforce strict third-party security requirements, including contractual controls, due-diligence processes, incident-reporting obligations, and adherence to recognised international standards. Misalignment or non-compliance by external providers can compromise parliamentary operations, data privacy, or even democratic processes.

Part III: Emerging technologies in cybersecurity

Chapter 9: AI and cybersecurity

9.1. Implement Robust Safeguards Against AI-Driven Threats (LLMs and Agentic AI)

Parliaments should deploy technical and procedural controls to mitigate risks created by LLMs and agentic AI systems. This includes defences against prompt injection, training data poisoning, model misuse, identity spoofing, and agentic goal-hijacking, all of which can compromise legislative data, manipulate workflows, or distort parliamentary processes.

9.2. Adopt AI-Enabled Cybersecurity Tools to Strengthen Detection, Prevention, and Response

AI can significantly enhance parliamentary cybersecurity when deployed responsibly. Parliaments should integrate AI-powered phishing protection, automated vulnerability assessment, AI-driven behavioural analytics, data loss prevention, and automated patch management to support overburdened IT teams and improve detection of anomalies such as unusual data access or atypical user behaviour.

9.3. Establish Clear AI Governance Principles: Explainability, Data Sovereignty, and Human-in-the-Loop Controls

As AI tools are integrated into parliamentary workflows, guidelines must ensure that AI decisions are transparent and accompanied by human-understandable explanations. Parliaments should also prioritise data sovereignty, requiring self-hosted or tightly controlled AI deployments for sensitive information. Above all, AI assistance must augment, not replace, human judgement, preserving trust, accountability, and democratic legitimacy within parliamentary operations.

Chapter 10: Information security

10.1. Establish a Rigorous, Institution-Wide Information Classification and Handling Framework

Parliaments should implement a comprehensive framework that identifies, categorises, and classifies all information, from draft legislation and internal communications to citizen data and administrative records. This includes clear labelling protocols (e.g. Unclassified, Protected, Secret), handling rules, access limitations, and secure disposal requirements such as controlled shredding for classified documents. This ensures confidentiality, integrity, and availability across the entire information lifecycle.

10.2. Strengthen Access Controls and Cryptographic Protections Across All Parliamentary Systems

Given the sensitivity and diversity of parliamentary information, organisations must enforce role-based and discretionary access controls, combined with strong application of the CIA triad (confidentiality, integrity, availability). Cryptographic measures, including encryption of stored and transmitted data, digital signatures to protect document integrity, and robust key-management policies, should be standardised and continuously updated according to NIST, ENISA, OWASP, and CIS best practices.

10.3. Prepare for the Post-Quantum Era by Developing a PQC Transition Roadmap

Quantum computing threatens to break many of today's cryptographic systems, creating long-term risks for parliamentary data that must remain confidential for decades.

Parliaments should design and implement a post-quantum cryptography (PQC) roadmap, including early assessment of vulnerable systems, monitoring emerging standards (such as newly approved NIST PQC algorithms), and coordinating migration strategies with national authorities. This ensures future-proof protection of sensitive archives and communications.

Chapter 11: Technological and political transition

11.1. Implement Strict, Time-Bound Identity and Access Management During Political Transitions

Transitions following elections or leadership changes create volatile periods in which departing members, incoming MPs, and shifting staff roles can lead to outdated credentials, lingering account privileges, and insecure document transfers. Parliaments should enforce immediate access revocation, controlled device reassignment, secure onboarding channels, and mandatory archiving protocols to prevent unauthorised access, insider leaks, and exploitation by adversaries during these high-risk moments.

11.2. Establish Crisis-Ready Incident Response and Authenticated Communication Channels

Periods of political tension, protests, or constitutional crises increase the likelihood of targeted cyber-attacks, website defacement, livestream disruption, and disinformation campaigns aimed at delegitimising parliamentary processes. Parliaments should maintain pre-established, rehearsed incident-response structures, ensure resilience of streaming and publication platforms, and use authenticated online communication channels to rapidly counter forgeries, deepfakes, and manipulated content.

11.3. Strengthen Oversight and Legislative Safeguards for Election-Related Technologies

Because parliaments rely on secure electoral systems for their own legitimacy, they must ensure that national voting technologies, voter databases, result-reporting systems, and internal parliamentary voting platforms meet strong cybersecurity standards. This requires independent audits, transparent reporting, robust access controls, secure fallback mechanisms, and statutory requirements governing election infrastructure, paired with active parliamentary oversight of governments and electoral commissions.

Part IV: Implementation and strategic approaches

Chapter 12: Budgeting and resource allocation

12.1. Adopt a Risk-Driven, Framework-Aligned Budgeting Approach

Parliaments should allocate cybersecurity resources based on a formal assessment of institutional risks, prioritising funding for systems whose compromise would significantly disrupt parliamentary operations. Aligning budgets with recognised frameworks, such as NIST CSF, ISO/IEC 27001, and COBIT, ensures that spending decisions are objective, auditable, and strategically justified, reinforcing both internal governance and external accountability.

12.2. Build a Sustainable, Multi-Year Cybersecurity Investment Portfolio

Cybersecurity is not a one-off project but a continuous lifecycle requiring predictable funding for monitoring, patching, licensing, cloud services, and incident response. Parliaments should create a balanced investment portfolio that includes foundational hygiene (MFA, patching, endpoint detection and response), enhanced protection for critical assets (voting systems, chamber technologies), and robust operational capabilities (threat intelligence, continuous monitoring, crisis exercises). Strategic procurement, tool consolidation, and shared services (e.g. CERT collaboration) can significantly improve cost-efficiency.

12.3. Prioritise Human Capability and Cyber-security Culture as Core Budget Categories

Because human behaviour is one of the greatest sources of institutional vulnerability, parliaments must dedicate a significant, recurring portion of the cybersecurity budget to workforce development. This includes: targeted training for MPs and political staff, upskilling cybersecurity professionals, continuous awareness campaigns, leadership crisis-decision exercises, and inter-institutional exchanges and red-team/blue-team simulations. These investments deliver some of the highest returns by reducing incidents, accelerating detection and response, improving compliance, and strengthening digital trust.

Chapter 13: Creating and cultivating a security-conscious parliamentary culture

13.1. Empower Parliamentary Leadership to Act as Visible Champions of Cybersecurity

Because authority in parliaments is distributed and cannot rely on strict enforcement, cybersecurity culture must be modelled from the top. Speakers, clerks, committee chairs, and party leaders should publicly endorse secure practices, participate in cybersecurity awareness events (e.g. Cyber Security Awareness Month), and communicate that cybersecurity is a democratic safeguard, not an administrative burden. Leadership endorsement helps normalise secure behaviour and reduces resistance among MPs and staff.

13.2. Develop Tailored, Continuous, Role-Specific Cybersecurity Education for MPs and Staff

Generic training is ineffective in a parliamentary context. Instead, parliaments should provide targeted learning experiences tailored to MPs, constituency assistants, party strategists, committee clerks, and administrative staff, each with distinct risk profiles and digital practices. Short micro-lessons, real incident case studies, reminders tied to parliamentary workflows, and recurring awareness campaigns help reinforce secure habits without overwhelming busy political actors.

13.3. Promote Trust-Based, Incentive-Driven Cultural Change Rather Than Enforcement

Because MPs cannot be coerced into compliance, parliaments should adopt supportive and incentive-focused approaches to cybersecurity. This includes making secure tools easier to use than insecure ones, offering privileged access to services for those who follow secure practices, and using recognition and positive reinforcement to encourage good behaviour. Exercises such as tabletop simulations and crisis scenarios should be used to build shared understanding and trust across political and administrative actors.

Chapter 14: The creation and maintenance of cyber resilience networks

14.1. Build Institutionalised Cyber Resilience Networks Through Structured Governance Frameworks

Parliaments should move from isolated defensive postures to formal cyber resilience networks that include other branches of government, national cyber agencies, academia, and trusted private-sector partners. These networks require clear governance protocols, including rules for consultation, data sharing, incident coordination, and mutual assistance. Well-defined structures ensure that information flows securely and that parliaments can rely on partners for early warnings, shared intelligence, and coordinated response capabilities.

14.2. Develop Trust-Building Mechanisms and Tiered Information-Sharing Agreements

Given the political sensitivity and autonomy of parliamentary institutions, effective cooperation depends on trust cultivated over time. Parliaments should invest in regular joint exercises, cross-institution workshops, and low-risk collaborative activities to strengthen confidence between actors. They should also adopt tiered information-sharing models that specify what can be shared internally, with trusted third parties (e.g. ISACs), or only in anonymised form, balancing confidentiality with the need for situational awareness and collective defence.

14.3. Participate in National and International Cyber Alliances to Enhance Resilience

Parliaments should actively engage with national, regional, and global cyber resilience initiatives, such as CERT-EU, MS-ISAC, NCSL/NALIT networks, the IPU Centre for Innovation in Parliament, CPA, NATO PA, OSCE PA, and ParlAmericas. These alliances provide access to threat intelligence, peer learning, coordinated defence strategies, and capacity-building opportunities. Leveraging such partnerships strengthens both domestic cybersecurity posture and global democratic resilience.

Part V: Cybersecurity policies and future considerations

Chapter 15: Toward cybersecurity policies for parliament

15.1. Establish a Coherent, Centralised Policy Framework with Regular Review Cycles

Parliaments should adopt a formal policy framework that defines how cybersecurity-related policies are drafted, approved, implemented, and updated. Because parliamentary digital risks evolve rapidly, review schedules must be flexible, risk-based, and triggered by changes in legislation, technology, or operational needs. This ensures that policies remain accurate, relevant, and aligned with governance requirements, including oversight by MPs when necessary.

15.2. Implement Dedicated, High-Granularity Policies for Critical Cyber Domains

To protect parliamentary systems effectively, parliaments should maintain specialised policies covering: IT security, acceptable use, high-risk travel, information classification, privileged access, procurement, teleworking, security screening, and incident response. These policies must include strict access controls, secure handling requirements, mandatory MFA, privileged-account safeguards, supply-chain integrity assessments, and crisis-ready response playbooks. Clear, domain-specific rules reduce ambiguity and minimise vulnerabilities in parliamentary operations.

15.3. Integrate AI and Privacy Governance into Parliamentary Cybersecurity Policies

Given the rising use of AI-based tools and increasing privacy obligations, parliaments must adopt dedicated AI and privacy policies. These policies should ensure: responsible, explainable, human-centred use of AI; safeguards against misinformation, bias, and misuse of automated systems; strict protection for personal information and clear processes for breach handling; and transparency, purpose limitation, and data-minimisation principles. Embedding AI and privacy governance into the broader cybersecurity policy ecosystem reinforces digital trust and protects institutional legitimacy.

Chapter 16: The future of parliamentary cybersecurity

16.1. Establish a Future-Ready Parliamentary Cyber Governance Framework

Parliaments should create or formalise a cross-functional body, such as a steering committee, that provides continuous oversight of cyber risks, aligns cybersecurity with democratic mandates, and integrates emerging technologies, threat intelligence, and horizon-scanning methodologies (e.g. scenario planning, three-horizons analysis). This ensures that cybersecurity remains a strategic priority rather than a reactive technical function.

16.2. Strengthen Supply-Chain and Software-Provenance Assurance (Including SBOM Requirements)

Given the predicted rise of supply-chain intrusions, parliaments must require Software Bills of Materials (SBOMs) from vendors, enforce stricter vendor-security scrutiny, and ensure transparent component inventories for all digital systems supporting legislative work. This is essential as adversaries increasingly exploit third-party dependencies, and regulations such as the EU Cyber Resilience Act already make SBOMs mandatory for manufacturers.

16.3. Begin Early Planning for Post-Quantum Cryptography and Quantum-Secure Communication

Because quantum computing threatens current encryption methods, parliaments should map their cryptographic dependencies, evaluate systems at risk (e.g. remote voting, archival databases), and build a phased migration plan toward quantum-resistant algorithms. Engagement with national cyber agencies and participation in initiatives such as EuroQCI (for secure quantum-enabled communication) will be essential to ensuring long-term democratic resilience.

Guidelines

Table 17.1

Part I	Understanding parliamentary cyber vulnerabilities
Chapter 2	**Mapping the threat landscape**
2.1	Strengthen Human-Focused Security Measures to Reduce Social Engineering Risks
2.2	Enforce Robust Credential Management and Multi-Factor Authentication (MFA)
2.3	Enhance Resilience Through System Hardening, Patch Management, and Protection Against Zero-Day Exploits
Chapter 3	**Institutional complexity and security**
3.1	Establish a Whole-of-Parliament Cybersecurity Governance Model
3.2	Implement Targeted, Role-Specific Cybersecurity Training for All Parliamentary Actors
3.3	Strengthen Collaboration with External Cybersecurity Partners While Safeguarding Parliamentary Autonomy
Chapter 4	**Technological ecosystem vulnerabilities**
4.1	Reduce End-User Computing Risk Through Standardisation and Training
4.2	Prioritise Risk-Based Modernisation of Legacy Systems
4.3	Empower the CISO with Strategic Architecture Leadership
Chapter 5	**Infrastructure security measures**
5.1	Implement a Comprehensive and Regularly Tested Backup and Recovery Strategy
5.2	Strengthen Supply-Chain Security by Enforcing Rigorous Third-Party Requirements
5.3	Establish a Continuous Vulnerability Management and Penetration Testing Programme
Part II	**Developing a parliamentary cybersecurity framework**
Chapter 6	**Governance and risk management**
6.1	Establish a Dedicated Cybersecurity Governance Committee
6.2	Define and Operationalise Risk Appetite and Tolerance Across the Institution
6.3	Implement a Structured, Continuous Risk Management Framework

Chapter 7	**Digital sovereignty and cybersecurity in parliaments**
7.1	Strengthen Digital Sovereignty Through National Control of Critical Parliamentary Systems
7.2	Develop Internationally Coherent Legal Frameworks and Cross-Border Cyber Agreements
7.3	Build Strategic Alliances and Support Open, Sovereign-Friendly Innovation Ecosystems
Chapter 8	**Compliance issues and regulatory landscape**
8.1	Align Parliamentary Cybersecurity Practices With International and Regional Regulatory Frameworks
8.2	Establish and Maintain an Institution-Wide Minimum Cybersecurity Baseline
8.3	Strengthen Third-Party Risk Management and Supply-Chain Compliance
Part III	**Emerging technologies in cybersecurity**
Chapter 9	**AI and cybersecurity**
9.1	Implement Robust Safeguards Against AI-Driven Threats (LLMs and Agentic AI)
9.2	Adopt AI-Enabled Cybersecurity Tools to Strengthen Detection, Prevention, and Response
9.3	Establish Clear AI Governance Principles: Explainability, Data Sovereignty, and Human-in-the-Loop Controls
Chapter 10	**Information security**
10.1	Establish a Rigorous, Institution-Wide Information Classification and Handling Framework
10.2	Strengthen Access Controls and Cryptographic Protections Across All Parliamentary Systems
10.3	Prepare for the Post-Quantum Era by Developing a PQC Transition Roadmap
Chapter 11	**Technological and political transition**
11.1	Implement Strict, Time-Bound Identity and Access Management During Political Transitions
11.2	Establish Crisis-Ready Incident Response and Authenticated Communication Channels
11.3	Strengthen Oversight and Legislative Safeguards for Election-Related Technologies
Part IV	**Implementation and strategic approaches**
Chapter 12	**Budgeting and resource allocation**
12.1	Adopt a Risk-Driven, Framework-Aligned Budgeting Approach
12.2	Build a Sustainable, Multi-Year Cybersecurity Investment Portfolio
12.3	Prioritise Human Capability and Cybersecurity Culture as Core Budget Categories
Chapter 13	**Creating and cultivating a security-conscious parliamentary culture**
13.1	Empower Parliamentary Leadership to Act as Visible Champions of Cybersecurity
13.2	Develop Tailored, Continuous, Role-Specific Cybersecurity Education for MPs and Staff
13.3	Promote Trust-Based, Incentive-Driven Cultural Change Rather Than Enforcement
Chapter 14	**The creation and maintenance of cyber resilience networks**
14.1	Build Institutionalised Cyber Resilience Networks Through Structured Governance Frameworks
14.2	Develop Trust-Building Mechanisms and Tiered Information-Sharing Agreements
14.3	Participate in National and International Cyber Alliances to Enhance Resilience
Part V	**Cybersecurity policies and future considerations**
Chapter 15	**Toward cybersecurity policies for parliament**
15.1	Establish a Coherent, Centralised Policy Framework with Regular Review Cycles
15.2	Implement Dedicated, High-Granularity Policies for Critical Cyber Domains
15.3	Integrate AI and Privacy Governance into Parliamentary Cybersecurity Policies
Chapter 16	**The future of parliamentary cybersecurity**
16.1	Establish a Future-Ready Parliamentary Cyber Governance Framework
16.2	Strengthen Supply-Chain and Software-Provenance Assurance (Including SBOM Requirements)
16.3	Begin Early Planning for Post-Quantum Cryptography and Quantum-Secure Communication

Acronyms

AI	Artificial Intelligence
ANSSI	Agence nationale de la sécurité des systèmes d'information (French National Cybersecurity Agency)
APT	Advanced Persistent Threat
AUP	Acceptable Use Policy
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
C-SCRM	Cybersecurity Supply Chain Risk Management
CAF	Cyber Assessment Framework
CCCS	Canadian Centre for Cyber Security
CERT-EU	Computer Emergency Response Team – European Union
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
COPASIR	Committee for the Security of the Republic (Italy)
CPA	Commonwealth Parliamentary Association
CSF	Cybersecurity Framework
CSIRTs	Computer Security Incident Response Teams
CVE	Common Vulnerabilities and Exposures
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
ENISA	European Union Agency for Cybersecurity
EPTA	European Parliamentary Technology Assessment
EU	European Union
EUC	End-User Computing
EUCS	End-User Computing Satisfaction
EuroQCI	European Quantum Communication Infrastructure
GDPR	General Data Protection Regulation
GRU	General Staff Main Intelligence Directorate (Russian military intelligence)
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IICB	Interinstitutional Cybersecurity Board
IoT	Internet of Things
IPU	Inter-Parliamentary Union
IRIS2	Infrastructure for Resilience, Interconnection and Security by Satellite
ISAC	Information-Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
ISCS	Information Security Classification Standard
ISO	International Organization for Standardization
ITRE	Committee on Industry, Research and Energy
LLM(s)	Large Language Model(s)
MAC	Mandatory Access Control
MFA	Multi-Factor Authentication
MP	Member of Parliament
MS-ISAC	Multi-State Information Sharing and Analysis Center
MTD	Maximum Tolerable Downtime
NALIT	National Association of Legislative Information Technology
NASCIO	National Association of State Chief Information Officers
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NCSL	National Conference of State Legislatures
NGA	National Governors Association
NIS2	Network and Information Systems [Directive]
NIST	National Institute of Standards and Technology
OSCE	Organization for Security and Co-operation in Europe
OWASP	Open Worldwide Application Security Project
PA	Parliamentary Assembly
PQC	Post-Quantum Cryptography
RBAC	Role-Based Access Control
ROI	Return on Investment
RPO	Recovery point objective
RTO	Recovery time objective
SBOM	Software Bill of Materials
SLTT	State, local, tribal, and territorial
SOC	Security operations centre
USB	Universal Serial Bus
USD	United States Dollar
WFD	Westminster Foundation for Democracy

List of figures

Figure 1.1	Book chapters and cybersecurity concerns in parliaments
Figure 5.1	3-2-1 rule for backups
Figure 5.2	Vulnerability management process
Figure 6.1	NIST cybersecurity framework 2.0
Figure 6.2	Risk management phases
Figure 9.1	Transition to AI-assisted cybersecurity
Figure 14.1	Cybersecurity vs cyber resilience
Figure 16.1	Future thinking cybersecurity
Figure 16.2	Suggested immediate, near-term, and long-term actions

List of tables

Table 6.1	Measures of cybersecurity governance effectiveness
Table 6.2	Indicative risk appetite levels in a parliamentary context
Table 6.3	Overview of response strategies
Table 17.1	Guideline overview

Contributor bios

Vasileios Alexiou

Vasileios Alexiou has more than two decades of experience in cybersecurity, risk management, and digital governance. He has held senior executive and advisory roles across public and private sectors and currently serves as Chief Information Security Officer of the Hellenic Parliament, advising leadership on cyber risk, compliance, and institutional resilience at national and international level. Recognised for advancing operational excellence, building high-performing teams, and ensuring delivery against strategic, financial, and regulatory objectives.

Victoria Baines

Dr Victoria Baines is Professor Emerita of Information Technology and Visiting Professor of Technology and Society at Gresham College, London. She has published research on cyberspace governance, digital surveillance, the future of cybercrime, and the rhetoric of security. She formerly led the Strategy team at Europol's European Cybercrime Centre, where she was responsible for the EU's cyber threat analysis. She has also worked in safety operations for a global online platform and now advises governments, technology companies, and international organisations on threat analysis and data strategy She is a Fellow of the British Computer Society and a Court Liveryman of the Worshipful Company of Information Technologists.

Franklin De Vrieze

Franklin De Vrieze is Head of Practice Accountability at Westminster Foundation for Democracy. He is a democracy and governance expert with extensive experience in post-conflict, fragile, and transition countries. His areas of expertise include parliamentary strengthening, post-legislative scrutiny and legislative impact analysis, institution building for anti-corruption and integrity, and the oversight role of parliaments on public finances and public debt. He works at the nexus of parliaments and technology and was co-editor of AI Guidelines for Parliaments, published in 2024. Over the past 25 years, his work has consistently focused on ensuring that democratic institutions deliver with integrity and efficiency. His previous positions included Programme Manager of UNDP's Global Programme on Parliamentary Strengthening and Team Leader of the Central Governance Unit at the OSCE Mission in Kosovo.

Fotios Fitsilis

Prof. Dr Fotis Fitsilis pioneers artificial intelligence in parliaments. Since 2009, he has served in the Scientific Service of the Hellenic Parliament in Athens, driving innovation in the evolution of legislatures toward data-driven parliamentary institutions. Author of several books and academic publications, he co-edited the first global AI Guidelines for Parliaments in 2024 and is a frequent speaker at international forums. He is Professor of AI and Parliamentary Governance at Universidad Austral in Buenos Aires.

Stéphane Gagnon

Stéphane Gagnon is Associate Professor of Business Technology Management with the Department of Administrative Sciences at the Université du Québec en Outaouais (UQO). He obtained in 2001 a Ph.D. in Business Administration from the Université du Québec à Montréal (UQAM), specialising in Technology Management and Strategy. His research is focused on analytics and intelligent systems applied in cybersecurity and fighting disinformation and corruption.

Leonidas Kallipolitis

Leonidas Kallipolitis is a senior IT and cybersecurity executive with over 15 years of experience in software engineering, cybersecurity strategy, and technology leadership. He is actively involved in cybersecurity research and innovation, contributing to the design and validation of advanced security solutions. With a strong focus on aligning technology with business objectives, he delivers resilient, secure solutions that strengthen organisational cybersecurity posture.

Sean McSpaden

Sean McSpaden has served in Oregon State government for the past 27 years. In the executive branch, he served as Oregon's Deputy State Chief Information Officer and in the legislative branch serves as Principal Legislative IT Analyst and as Committee Administrator for Oregon's Joint Legislative Committee on Information Management and Technology. He serves as Oregon's representative to the National Conference of State Legislatures (NCSL) Taskforce on Artificial Intelligence, Cybersecurity, and Privacy and is a Senior Fellow with the Center for Digital Government and Center for Public Sector AI. He is a frequent moderator and speaker for technology-related webinars and state and national forums across the United States. He holds a master's degree in business administration, is an ISACA Certified Information Security Manager, and holds a Project Management Professional certification from the Project Management Institute.

Mark Thomas

Mark Thomas is an internationally recognised expert in governance, risk, cybersecurity, and digital trust. He advises governments and global enterprises on building resilient governance systems, strengthening oversight and assurance structures, and enabling trusted digital transformation across complex, emerging, and high-risk environments.

Hedi Touati

Hedi Touati is the Chief Information Security Officer and director of cybersecurity at the House of Commons of Canada. He is responsible for defining and implementing the organisation's enterprise cybersecurity strategy, governance framework, IT security policies, and security awareness programmes, as well as overseeing security operations, including the 24/7 security operations centre and incident management. With over 25 years of experience in cybersecurity, IT security architecture, and technology strategy, he has held progressively senior roles within the House of Commons, including Principal Security Architect, IT Security Strategist. He holds a PhD in Microelectronics from Polytechnique Grenoble, is a certified information systems security professional, and brings strong private-sector experience from Nortel Networks in systems architecture and design. In parallel with his executive role, he has kept strong ties with the academic environment as a lecturer at the Université du Québec en Outaouais since 1998, teaching cybersecurity and computer science.

Vasilis Tountopoulos

Dr Vasilis Tountopoulos is an ICT Business Innovation expert, leading business development, innovation, and commercialisation activities for integrated cybersecurity solutions. He also provides consulting services on project management, technical specifications, and research innovation for national and EU co-funded research projects. He has more than 24 years of experience in EU and National co-funded and commercial ICT projects, leading activities with respect to the analysis of customer needs and business requirements, the specification of technical design, and the development of business modelling and commercialisation opportunities for new technical solutions. In the recent years, he has been engaged with the analysis of the strategic, organisational, and technological dimensions of cybersecurity in the context of the established EU regulations (Cybersecurity Act, Cyber Resilience Act, Cyber Solidarity Act) and directives (NIS2) and the application of breakthrough AI-assisted technologies for cybersecurity awareness, analysis, and maturity assessment in various business sectors and vertical domains. Vasilis holds a PhD degree in Electrical and Computer Engineering from the National Technical University of Athens (NTUA) and a diploma in Electrical and Computer Engineering from the University of Patras.

References

Chapter 2

[1] Gillett, F., & Comerford, R. (2022, April 22). Two men charged with spying for China under Official Secrets Act. BBC news. https://www.bbc.co.uk/news/uk-68874822

[2] National Cyber Security Centre. (2022, May 10). Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion. https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion

[3] Bundesamt für Verfassungsschutz [German Federal Office for the Protection of the Constitution]. (2024, September 5). Joint Cybersecurity Advisory on Russian military cyber actors targeting U.S. and global critical infrastructure. https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/cyber/2024-09-05-cybersecurity-advisory-3.pdf

[4] For more on this case study, see Tikk, E., Kaska, K., & Vihul, L. (2010). International cyber incidents: Legal considerations. Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

[5] For more on this, see for example Gajjar, D. (2024, 23 May). Cyber security of elections. https://post.parliament.uk/cyber-security-of-elections/ (UK); Government of Canada. (2025). Cyber threats to elections. https://www.cyber.gc.ca/en/guidance/cyber-threats-elections (Canada); and Cybersecurity & Infrastructure Security Agency. (n.d.). Election security. Retrieved February 20, 2026, from https://www.cisa.gov/topics/election-security (United States).

[6] Châtelet, V. (2025, April 18). Exposing Pravda: How pro-Kremlin forces are poisoning AI models and rewriting Wikipedia. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-and-rewriting-wikipedia/

[7] Loft, P. (2025, December 5). Iranian state threat activities in the UK (Research Briefing No. 10143). House of Commons Library. https://researchbriefings.files.parliament.uk/documents/CBP-10413/CBP-10413.pdf; MacAskill, E. (2017, October 14). Iran to blame for cyber-attack on MPs' emails – British intelligence. The Guardian. https://www.theguardian.com/world/2017/oct/14/iran-to-blame-for-cyber-attack-on-mps-emails-british-intelligence

[8] BBC news. (2019, January 4). German politicians targeted in mass data attack. https://www.bbc.co.uk/news/world-europe-46757009

[9] Foo, Y. C. (2023, February 28). European Parliament latest EU body to ban TikTok from staff phones. Reuters. https://www.reuters.com/technology/european-parliament-ban-tiktok-staff-phones-eu-official-says-2023-02-28/; Murphy, M. (2023, March 1). China hits out at US over TikTok ban on federal devices. BBC news. https://www.bbc.co.uk/news/world-asia-china-64795548; BBC news. (2023, March 23). TikTok banned from UK Parliament over security concerns. https://www.bbc.co.uk/news/uk-politics-65055712

[10] Liang, A. (2022, November 3). TikTok says staff in China can access UK and EU user data. BBC news. https://www.bbc.co.uk/news/business-63494951; Euractiv. (2025, May 3). China denies accessing data after TikTok hit with huge EU fine. https://www.euractiv.com/news/china-denies-accessing-data-after-tiktok-hit-with-huge-eu-fine/

[11] The White House. (2025, September 25). Saving TikTok while protecting national security [Executive Order]. https://www.whitehouse.gov/presidential-actions/2025/09/saving-tiktok-while-protecting-national-security/

[12] Ye, J., & Dey, M. (2024, April 19). Apple pulls WhatsApp, Threads from China app store after Beijing order. Reuters. https://www.reuters.com/technology/apple-removes-whatsapp-threads-china-app-store-wsj-reports-2024-04-19/

[13] Baines, V. (2023, January 23). Hacktivism is a risky career path. Wired. https://www.wired.com/story/cybersecurity-hacktivism/

[14] BBC news. (2017, May 13). Cyber-attack: Europol says it was unprecedented in scale. https://www.bbc.com/news/world-europe-39907965

[15] Tidy, J. (2025, July 10). Four arrested in connection with M&S and Co-op cyber-attacks. BBC news. https://www.bbc.com/news/articles/cwykgrv374eo

[16] France24 (2018, July 12). How a Macedonian town became a 'fake news' epicentre. https://www.france24.com/en/20180712-how-macedonian-town-became-fake-news-epicentre

Chapter 3

[17] Konrath, C., & Rathmair, A. (2026). Parliaments in the digital age – building blocks for a theoretical framework. In L. Hagedorn, U. Schmid, S. Winter, & S. Woltran (Eds.), Lecture notes in computer science: Vol. 16319. Digital humanism (pp. 280–294). Springer. https://doi.org/10.1007/978-3-032-11108-1_20

[18] Dunkelman, O. (2025). Privacy – from the ivory tower to the trenches in the parliament. In CODASPY 25 – proceedings of the fifteenth ACM conference on data and application security and privacy (pp. 1–4). Association for Computing Machinery. https://doi.org/10.1145/3714393.3726521

[19] Soto Barrientos, F. S., Fuentes-Bravo, C. F., & Hernández, S. M. (2024). Crowdlaw and digital parliament in law-making: Challenges for Chile before the comparative experience. Revista Chilena de Derecho y Tecnologia, 13, 1–28. https://doi.org/10.5354/0719-2584.2024.69511

[20] Koryzis, D., Dalas, A., Spiliotopoulos, D., & Fitsilis, F. (2021). Parltech: Transformation framework for the digital parliament. Big Data and Cognitive Computing, 5(1), 15. https://doi.org/10.3390/bdcc5010015

[21] Serra-Silva, S. (2023). Beyond national boundaries in the study of digital public engagement: Interparliamentary institutions and cooperation in the Austrian and Portuguese national parliaments. Policy and Internet, 15(1), 36–54. https://doi.org/10.1002/poi3.326

Chapter 4

[22] Chen, J. C. H., Holt, R. W., & Sun, D. B. (2005). Organization and management issues in end user computing. In Encyclopedia of information science and technology: Vol. I (pp. 2230–2235). IGI Global. https://doi.org/10.4018/978-1-59140-553-5.ch393

[23] Shayo, C., & Guthrie, R. A. (2008). End-user computing success measurement. In S. Clarke (Ed.), End-user computing: Concepts, methodologies, tools, and applications. (pp. 1523–1530). IGI Global. https://doi.org/10.4018/978-1-59904-945-8.ch103

[24] Panko, R. R., & Port, D. N. (2013). End user computing: The dark matter (and dark energy) of corporate IT. Journal of Organizational and End User Computing, 25(3), 32–51. https://doi.org/10.4018/joeuc.2013070101

[25] Mann, R. G. (2023). Business risk and user-created solutions. ITNOW, 65(3), 38–39. https://doi.org/10.1093/itnow/bwad092

[26] Fitsilis, F., Koryzis, D., Svolopoulos, V., & Spiliotopoulos, D. (2017). Implementing digital parliament innovative concepts for citizens and policy makers. In C.-H. Tan & F.F.-H. Nah (Eds.), Lecture notes in computer science: Vol. 10293 (pp. 154–170). Springer. https://doi.org/10.1007/978-3-319-58481-2_13

[27] Ahmed, R. K., Ahmed, O., Pappel, I., & Draheim, D. (2022). E-court system evaluation through the user's perspective: Applying the end-user computing satisfaction (EUCS) model. In L. Hagen, M. Solvak, & S. Hwang (Eds.), ACM international conference proceedings series. Digital government research (pp. 293–299). Association for Computing Machinery. https://doi.org/10.1145/3543434.3543560

[28] Bradley, I. D., & Norville, B. (2018). An enterprise cybersecurity strategy for federal critical infrastructure modernization. In Integrated communications, navigation, surveillance conference (pp. 1C41–1C47). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ICNSURV.2018.8384833

[29] Gowdanakatte, S., Ray, I., & Abdelgawad, M. (2023). Model based risk assessment and risk mitigation framework for cyber-physical systems. In Proceedings of 2023 5th IEEE international conference on trust, privacy and security in intelligent systems and applications (pp. 203–212). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/TPS-ISA58951.2023.00034

[30] Chuma, K. G. (2025). Legacy electronic health record systems as culprit behind cybersecurity risks in public healthcare facilities of South Africa. Global Security – Health, Science and Policy, 10(1). https://doi.org/10.1080/23779497.2025.2532556

[31] Sam, D., & Liu, X. (2023). The impact of unplanned system outages on critical infrastructure sectors: Cybersecurity perspective. Issues in Information Systems, 24(4), 273–281. https://doi.org/10.48009/4_iis_2023_121

[32] Abu Bakar, H., Razali, R., & Jambari, D. I. (2022). A qualitative study of legacy systems modernisation for citizen-centric digital government. Sustainability (Switzerland), 14(17). https://doi.org/10.3390/su141710951

[33] Abu Bakar, H., Razali, R., & Jambari, D. I. (2021). Legacy systems modernisation for citizen-centric digital government: A conceptual model. Sustainability (Switzerland), 13(23). https://doi.org/10.3390/su132313112

[34] Abu Bakar, H. K. M., Razali, R., & Jambari, D. I. (2019). Implementation phases in modernisation of legacy systems. In International conference on research and innovation in information systems: Vol. December 2019. IEEE Computer Society. https://doi.org/10.1109/ICRIIS48246.2019.9073628

[35] Singh, V., Korlu, C., & Assuncao, W. K. G. (2025). Experiences on using large language models to re-engineer a legacy system at Volvo group. In Proceedings of 2025 IEEE international conference on software analysis, evolution and reengineering (pp. 102–112). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/SANER64311.2025.00018

[36] Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2023). The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. Government Information Quarterly, 40(1). https://doi.org/10.1016/j.giq.2022.101784

[37] Stamatescu, G., Stamatescu, I., Arghira, N., & Fagarasan, I. (2020). Cybersecurity perspectives for smart building automation systems. In Proceedings of the 12th international conference on electronics, computers and artificial intelligence (pp. 1–5). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ECAI50035.2020.9223152

[38] Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. Urban Governance, 5(1), 1–19. https://doi.org/10.1016/j.ugj.2024.12.010

[39] Karpiuk, M. (2021). Organisation of the national system of cybersecurity: Selected issues. Studia Iuridica Lublinensia, 30(2), 233–244. https://doi.org/10.17951/sil.2021.30.2.233-244

[40] Ndumbe, S. I., & Velikov, P. (2024). Government strategies on cybersecurity and how artificial intelligence can impact cybersecurity in healthcare with special reference to the UK. In H. Jahankhani, G. Bown, M. S. Sharif, & O. Hussien (Eds.), Cybersecurity and artificial intelligence. Advanced sciences and technologies for security applications (pp. 217–236). Springer. https://doi.org/10.1007/978-3-031-52272-7_9

[41] Akpabio, E., Agarmore, S., & Kumar, A. (2026). Fortifying the future: Cybersecurity strategies for critical energy infrastructure. In T. Senjyu, C. So-In, & A. Joshi (Eds.), Lecture notes in networks and systems: Vol. 1460 (pp. 497–507). Springer. https://doi.org/10.1007/978-981-96-7502-9_40

[42] Alauthman, M., Almomani, A., Al-Qerem, A., Maqousi, A. A., & Aldweesh, A. (2025). Cybersecurity challenges in startup-driven digital governance ecosystems: Strategies and solutions. In Startup-driven e-government: Digital innovation for sustainable ecosystems (pp. 633–658). IGI Global. https://doi.org/10.4018/979-8-3373-0817-3.ch024

Chapter 5

[43] Malatji, M., Marnewick, A. L., & von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information and Computer Security, 30(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091

[44] Tari, Z., & Mahmud, R. (2025). Augmenting digital ecosystem resilience through human-centric cybersecurity solutions. IEEE Transactions on Engineering Management, 72, 3892–3908. https://doi.org/10.1109/TEM.2025.3606637

[45] Dong, K., Zhen, J., Xie, Z., & Chen, L. (2025). Building cybersecurity resilience: Integrating defense and recovery investment strategies in an expected resilience framework. Journal of Enterprise Information Management, 38(2), 502–531. https://doi.org/10.1108/JEIM-04-2023-0189

[46] Prakesh, V., Khare, S., Talwandi, N. S., Lalar, S., & Thakur, P. (2025). Strategic framework form cybersecurity risk management: Enhancing resilience in an evolving threat landscape. In N. R. Roy, P. Kumar, A. P. Singh, & A. Kaul (Eds.), Lecture notes in networks and systems: Vol. 1287 (pp. 173–183). Springer. https://doi.org/10.1007/978-981-96-3284-8_13

[47] Yulianto, S., Gaol, F. L., Supangkat, S. H., & Ranti, B. (2023). A comprehensive model for enhancing cybersecurity resilience and IT governance through red teaming exercises. In Proceedings of the ICT 2023 – 29th international conference on telecommunications: Next-generation telecommunications for digital inclusion and universal access. Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ICT60153.2023.10374068

[48] Singh, T. (2025). Digital resilience, cybersecurity and supply chains. Taylor and Francis. https://doi.org/10.4324/9781003604969

[49] National Institute of Standards and Technology. (2026, February 11). Cybersecurity supply chain risk management. https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

[50] European Union Agency for Cybersecurity. (2025, December 8). Good practices for supply chain cybersecurity. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

[51] European Commission. (2026). Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[52] Kelemen, R., Squillace, J., Medvácz, Á., Cappella, J., Bučko, B., & Mazuch, M. (2025). Cybersecurity regulations and software resilience: Strengthening awareness and societal stability. Social Sciences, 14(10), 578. https://doi.org/10.3390/socsci14100578

[53] Harizaj, M., Qafa, R., & Idrizi, O. (2026). Strategic vulnerability analysis of cybersecurity frameworks: Toward a hybrid model for governance and resilience. In K. Dhoska & E. Spaho (Eds.), Communications in computer and information science: Vol. 2670 (pp. 84–96). Springer. https://doi.org/10.1007/978-3-032-07370-9_8

Chapter 6

[54] International Organization for Standardization. (2020). Information security, cybersecurity and privacy protection – Governance of information security (ISO/IEC Standard No. 27014:2020). https://www.iso.org/standard/74046.html

[55] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

[56] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – information security controls (ISO/IEC Standard No. 27002:2022). https://www.iso.org/standard/75652.html

[57] National Cyber Security Centre. (2023, June 23). Cyber security governance. In Risk management [Guidance] (p. 4). https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance

[58] National Conference of State Legislatures. (2018, January). Budgeting for cybersecurity. https://documents.ncsl.org/wwwncsl/Task-Forces/Cybersecurity-Privacy/Budgeting_for_Cybersecurity_FINALJan2018.pdf

[59] Center for Internet Security, & Center for Technology in Government at the University at Albany. (2020, October). Managing cyber threats through effective governance: A call to action for governors and state legislatures. https://documents.ncsl.org/wwwncsl/Task-Forces/Cybersecurity-Privacy/Managing-Cyber-Threats-through-Effective-Governance.pdf

[60] European Union Agency for Cybersecurity. (2023, February). A governance framework for national cybersecurity strategies. https://www.enisa.europa.eu/sites/default/files/publications/A%20Governance%20Framework%20National%20Cybersecurity%20%20Strategies.pdf

[61] National Institute of Standards and Technology. (2024, February 26). The NIST cybersecurity framework (CSF) 2.0. US Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

[62] Committee on Industry, Research and Energy. (n.d.). About. European Parliament. Retrieved February 20, 2026, from https://www.europarl.europa.eu/committees/en/itre/about

[63] National Institute of Standards and Technology. (2018, April 16). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[64] Information Systems Audit and Control Association. (2015). Certified information security manager review manual (14th ed.).

[65] Information Systems Audit and Control Association. (2025). Certified in Risk and Information Systems Control (CRISC). https://www.isaca.org/credentialing/crisc

Chapter 7

[66] Okike, E. U., & Okike, E. (2026). Analysis of cyber security challenges, protection strategies, IT governance, compliance and the law. In N. Atulya K., J. Dharm Singh, M. Durgesh Kumar, & A. Joshi (Eds.), Lecture notes in networks and systems: Vol. 1730. Intelligent sustainable systems (pp. 225–235). Springer. https://doi.org/10.1007/978-3-032-11512-6_19

[67] Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–information security compliance and violation behaviour in organisations: A systematic review. Social Sciences, 11(9). https://doi.org/10.3390/socsci11090386

[68] Balarabe, K. (2025). Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law. Computer Law & Security Review, 58, 106180. https://doi.org/10.1016/j.clsr.2025.106180

[69] Roberts, H. (2025). Digital sovereignty. In A companion to digital ethics (pp. 257–266). John Wiley & Sons. https://doi.org/10.1002/9781394240821.ch21

[70] Jonathan, G. M. (2026). Charting the crossroads of digital sovereignty and digital transformation. In A. Kő, F. Buccafurri, G. Kotsis, A. M. Tjoa, & I. Khalil (Eds.), Electronic government and the information systems perspective (pp. 57–71). Springer. https://doi.org/10.1007/978-3-032-02225-7_5

[71] Qu, R., Yuan, Y., & Xu, J. (2025). Pathways to safeguarding digital sovereignty within a multi-level governance framework: A cross-national comparative study based on the FsQCA method. Policy & Internet, 17(3), e70009. https://doi.org/10.1002/poi3.70009

[72] Dicey, A. V. (1979). The nature of parliamentary sovereignty. In A. V. Dicey (Ed.), Introduction to the study of the law of the constitution (pp. 39–86). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-17968-8_2

[73] Barber, N. W. (2011). The afterlife of parliamentary sovereignty. International Journal of Constitutional Law, 9(1), 144–154. https://doi.org/10.1093/icon/mor023

[74] Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in digital sovereignty: A review of security, privacy, and governance challenges. Public Organization Review. https://doi.org/10.1007/s11115-025-00968-0

[75] Thumfart, J. (2025). Digital sovereignty as postliberalism: A response to Milton Mueller's open letter. Telos, 2025(210), 135–145. https://doi.org/10.3817/0325210135

[76] Repetto, E. (2025). Concept 'stretching' or concept innovation? A review of the usages of sovereignty in the digital sovereignty literature. Policy & Internet, 17(3), e70011. https://doi.org/10.1002/poi3.70011

[77] Rone, J. (2024). 'The sovereign cloud' in Europe: Diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. Journal of European Public Policy, 31(8), 2343–2369. https://doi.org/10.1080/13501763.2024.2348618

[78] Kianpour, M., Earls Davis, P. A., & Windekilde, I. M. (2025). Digital sovereignty in practice: Analyzing the EU's NIS2 directive. International Journal of Information Security, 24(4), 167. https://doi.org/10.1007/s10207-025-01090-4

[79] Tridgell, J. (2025). Open or closing doors? The influence of 'digital sovereignty' in the EU's Cybersecurity Strategy on cybersecurity of open-source software. Computer Law & Security Review, 56, 106078. https://doi.org/10.1016/j.clsr.2024.106078

[80] Fratini, S. (2025). The sociotechnical politics of digital sovereignty: Frictional infrastructures and the alignment of privacy and geopolitics. Big Data & Society, 12(4), 20539517251400729. https://doi.org/10.1177/20539517251400729

[81] Balder, J., & Stark, R. (2025). Development of an open innovation knowledge platform in the context of digital sovereignty. In U. Schmuntzsch, A. Shajek, & E. A. Hartmann (Eds.), New digital work II: Digital sovereignty of companies and organizations (pp. 195–216). Springer. https://doi.org/10.1007/978-3-031-69994-8_12

[82] Ganten, P., Seyffarth, M., & Kuhlmann, N. (2025). Successful digital transformation in economy and industry requires open source. In U. Schmuntzsch, A. Shajek, & E. A. Hartmann (Eds.), New digital work II: Digital sovereignty of companies and organizations (pp. 17–31). Springer. https://doi.org/10.1007/978-3-031-69994-8_2

[83] Hernández-Cano, A., Hägele, A., Huang, A. H., Romanou, A., Solergibert, A.-J., Pasztor, B., Messmer, B., Garbaya, D., Ďurech, E. F., Hakimi, I., García Giraldo, J., Ismayilzada, M., Foroutan, N., Moalla, S., Chen, T., Sabolčec, V., Xu, Y., Aerni, M., AlKhamissi, B.,… Schlag, I. (2025). Apertus: Democratizing open and compliant LLMs for global language environments. arXiv. Retrieved from http://hdl.handle.net/20.500.11850/793162

[84] Ishkhanyan, A. (2025). The sovereignty–internationalism paradox in AI governance: Digital federalism and global algorithmic control. Discover Artificial Intelligence, 5(1), 123. https://doi.org/10.1007/s44163-025-00374-x

Chapter 8

[85] EBSCO. (n.d.). Parliamentary system. Retrieved February 20, 2026, from https://www.ebsco.com/research-starters/history/parliamentary-system

[86] Department for Science, Innovation and Technology. (2025, August 11). Mapping cyber governance code to NIST Cyber Security Framework. https://www.gov.uk/government/publications/cyber-governance-mapping/mapping-cyber-governance-code-to-nist-cyber-security-framework

[87] International Organization for Standardization. (2020). Information security, cybersecurity and privacy protection – Governance of information security (ISO/IEC Standard No. 27014:2020). https://www.iso.org/standard/74046.html

[88] ScienceDirect. (n.d.). Parliamentary system. Retrieved February 20, 2026, from https://www.sciencedirect.com/topics/social-sciences/parliamentary-system

[89] European Union. (n.d.). European Parliament. Retrieved February 20, 2026, from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-parliament_en

[90] The Borgen Project. (2020). How a parliamentary system works. https://borgenproject.org/how-a-parliamentary-system-works/

[91] Klopfer, F., Rizmal, I., Sekuloski, M., Hatzl, T., & Mladenovic, D. (2019). Introduction to cybersecurity governance: A tool for members of parliament. Geneva Centre for Security Sector Governance (DCAF). https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyToolENGLISH.pdf

[92] Commonwealth Parliamentary Association. (2025). Parliamentary security: An introductory guide. https://www.cpahq.org/media/q4tfx4i4/parliamentary-security_introductory_guide_final.pdf

[93] European Parliament. (2025, November 12). Answer to written question E-003669/25. https://www.europarl.europa.eu/doceo/document/E-10-2025-003669-ASW_EN.html

[94] National Democratic Institute & House Democracy Partnership. (2022). Cybersecurity handbook for parliaments. https://parliaments.cyberhandbook.org

[95] Directive (EU) 2022/2555. Measures for a high common level of cybersecurity across the Union (NIS2 Directive). European Parliament, Council of the European Union. http://data.europa.eu/eli/dir/2022/2555/oj

[96] Regulation (EU) 2024/2847. Horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). European Parliament, Council of the European Union. http://data.europa.eu/eli/reg/2024/2847/oj

[97] Inter-Parliamentary Union. (2026, January 25). Parliamentary actions on AI policy. https://www.ipu.org/impact/democracy-and-strong-parliaments/artificial-intelligence/parliamentary-actions-ai-policy

[98] SANS (n.d.). Incident response. Retrieved February 20, 2026, from https://www.sans.org/security-resources/glossary-of-terms/incident-response

[99] NCSC. (2023). Cyber security governance.

https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance

Chapter 9

[100] Westminster Foundation for Democracy. (2024). Guidelines for AI in parliaments. https://www.wfd.org/ai-guidelines-parliaments

[101] OWASP. (2025). OWASP top 10 for LLM applications 2025. https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/

[102] OWASP. (2025). Agentic AI – threats and mitigations. https://genai.owasp.org/resource/agentic-ai-threats-and-mitigations

[103] European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025. https://enisa.europa.eu/publications/enisa-threat-landscape-2025

[104] SANS. (2025). SANS 2025 security awareness report. https://www.sans.org/for-organizations/workforce/resources/security-awareness-report

[105] Bernardo, V. (n.d.). Deepfake detection. European Data Protection Supervisor. Retrieved February 20, 2026, from https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/deepfake-detection_en

[106] Sennitt, O. (2025, October 18). Tory MP reports deepfake defection video to police. BBC news. https://www.bbc.com/news/articles/c62e7xz02dpo

[107] Seitz-Wald, A., & Memoli, M. (2024, January 22). Fake Joe Biden robocall tells New Hampshire Democrats not to vote Tuesday. NBC news. https://www.nbcnews.com/politics/2024-election/fake-joe-biden-robocall-tells-new-hampshire-democrats-not-vote-tuesday-rcna134984

Chapter 10

[108] European Council. (2024). The general data protection regulation. https://www.consilium.europa.eu/en/policies/data-protection-regulation/

[109] European Parliament. (n.d.). Open data portal. Retrieved February 20, 2026, from https://data.europarl.europa.eu

[110] Data.gov. (n.d.). The home of the U.S. government's open data. Retrieved February 20, 2026, from https://data.gov/

[111] House of Commons Library. (2026). Parliament and elections data. UK Parliament. https://commonslibrary.parliament.uk/data/parliament-elections-data/

[112] Barker, E. (2020). Guideline for using cryptographic standards in the Federal Government: Cryptographic mechanisms (NIST Special Publication 800-175B Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-175Br1

[113] European Union Agency for Cybersecurity. (2013). Recommended cryptographic measures – Securing personal data. https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data

[114] OWASP. (2021). A02:2021 – Cryptographic failures. https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

[115] Center for Internet Security. (2026). CIS critical security controls navigator. https://www.cisecurity.org/controls/cis-controls-navigator

[116] European Telecommunications Standards Institute. (2015). Quantum safe cryptography and security: An introduction, benefits, enablers and challenges (ETSI White Paper No. 8). https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[117] National Institute of Standards and Technology. (2024, August 13). Announcing approval of three federal information processing standards (FIPS) for post-quantum cryptography. https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

[118] European Commission. (2025). Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[119] Quantum Computing Cybersecurity Preparedness Act, H.R. 7535, 117th Cong. (2021–2022). https://www.congress.gov/bill/117th-congress/house-bill/7535

Chapter 11

[120] Commonwealth Parliamentary Association. (2025). Parliamentary security: An introductory guide. https://www.cpahq.org/media/q4tfx4i4/parliamentary-security_introductory_guide_final.pdf

[121] Commonwealth Parliamentary Association. (2025, January 29). Parliamentary security: New CPA handbook provides guidance to parliaments. https://www.cpahq.org/news/2025_01-parliamentary-security-guide/

[122] National Cyber Security Centre. (2023). Guidance for high-risk individuals on protecting your accounts and devices. https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals

[123] Ministry of Justice. (2023). Cyber security guidance: General edition. https://security-guidance.service.justice.gov.uk/moj-guidance.pdf

[124] European Commission. (2024). Memo: Known information interference operations during the June 2024 elections for the European Parliament. https://ec.europa.eu/commission/presscorner/api/files/attachment/879707/Memo%20-%20Known%20information%20interference%20operations%20during%20EP%20elections.pdf

[125] Freedom House. (2019). Digital election interference. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/digital-election-interference

[126] Directive (EU) 2022/2555. Measures for a high common level of cybersecurity across the Union (NIS2 Directive). European Parliament, Council of the European Union. http://data.europa.eu/eli/dir/2022/2555/oj

[127] Fluri, P., & Johnsson, A. B. (Eds.). (2003). Parliamentary oversight of the security sector: Principles, mechanisms and practices (corrected English ed.). IPU & Geneva Centre for Security Sector Governance (DCAF). https://www.dcaf.ch/sites/default/files/publications/documents/ipu_hb_english_corrected.pdf

[128] Department for Science, Innovation and Technology. (2024, September 30). Cyber Security and Resilience Bill (UK Government legislation collection). gov.uk. https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

[129] Faeta, G., Schweizer, P., Dellamula, S., & Frimpong, S. (2025). Common security: Concept and good practices for parliamentarians (Applied research project final report). Geneva Graduate Institute & IPU. https://www.graduateinstitute.ch/sites/internet/files/2025-10/ARP_CommonSecurity_final---Selma-Dellamula.pdf

[130] Geneva Centre for Security Sector Governance. (2015). Parliaments: Roles and responsibilities in good security sector governance (SSR Backgrounder). https://www.files.ethz.ch/isn/195681/DCAF_BG_8_Parliaments.11.15.pdf

[131] BBC news. (2017, June 24). Parliament hit by 'sustained' cyber-attack. https://www.bbc.com/news/uk-40394074

[132] New Zealand Government. (2024, March 26). Parliamentary network breached by the PRC. https://www.beehive.govt.nz/release/parliamentary-network-breached-prc

[133] Klopfer, F., Rizmal, I., Sekuloski, M., Hatzl, T., & Mladenovic, D. (2019). Introduction to cybersecurity governance: A tool for members of parliament. Geneva Centre for Security Sector Governance (DCAF). https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyToolENGLISH.pdf

[134] Deutsche Welle. (2015, November 6). Bundestag counting cost of cyberattack. https://www.dw.com/en/bundestag-counting-cost-of-cyberattack/a-18512512

[135] Decode39. (2024, March 27). Italian MPs hit by Chinese hacking spree. https://decode39.com/8928/italian-mps-chinese-hacking-spree/

[136] Saeva, E., & Tasheva, I. (2024). The 2024 EU elections and cybersecurity: A retrospective and lessons learned. European View, 23(2), 226–234. https://doi.org/10.1177/17816858241288397

[137] European Commission. (n.d.). EU cybersecurity policies. Retrieved February 20, 2026, from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[138] European Parliament. (2024, February 8). Serbia did not fulfil its commitments to free and fair elections, say MEPs [Press release]. https://www.europarl.europa.eu/news/en/press-room/20240202IPR17327/serbia-did-not-fulfil-its-commitments-to-free-and-fair-elections-say-meps

[139] European Commission. (2025, June 6). Report on the 2024 elections to the European Parliament (Communication COM(2025)287 final). https://commission.europa.eu/document/download/2a7fddb2-e927-4079-92cc-4bb4279e9a46_en

[140] European Union Agency for Cybersecurity. (2024). Best practices for cyber crisis management. https://data.europa.eu/doi/10.2824/767828

[141] European Union Agency for Cybersecurity. (2021). ENISA threat landscape 2021. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf

[142] Reuters. (2020, September 1). Norway's parliament says it was hit by 'significant' cyber attack. https://www.reuters.com/world/norways-parliament-says-it-was-hit-by-significant-cyber-attack-2020-09-01/

[143] Przetacznik, J., & Tarpova, S. (2022, June). Russia's war on Ukraine: Timeline of cyber-attacks (EPRS Briefing No. 733.549). European Parliamentary Research Service, European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

[144] Díaz Crego, M., & Mańko, R. (2022, January). Parliaments in emergency mode: Lessons learnt after two years of pandemic (EPRS Briefing No. PE 698.879). European Parliamentary Research Service, European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698879/EPRS_BRI(2022)698879_EN.pdf

[145] Deveaux, K., Švecová, N., & Baker, T. (2021). Parliaments responding to a pandemic: Lessons learned for emergency planning. House Democracy Partnership, Swiss Agency for Development and Cooperation & National Democratic Institute. https://www.ndi.org/sites/default/files/Parliaments%20Responding%20to%20a%20Pandemic_%20Lessons%20Learned%20for%20Emergency%20Planning_FINAL.pdf

Chapter 12

[146] Commonwealth Parliamentary Association. (2022). Cybersecurity and digital resilience for parliaments. https://www.cpahq.org/

[147] European Union Agency for Cybersecurity. (2023). Cybersecurity in the public sector: Building digital resilience in government and parliament. https://www.enisa.europa.eu/publications

[148] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

[149] National Institute of Standards and Technology. (2021). Risk Management framework for information systems and organizations: A system life cycle approach for security and privacy (SP 800-37 Rev. 2). https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[150] National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[151] Information Systems Audit and Control Association. (2019). COBIT 2019 framework: Governance and management objectives. https://www.isaca.org/resources/cobit

[152] Inter-Parliamentary Union, & Global Partners Digital. (2021). Cybersecurity in parliaments: Building resilient institutions in the digital age. https://www.ipu.org/resources/publications

[153] Canadian Centre for Cyber Security. (2021). Baseline cyber security controls for small and medium organizations. https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Chapter 13

[154] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers and Security, 109. https://doi.org/10.1016/j.cose.2021.102387

[155] Baird, P. (2023). Improving risk management: Combining security and cyber insurance practices. Network Security, 2023(11). https://doi.org/10.12968/S1353-4858(23)70052-4

[156] Ramluckan, T., van Niekerk, B., & Martins, I. (2020). A change management perspective to implementing a cyber security culture. In T. Eze, L. Speakman, & C. Onwubiko (Eds.), European Conference on Information Warfare and Security: Vol. 2020-June (pp. 442–448). Curran Associates. https://doi.org/10.34190/EWS.20.059

[157] Bundschuh, L., Thorn, D., Härting, R.-C., Reichstein, C., Takeuchi, H., & Scheppach, J. (2025). Determinants of a successful establishment of a cyber security culture in enterprises. In Y.-W. Chen, R. J. Howlett, R. J. Howlett, L. C. Jain, L. C. Jain, & J. Flearmoy (Eds.), Procedia Computer Science: Vol. 270 (pp. 4315–4323). Elsevier. https://doi.org/10.1016/j.procs.2025.09.556

[158] Corradini, I., & Nardelli, E. (2019). Building organizational risk culture in cyber security: The role of human factors. In T. Z. Ahram & D. Nicholson (Eds.), Advances in Intelligent Systems and Computing: Vol. 782 (pp. 193–202). Springer. https://doi.org/10.1007/978-3-319-94782-2_19

[159] Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. Journal of Computer Information Systems, 62(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

[160] Reid, R., & van Niekerk, J. (2014). Towards an education campaign for fostering a societal, cyber security culture. In S. M. Furnell & N. L. Clarke (Eds.), Proceedings of the 8th International Symposium on Human Aspects of Information Security and Assurance (pp. 174–184). Elsevier. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84975727364&partnerID=40&md5=642a725bb0c9c64b98483b78093a631e

[161] Yamin, M. M., Erdodi, L., Torseth, E., & Katt, B. (2022). Selecting and training young cyber talent: A recurrent European cyber security challenge case study. In D. D. Schmorrow & C. M. Fidopiastis (Eds.), Lecture Notes in Computer Science: Vol. 13310 (pp. 304–321). Springer. https://doi.org/10.1007/978-3-031-05457-0_24

[162] McLaughlin, K. L. (2025). Securing talent: Building and retaining high-performance cybersecurity teams. Taylor and Francis. https://doi.org/10.1201/9781003462064

[163] Cherinka, R. (2019). Using cyber competitions to build a cyber security talent pipeline and skilled workforce. In S. Kapoor, R. Bhatia, & K. Arai (Eds.), Advances in Intelligent Systems and Computing: Vol. 857 (pp. 280–289). Springer. https://doi.org/10.1007/978-3-030-01177-2_20

[164] José, I., LaPort, K., & Trippe, D. M. (2016). Requisite attributes for cyber security personnel and teams: Cyber risk mitigation through talent management. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), Psychosocial Dynamics of Cyber Security (pp. 167–193). Taylor and Francis. https://doi.org/10.4324/9781315796352-17

Chapter 14

[165] National Institute of Standards and Technology. (2015, December). Annex A: terms and conditions. In Supplemental information for the interagency report on strategic U.S. government engagement in international standardization to achieve U.S. objectives for cybersecurity (Report 8074, Volume 2). US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

[166] National Institute for Standards and Technology. (2021, December). Appendix A: Glossary. In Developing cyber-resilient systems: A systems security engineering approach (Special Publication 800-160, Vol. 2, Rev.1). US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

[167] National Institute for Standards and Technology. (2016, October). Guide to cyber threat information sharing (Special Publication 800-150). US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[168] European Union Agency for Cybersecurity. (n.d.). Information Sharing and Analysis Centers (ISACs). Retrieved February 20, 2026, from https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/information-sharing-and-analysis-centers-isacs

[169] Center for Internet Security. (n.d.). About us. Retrieved February 20, 2026, from https://www.cisecurity.org/about-us

[170] Center for Internet Security. (n.d.). Multi-State Information Sharing and Analysis Center: America's frontline cyber defense partner for SLTTs. Retrieved February 20, 2026, from https://www.cisecurity.org/ms-isac

[171] Computer Emergency Response Team – European Union. (n.d.). About us. Retrieved February 20, 2026, from https://cert.europa.eu/about-us

[172] Cybersecurity and Infrastructure Security Agency. (n.d.). Home. US Department of Homeland Security. Retrieved February 20, 2026, from https://www.cisa.gov/

[173] Cybersecurity and Infrastructure Security Agency. (n.d.). Joint cyber defense collaborative. US Department of Homeland Security. Retrieved February 20, 2026, from https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative

[174] National Conference of State Legislatures. (n.d.). Taskforce on Artificial Intelligence, Cybersecurity and Privacy. Retrieved February 20, 2026, from https://www.ncsl.org/in-dc/task-forces/task-force-on-artificial-intelligence-cybersecurity-and-privacy

[175] National Conference of State Legislatures. (2018, January). Budgeting for cybersecurity. https://documents.ncsl.org/wwwncsl/Task-Forces/Cybersecurity-Privacy/Budgeting_for_Cybersecurity_FINALJan2018.pdf

[176] National Conference of State Legislatures. (2025, August 11). Artificial intelligence toolkit. https://www.ncsl.org/technology-and-communication/artificial-intelligence-policy-toolkit

[177] National Conference of State Legislatures. (n.d.). National Association of Legislative Information Technology. Retrieved February 20, 2026, from https://www.ncsl.org/legislative-staff/nalit

[178] Center for Internet Security. (n.d.). CIS critical security controls. Retrieved February 20, 2026, from https://www.cisecurity.org/controls

[179] Center for Internet Security. (n.d.). CIS benchmarks list. Retrieved February 20, 2026, from https://www.cisecurity.org/cis-benchmarks

[180] Governor's Office of Emergency Services (n.d.). California Cybersecurity Integration Center. State of California. Retrieved February 20, 2026, from https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/

[181] Florida Center for Cybersecurity at the University of South Florida. (n.d.). Welcome to Cyber Florida. Retrieved February 20, 2026, from https://cyberflorida.org/

[182] CyberTrust Massachusetts. (n.d.). CyberTrust Massachusetts is a non-profit committed to building opportunity and security through a consortium of statewide businesses and colleges. Retrieved February 20, 2026, from https://www.cybertrustmass.org/

[183] North Carolina Department of Public Safety. (n.d.). NC Joint Cybersecurity Task Force (JCTF) Resource Page. Retrieved February 20, 2026, from https://www.ncdps.gov/nc-joint-cybersecurity-task-force-jctf-resource-page

[184] North Dakota Information Technology. (2023, August). Cybersecurity: Joint Cyber Security Operations Center (JCSOC) 2021-present. Retrieved April 2, 2026, from https://www.nascio.org/wp-content/uploads/2023/08/ND_Cybersecurity.pdf

[185] Ingles, J. (2016, September 29). New CyberOhio initiative is meant to protect businesses in Ohio from hackers. The Statehouse News Bureau. https://www.statenews.org/government-politics/2016-09-29/new-cyberohio-initiative-is-meant-to-protect-businesses-in-ohio-from-hackers

[186] Oregon Cybersecurity Center of Excellence. (n.d.). Home. Retrieved February 20, 2026, from https://www.occoe.org/

[187] Texas Department of Information Resources. (2023). An overview of regional security operations centers in Texas. https://dir.texas.gov/sites/default/files/2024-01/An%20Overview%20of%20RSOCs%20in%20Texas%20Jan%202024.pdf

[188] National Governors Association. (n.d.). Resource Center for State Cybersecurity. Retrieved February 20, 2026, from https://www.nga.org/statecyber/

[189] National Association of State Chief Information Officers. (n.d.). Home. Retrieved February 20, 2026, from https://www.nascio.org/

[190] Inter-Parliamentary Union. (n.d.). Center for Innovation in Parliament. Retrieved February 20, 2026, from https://www.ipu.org/impact/democracy-and-strong-parliaments/centre-innovation-in-parliament

[191] Inter-Parliamentary Union, & Association of Secretaries General of Parliaments. (2023). Guide to digital transformation in parliaments. https://asgp.co/wp-content/uploads/2023/09/IPU_Digital_Transformation_Parliaments_EN_LR.pdf

[192] Inter-Parliamentary Union. (2024). World e-parliament report. https://www.ipu.org/resources/publications/reports/2024-10/world-e-parliament-report-2024

[193] Commonwealth Parliamentary Association. (n.d.). Home. Retrieved February 20, 2026, from https://www.cpahq.org/

[194] Commonwealth Parliamentary Association. (2025). Parliamentary security: An introductory guide. https://www.cpahq.org/media/q4tfx4i4/parliamentary-security_introductory_guide_final.pdf

[195] Commonwealth Parliamentary Association UK. (n.d.). e-Handbook on cybersecurity & cybercrime. Retrieved February 20, 2026, from https://www.uk-cpa.org/e-handbook-on-cybersecurity-cybercrime

[196] NATO Parliamentary Assembly. (n.d.). Home. Retrieved February 20, 2026, from https://www.nato-pa.int/

[197] NATO Parliamentary Assembly. (2025, May 25). NATO Assembly calls for decisive action on cyberattacks and disinformation, stronger partnerships. https://www.nato-pa.int/news/nato-assembly-calls-decisive-action-cyberattacks-and-disinformation-stronger-partnerships

[198] Organization for Security and Co-operation in Europe Parliamentary Assembly. (n.d.). Home. Retrieved February 20, 2026, from https://www.oscepa.org/en/

[199] ParlAmericas. (n.d.). Digital governance & AI. Retrieved February 20, 2026, from https://parlamericas.org/digital-governance-and-ai/

[200] Computer Emergency Response Team – European Union. (n.d.). IICB. Retrieved February 20, 2026, from https://cert.europa.eu/iicb/

[201] European Parliamentary Technology Assessment. (n.d.). Home. Retrieved February 20, 2026, from https://eptanetwork.org/

Chapter 16

[202] For more on this, see Baines, V. (2023). UK plc and supply chain cyber security: Where in the world is my data?. British Foreign Policy Group. https://bfpg.wpenginepowered.com/wp-content/uploads/2023/04/BFPG-UK-plc-and-Supply-Chain-Cyber-Security-April-2023-2.pdf

[203] Cybersecurity and Infrastructure Security Agency. (n.d.). Executive Order on improving the nation's cybersecurity. US Department of Homeland Security. Retrieved February 20, 2026, from https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity

[204] Regulation (EU) 2024/2847. Horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). European Parliament, Council of the European Union. https://data.europa.eu/eli/reg/2024/2847/oj

[205] Regulation (EU) 2024/1689. Harmonised rules on artificial intelligence (Artificial Intelligence Act). European Parliament, Council of the European Union. http://data.europa.eu/eli/reg/2024/1689/oj

[206] See, for example, the Biden Administration's Quantum Computing Cybersecurity Preparedness Act, signed into US law in December 2022. Quantum Computing Cybersecurity Preparedness Act, H.R. 7535, 117th Cong. (2021–2022). https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Quantum%20Computing%20Cybersecurity%20Preparedness%20Act.pdf

[207] European Commission. (2025). European Quantum Communication Infrastructure – EuroQCI. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[208] European Commission. (2024). IRIS2: The new EU secure satellite constellation. https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

Westminster Foundation for Democracy (WFD) is the UK public body dedicated to supporting democracy around the world. Operating internationally, WFD works with parliaments, political parties, and civil society groups as well as on elections to help make political systems fairer, more inclusive and accountable.

www.wfd.org

Scan here to sign up to WFD news

WFD

Westminster Foundation for Democracy is an executive Non-departmental Public Body sponsored by the Foreign, Commonwealth & Development Office.

Foreign, Commonwealth & Development Office