
# November 2025 Cyber News

*On behalf of the Yuval Ne'eman Workshop for Science, Technology and Security, we are happy to share with you some of the most interesting events and developments that took place in November 2025.*

**November 4 – Google Cloud Security released its 2026 Cybersecurity Forecast** The report highlights three key trends: (1) the use of AI in cyberattacks; (2) evolving cybercriminal tactics; (3) nation-state operations linked to Russia, Iran, China, and North Korea. The authors anticipate growing deployment of AI agents within organizations for cybersecurity tasks, which will require identity and access management systems to treat such agents as distinct digital entities, independent of human users. However, the use of unauthorized AI agents by employees may increase the risk of sensitive data leaks. On the cybercrime field, the report warns of increased financially motivated attacks on virtualization infrastructure supporting virtual machines, which has become a security gap due to outdated software and other factors. Finally, the authors predict that Chinese state-backed hackers may ramp up espionage operations targeting semiconductor manufacturing facilities, driven by U.S. export controls and the expanding domestic AI sector in China.

**November 5 – India Released National Framework for AI Governance Under IndiaAI Mission**
India's Ministry of Electronics and Information Technology released its National Framework for AI Governance as part of the IndiaAI Mission, a government-backed initiative approved in March 2024 to promote the safe, ethical, and responsible cross-sectoral adoption of AI. Grounded in seven core principles, the framework sets out policy recommendations across three-time horizons. In the short term, the plan calls for the creation of an Artificial Intelligence Governance Group (AIGG) to shape and oversee India's position on AI governance. In the medium term, the framework guides the development of unified standards for content authentication, data

integrity, and cybersecurity, alongside sandbox-based pilot programs in high-risk domains. In the long term, it recommends continuous evaluation of governance mechanisms, new legislation responsive to evolving risks, and enhanced international cooperation to harmonize global standards. The framework also sets out specific guidelines for AI developers, system users, and regulators, emphasizing compliance with Indian laws governing IT, data protection, and copyright, and encourages the use of flexible, reviewable regulatory mechanisms.

**November 12 – US Extended Key Cybersecurity Measures Following Government Shutdown**

US President Donald Trump signed the Continuing Appropriations, Agriculture, Legislative Branch, Military Construction and Veterans Affairs, and Extensions Act, 2026. The law provides ongoing appropriations for the 2026 fiscal year and restores continuity of government operations after a 43-day shutdown. In the field of cybersecurity, the law extends until January 30, 2026, three major provisions that expired on September 30, 2025. These include: (1) the 2015 Cybersecurity Information Sharing Act, which promotes the exchange of cyber threat indicators between the private sector and federal government while offering legal protections related to privacy and antitrust concerns; (2) the Federal Cybersecurity Enhancement Act, aimed at strengthening cybersecurity across federal systems, including mandatory implementation of best practices such as multi-factor authentication for high-risk users; (3) the State and Local Cybersecurity Grant Program, a DHS initiative for enhancing cybersecurity capabilities at the state and local levels, particularly for critical infrastructure, through strategic planning, cyber exercises, and the recruitment of cybersecurity professionals.

**November 13 – Anthropic Reported First Known Use of Agentic AI in Cyber Espionage**

AI firm Anthropic published a report detailing the first documented use of agentic AI in a cyber espionage campaign. According to the findings, the China-backed group GTG-1002 conducted cyber espionage attacks in September 2025 against nearly 30 targets, including financial institutions and chemical manufacturers, with only some of the attacks reported as successful. The attackers leveraged Claude Code, Anthropic's AI code generation tool, to automate 80–90% of the operation. The campaign began with identifying targets and gathering reconnaissance, then moved on to uncovering system weaknesses and crafting malicious code tailored to those vulnerabilities. From there, the attackers stole credentials, moved laterally through internal networks, and ultimately extracted data — which Claude later sorted and classified by its sensitivity. Anthropic noted that while Claude enabled significant automation, it still exhibits errors – such as flagging outdated vulnerabilities – that currently limit fully autonomous cyberattacks.

---