

Cybersecurity-as-a-Society (CaaS)

Victor Bohman Lind

Publication Date: December 2025

Abstract

A widening disconnect exists between digital system architectures and legislative governance frameworks. This paper examines this divide and proposes a paradigm shift. Cybersecurity must no longer be treated merely as an IT operational cost. Instead, it must be recognized as a foundational pillar of democratic stability, civic duty, and pan-European strategic autonomy. Through a cross-sector analysis focusing on European digital sovereignty and Swedish infrastructure resilience, we analyze technical vulnerabilities alongside high-level public policy to provide actionable recommendations for individuals, enterprise management, and policymakers.

1 Introduction

Cybersecurity has evolved from a niche operational IT function into a foundational element of national security, economic stability, and social cohesion. However, a persistent disconnect remains between digital system operators and the executive decision-makers who establish strategic goals and regulatory frameworks. This report bridges that gap by examining the intersection of technical cybersecurity practices with broader societal objectives pursued by governments, enterprises, and citizens.

Written from a European perspective with specific focus on Swedish governance, this analysis identifies technical measures that yield tangible public benefits. Recent events highlight the critical necessity of aligning technical expertise with legislative decision-making. Prominent examples include the European Council's Chat Control legislative debates and the implementation challenges of the "Millennium" healthcare system in Sweden's Västra Götaland region, which involved a complex enterprise vendor implementation.

1.1 Document Structure

The paper is structured as follows:

- **Section 2:** Defines *Cybersecurity-as-a-Society* by re-contextualizing the traditional CIA triad for macro-societal scope.
- **Section 3:** Conducts empirical and strategic research into systemic challenges, human factors, vendor dependencies, and legislative deficits.

- **Section 4:** Synthesizes concrete recommendations for citizens, enterprise executive teams, and legislators.

- **Section 5:** Provides concluding remarks on achieving long-term systemic resilience.

2 Defining Cybersecurity-as-a-Society

To effectively address societal cybersecurity issues, the traditional CIA Triad (*Confidentiality, Integrity, and Availability*) must be scaled from an organizational framework to a macro-societal paradigm.

2.1 Confidentiality

While organizational confidentiality traditionally focuses on internal access controls, societal confidentiality expands to encompass critical national infrastructure and population-wide data privacy. As of 2024, over 80% of European Union citizens rely on public cloud internet services for daily digital communications, including e-mail, messaging, and video conferencing. Immense volumes of private, commercial, and governmental data are concentrated among a few infrastructure providers. Significant systemic risks arise when provider practices misalign with public interest. Similar risks emerge when regulatory proposals mandate backdoors into encrypted communications, which introduces critical vulnerabilities susceptible to exploitation by state actors or illicit groups.

2.2 Integrity

Beyond preventing unauthorized database modifications, societal integrity involves mitigating the disruption of social cohesion and public trust by hostile entities. European social media usage is heavily concentrated within non-European platforms, primarily US-based entities and Chinese-owned applications such as TikTok. This market concentration introduces non-negligible risks of foreign cognitive influence and electoral manipulation. Furthermore, continuous probing by state-aligned threat actors seeking to subvert public institutions requires strategic, unified geopolitical resilience.

2.3 Availability

Organizational availability focuses on service uptime; societal availability addresses systemic dependencies and single points of failure. Modern democratic societies rely fundamentally on continuous digital availability. Over-reliance on centralized, foreign private providers creates critical structural vulnerabilities. Geopolitical shifts or private corporate realignments could severely disrupt essential public utilities and governance functions.

3 Research & Analysis

3.1 The Non-Malicious Human Element

Data from global breach evaluations, including the Verizon DBIR 2024, indicates that over 68% of cyber incidents involve a non-malicious human component. This vulnerability predominantly manifests in two domains:

1. **Social Engineering (~40% of breaches):** Techniques such as phishing and pretexting bypass technical controls by directly exploiting cognitive biases.
2. **Administrative Errors (~28% of breaches):** Configuration mistakes, such as misdirected sensitive communications or exposed cloud buckets, unintentionally compromise sensitive assets.

To foster systemic resilience, digital hygiene must be integrated into foundational educational curricula. This integration must be supported by clear legal frameworks establishing proportional negligence liability.

3.2 Commercial E-mail Provider Concentration

Approximately 85% of the global consumer and enterprise e-mail market is controlled by foreign third-party providers that lack default end-to-end encryption (E2EE). Many commercial business models rely on automated content indexing for targeted advertising, compromising confidential corporate and civic communications. Furthermore, an estimated two-thirds of European local and federal government entities rely on foreign proprietary cloud communication platforms.

3.3 Legacy System Retention and Debt

Maintaining legacy computing infrastructure poses severe risks. Industry surveys indicate that roughly 62% of enterprises maintain legacy software platforms that no longer receive vendor security updates. The primary justifications cited for retaining these vulnerable environments are functional adequacy, downtime avoidance, and upgrade costs. This approach leads to catastrophic system failures and emergency, uncoordinated migrations.

3.4 Legislative Disconnect and Expertise Deficit

Efforts to regulate digital domains frequently conflict with basic cryptographic and systems principles due to a lack of technical expertise among legislators. A prominent example is the European Council's Chat Control initiative, which initially sought to mandate server- or client-side scanning across encrypted platforms. The computer science community widely evaluated this measure as inherently destructive to public digital security. Demographic analyses of parliamentary bodies show an overrepresentation of legal and political science degrees. For example, these disciplines account for over 65% combined in bodies such as the German Bundestag, while technical or computer science backgrounds account for only a small fraction (~2%).

3.5 Social Media and Infrastructure Centralization

With roughly 88% of European youth (ages 16–29) utilizing social media, public discourse is mediated by algorithms owned by foreign entities. Concurrently, core web infrastructure displays severe hyper-centralization:

- **Hyperscalers:** AWS and Microsoft Azure route over 55% of global web traffic.
- **Edge and CDN Services:** Cloudflare handles approximately 20% of global web requests.

Misconfigurations at any single vendor create widespread cascading outages across financial, administrative, and public utility sectors.

4 Strategic Recommendations

4.1 For Individuals (Civic Cyber-Hygiene)

- **Adopt Digital Citizenship:** Treat operational security as a collective defense effort rather than an individual inconvenience.
- **Mandate End-to-End Encryption:** Transition everyday communication to privacy-respecting, end-to-end encrypted tools such as Proton or Signal.
- **Utilize Open-Source Ecosystems:** Transition to open-source applications and operating systems, including Firefox, LibreOffice, and Linux, to mitigate vendor lock-in.

4.2 For Organizations (Enterprise Strategy)

- **Proactive Legacy Decommissioning:** Budget and execute planned retirements of end-of-life systems rather than relying on patch-extended maintenance.

- **Vendor and Geographic Diversification:** Architect infrastructure across multi-cloud or self-hosted, localized European data centers to build resilience against hyperscaler outages.

4.3 For Policymakers (Regulatory Frameworks)

- **Bridge the Legislative Technical Gap:** Establish permanent, independent technical advisory boards within legislative bodies and encourage technical candidates for public office.
- **Mandate National Digital Literacy:** Integrate modern practical cybersecurity and media literacy into primary and secondary education.
- **Implement Negligence Liability:** Enact legal frameworks that assign proportional financial liability to organizations failing to maintain baseline security standards or running unsupported legacy software.

5 Conclusion

Transitioning to a true Cybersecurity-as-a-Society framework requires shifting from reactive IT patches to a holistic, shared policy model. By addressing human vulnerabilities, mitigating vendor concentration, grounding legislation in technical realities, and fostering open-source sovereign alternatives, European nations can safeguard both their critical infrastructure and democratic institutions.