February 2025 Cyber News

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

February 4 – Greece and Cyprus Deepened Cybersecurity Collaboration at Inaugural Summit – The inaugural Cyber Intelligence Summit was held in Athens, where Greek Minister of Digital Governance, Dimitris Papastergiou, and Cypriot Deputy Minister for Innovation, Nicodemos Damianou, announced plans to strengthen cybersecurity cooperation between their countries. During the summit, the ministers discussed joint efforts to combat ransomware attacks, address the threat of deepfake content, and protect critical infrastructure—such as undersea cables—from both physical and cyber threats.

February 5 – Justice Department Disbanded FBI's Foreign Influence Task Force – The newly appointed U.S. Attorney General, Pam Bondi, has issued a memorandum directing the closure of the FBI's Foreign Influence Task Force (FITF). Established in 2017 by former FBI Director Christopher Wray, the FITF collaborated with the intelligence community, federal agencies, and the private sector to investigate and disrupt foreign influence efforts targeting U.S. public opinion and elections—primarily from adversaries such as Russia and China. According to Bondi, the decision aims to optimize the Department of Justice's resource allocation, including reducing criminal proceedings related to the Foreign Agents Registration Act (FARA). This law requires individuals and entities operating on behalf of foreign governments or organizations to disclose their activities to the Justice Department. Following this policy shift, FARA enforcement will be restricted to cases involving espionage in its narrowest sense.

February 6 – New UK Organization has Begun Measuring Cyber Incident Impact – The British Cyber Monitoring Center (CMC), a non-profit organization, has officially commenced its operations to measure the expected impact of cyber incidents. The CMC will monitor significant cyber events, classify their severity using a five-tier scale, and publicly report key details and consequences. Leveraging methodologies used to assess the impact of natural disasters, the CMC aims to rank cyber incidents based on the number of organizations that have sustained financial losses of £1,000 or more, alongside the total cumulative economic damage caused.

February 7 – China and Thailand Signed Cybersecurity and Anti-Fraud Cooperation Agreements – Chinese Premier Li Qiang and Thai Prime Minister Paetongtarn Shinawatra have signed 13 joint agreements to enhance strategic cooperation between their countries, including in cybersecurity, technology, innovation, and science. As part of these agreements, both nations committed to expanding collaboration between their law enforcement agencies to combat transnational crime, with a particular focus on cybercrime and online fraud in the Mekong River region, which includes China, Thailand, Myanmar, and Laos. Additionally, the two governments agreed to establish a Cyber Fraud Coordination Center in Bangkok. The agreements were signed during Shinawatra's visit to Beijing and follow Thailand's February 5 announcement that it had cut electricity and internet services to three areas in Myanmar, which had been used by criminal gangs to orchestrate online fraud schemes targeting China and Thailand

February 19 – Israel Outlined New National Cybersecurity Strategy – Israel's National Cyber Directorate published its National Cybersecurity Strategy for 2025-2028, focusing on strengthening the country's cyber defenses in response to cyberattacks during the Israel-Hamas War. Key elements of the strategy include implementing a national digital identity verification program to reduce identity theft and bolster the protection of supply chains for entities providing critical services. The government will also work on a coordinated readiness and response to cyber incidents by establishing a National Security Operations Center (NSOC) and fostering cybersecurity researchers to report new threats voluntarily. Additionally, the strategy emphasizes the development of skilled cybersecurity professionals, including expanding education and training programs starting from primary and middle schools. On the international front, Israel aims to deepen cooperation with allied nations and international organizations to establish agreed-upon behavioral norms and develop advanced defense technologies.

Make sure you don't miss the latest on cyber research
Join our mailing list