RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

G7 FRANCE ÉVIAN 2026

GROUPE DE TRAVAIL CYBERSÉCURITÉ

CYBERSECURITY WORKING GROUP

G7 CYBERSECURITY WORKING GROUP DECLARATION
27 May 2026

France, under the leadership of ANSSI, hosted the G7 Cybersecurity Working Group plenary session on May 27th, 2026, in Paris, to advance our shared objectives on strengthening collective cyber resilience and strategic coordination. Discussions addressed the growing impact of cyber threats on national security and economic resilience, including the resilience of IT systems and critical infrastructure.

The G7 Cybersecurity Working Group provides a platform for coordination among G7 cybersecurity authorities to address evolving cyber threats, emerging technologies and strengthen protection of critical infrastructure and digital supply chains. It aims to enhance cooperation and information sharing, foster dialogue on standards and best practices at both national and international levels, and build sustainable resilience in the face of emerging technologies such as artificial intelligence and quantum computing.

During our meeting, we recognized and commended the work completed during Canada's presidency, with the development of two key Cybersecurity Working Group outputs, reflecting substantial progress in strengthening collective cyber resilience and coordination among G7 members.

- Minimum Elements on a SBOM for AI, negotiated by Germany and Italy, lists the minimum elements of AI systems to foster transparency, security and trust by enabling risks or vulnerabilities to be identified quickly. This document was published in mid-May 2026.
- G7 Cyber Working Group Statement on PQC Migration, negotiated by Canada, provides practical guidance for technical management in medium-to-large organizations to prepare organizations to transition to post-quantum cryptography.

Building on the work carried out under the Italian and Canadian presidencies, we convened to focus on the following four priorities for the French Presidency:

- **Call for a transition to post-quantum cryptography**. As computational power grows stronger, the quantum threat and the risk of retroactive attacks make the migration to Post-Quantum Cryptography an urgent matter that public and private organizations can no longer afford to delay. This transition will require coordinated action across industry and government to mitigate risks and enable secure adoption of PQC.
- **Promote a shared understanding of the cybersecurity risks from and to advanced artificial intelligence.** Generative AI, and specifically Large Language Models (LLMs), has become a cornerstone of modern digital innovation, offering unprecedented flexibility and efficiency to organisations. However, this technology is also being weaponized by cyber-threat actors. Furthermore, AI systems have emerged as high-value targets themselves: risks such as model poisoning, software supply chain compromises, and sensitive data exfiltration expand our attack surface. As appropriate, regulation,

policies or guidance, such as the G7 Minimum Elements of an SBOM for AI and other software security guidance, can help assess and reduce the cybersecurity risks to and from AI systems. For the new attack surfaces, international standards could help countries to adopt a robust and common approach to securing models, and countries could look to existing standards on AI security – or those currently being developed. The threat of increased automation by cyber-threat actors will require us to significantly improve the cybersecurity landscape by applying fundamental cybersecurity principles and modernisation across the board. In this evolving context, emerging AI cyber capabilities, such as AI-assisted vulnerability discovery and AI-assisted code generation, reinforce the importance of software security and the prioritization of smart, efficient patching to target the most critical vulnerabilities.

- **Strengthen the cybersecurity of telecommunications.** Telecom cybersecurity is now a paramount global issue. The technical complexity and growing interdependency of our networks creates a systemic risk. This vulnerability warrants specific attention from the G7, serving as a prime forum to foster the coordination of digital security policies among partners.
- **Enhance the cybersecurity of SMEs.** As cyber threats increasingly permeate every layer of society, a critical public policy challenge is to elevate the digital maturity of all stakeholders—from individual citizens and large corporations to Small and Medium-sized Enterprises (SMEs). Given that SMEs form the backbone of the global economy, a cyberattack targeting them presents a systemic risk. Consequently, SME cybersecurity is now a fundamental pillar of national and economic resilience. Our governments share a responsibility for creating an environment where the parties best able to address a risk are the ones empowered and expected to do so. SMEs are critical and so we must expect, in particular from technology vendors, to ensure the cybersecurity of the products SMEs use. If products are secure by design, we can help secure our critical SMEs without putting undue process and financial burden on them.

The Working Group intends to continue these efforts throughout the rest of the French G7 presidency in 2026. A second meeting in fall 2026 will bring together participants to review progress and finalize the work prior to transitioning the presidency of the Working Group to the United States of America for 2027.