December 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 December 2025.

December 2 – US Lawmaker Pfluger Introduced Bill to Formalize Federal Responses to Foreign Cyberattacks

US Representative August Pfluger introduced The Cyber Deterrence and Response Act. The bill would authorize the President to designate foreign actors responsible for significant cyberattacks against the United States as major cyber threat actors. Such attacks are defined as incidents that result in disruption to the availability of computer networks, damage to critical infrastructure, theft of personal data or trade secrets, or interference in the electoral process. The legislation would also allow the President to impose a range of sanctions on designated actors, including the suspension or restriction of US financial or security assistance. The bill grants the President authority to waive the imposition of sanctions for up to one year, with the option of renewal, provided that a written justification is submitted to Congress stating that the waiver is necessary for national security reasons or for a significant humanitarian purpose. In addition, the National Cyber Director would be tasked with developing a national attribution framework to establish a criteria-based process for attributing state-sponsored cyberattacks, including mechanisms for cooperation with allies on evidence validation and the development of consistent principles for the public attribution of cyber operations.

December 2 – Australia Released Its National Artificial Intelligence Strategy

The Australian Government's Department of Industry, Science and Resources (DISR) published Australia's National AI Strategy. The strategy is structured around three core objectives: (1) building national AI capabilities through investment in digital and physical infrastructure; (2) ensuring that all Australians benefit from the opportunities created by AI; (3) promoting the safe adoption of AI across both the public and private sectors. For each objective, the strategy outlines a set of dedicated policy actions. To support capability-building, the government will develop a framework to guide the secure establishment and operation of data centers nationwide. For advancing the second objective, the Department of Education and the Department of Employment and Workplace Relations will collaborate on equipping students with AI-related skills before entering the workforce. Finally, in support of the third objective, the Department of Foreign Affairs and Trade and DISR will lead the development of a government strategy for regional leadership in AI, aimed at embedding values of transparency and safety within international AI norms.

December 8 – Check Point Published a Cyber Threats Report on US Government Institutions and Critical Infrastructure

The report presents a classification of hacker groups targeting critical infrastructure in the US According to the analysis, attacks pursuing strategic objectives are carried out primarily by APT groups linked to China and Russia and are characterized by utilizing Living off the Land techniques to establish long-term persistence within target networks. In contrast, attacks aimed at achieving financial gain are conducted mainly by ransomware criminals. The report further notes that many attacks target organizations in the healthcare sector, in part due to comparatively lower levels of cybersecurity maturity and a higher willingness to comply with ransom payment demands. In parallel, the report's author outlines potential trends in future cyber threats through 2030, including a projected increase in supply chain attacks carried out through compromises of CI/CD processes and software package repositories. The report recommends that the federal government and critical infrastructure operators strengthen the security of operational technology systems and industrial control systems, including through proactive threat hunting activities and enhanced cooperation between the public and private sectors.

December 16 – Greece Published Its National Cybersecurity Strategy

The Greek government's Ministry of Digital Governance published Greece's National Cybersecurity Strategy for 2026-2030 to align Greece's national cyber resilience with the levels observed in the European Union's most advanced member states. The strategy is grounded in five core principles: (1) establishing an effective cybersecurity management system within the public sector; (2) strengthening technical capabilities for the prevention of, preparedness for, and response to cyber incidents; (3) developing professional skills and expertise in cybersecurity; (4) promoting cooperation between the public and private sectors,

as well as international cooperation, in the field of cybersecurity; and (5) monitoring the implementation of the strategy and adapting it to technological developments. In line with these principles, the strategy seeks to enhance cybersecurity capabilities and awareness across the private sector and small businesses, while encouraging international cooperation to prevent cybercrime. In parallel, it promotes the establishment of a national framework for security risk assessment and for improving the security of supply chains and critical infrastructure.

December 18 – Countries and TikTok have Signed Joint Declaration to Launch Initiative against Cyber Crime

Thailand, Bangladesh, Nepal, Peru, the United Arab Emirates, and TikTok have signed a joint declaration launching a new cooperative initiative to combat online scams, including cyber fraud. The declaration was signed during an international conference on cooperation against online crime held in Bangkok, led by the Ministry of Foreign Affairs of Thailand and the United Nations Office on Drugs and Crime. The joint declaration establishes a framework for action and commitments across several areas, including the implementation of international conventions against transnational crime, including the United Nations Convention against Cybercrime; the promotion of legislation and the strengthening of national response capabilities; information and intelligence sharing to prevent and disrupt online crime; and the launch of public awareness campaigns on online crime. In addition, the signatory states committed to continued monitoring of trends in online crime, assessing the effectiveness of response measures, and considering the convening of additional conferences aimed at reducing online scams.
