February 2026 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 February 2026.

February 2 – American Lawmakers Introduced Legislation toStrengthen Energy Sector Cyber Resilience – U.S. Senators Kathy Castor and Gabe Evans introduced the bipartisan Energy Threat Analysis Center Act of 2026, aimed at strengthening the cyber resilience of the U.S. energy sector. The bill seeks to update the Department of Energy's Energy Sector Operational Support for Cyberresilience program, originally established under the 2021 Infrastructure Investment and Jobs Act (IIJA), in order to deepen cooperation between the federal government and energy companies. The proposed amendments would expand information sharing – both classified and unclassified – enhance the analysis of potential threats, and provide mitigation recommendations. The legislation also aims to improve the energy sector's understanding of adversaries' tactics, techniques, and procedures (TTPs), indicators of compromise (IoCs), and operational capabilities. To that end, it would authorize the Secretary of Energy to establish an Energy Threat Analysis Center, to be located at one or more physical sites. In addition, the bill would extend the program's authorization through 2031.

February 3 – Fiji Approved Its National Cybersecurity Strategy for 2026-2031 – Under the strategy, which has not yet been released to the public, Fiji will work to strengthen its national capabilities in cyber threat detection, incident response, and recovery to routine operations. In addition, Fiji will foster a skilled and diverse cybersecurity workforce, enhance national awareness of cyber threats, and advance regional and international cooperation to address cybersecurity challenges. The government also approved an accompanying action plan.

February 11 – Google Identified State-Linked Cyber Campaigns Targeting Defense Firms Globally – Google's Threat Intelligence Group (GTIG) published a blog post detailing cyber threats it identified targeting of the defense industrial base. According to the post, the Russian threat actor UNC5125 circulated a Google Forms questionnaire among military drone operators, falsely claiming it had been issued by the Ukrainian drone training academy Dronarium. Through the form, the group sought to collect information on operators' preferred communication applications, which it later exploited to distribute malware. In addition, the North Korean threat actor APT45 deployed the SMALLTIGER malware against companies in South Korea's defense, semiconductor, and automotive sectors, reportedly with the aim of stealing intellectual property that could support research and development programs in those industries in North Korea. Finally, the Chinese threat actor APT5 conducted two spear-phishing campaigns in the second half of 2024 and in May 2025 targeting employees at aerospace and defense companies. The phishing emails were tailored to recipients' roles, locations, and professional interests, and included, among other elements, invitations to industry events and job offers.

February 12 – Ukraine and Sweden Signed Five-Year Cybersecurity Cooperation Agreement – The State Service of Special Communications and Information Protection of Ukraine (SSSCIP) and Sweden's National Cyber Security Centre (NCSC) signed a five-year memorandum of understanding to advance bilateral cooperation in cybersecurity. Under the memorandum, the two countries will conduct joint training programs and exercises, during which Sweden will support efforts to deepen the professional expertise of Ukrainian cybersecurity specialists. The parties will also utilize advanced technologies and secure channels to share cyber threat intelligence. In turn, Ukraine will provide Sweden with insights derived from its experience in countering cyber warfare with Russia, aimed at strengthening the protection of Swedish government systems and critical infrastructure.

February 20 – India Enacted New Rules on AI-Generated Content – Amendments to India's 2021 Information Technology Rules, issued by the Ministry of Electronics and Information Technology (MeitY), have entered into force, introducing new obligations for Significant Social Media Intermediaries (SSMIs) regarding AI-generated synthetic content. Under the amendments, platforms that allow users to upload visual or audio content are required to mandate clear disclosure from content creators when such material has been generated synthetically. Platforms must also implement verification mechanisms to validate these disclosures, clearly label synthetic content, and publish it together with technical mechanisms enabling traceability of the resources used in its creation. In addition, SSMIs are required to deploy technological safeguards to prevent the creation and dissemination of certain categories of prohibited content, including fabricated documents and non-consensual intimate material. The regulations further mandate that SSMIs comply with official takedown orders within three hours and address urgent user complaints seeking content removal within two hours.

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

♿

The Blavatnik Interdisciplinary Cyber Research Center | Israel | +97236406041