January 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 January 2025.

January 1 – Lithuanian Armed Forces Established New Cyber Command – The Lithuanian Cyber Command (LTCYBERCOM) will plan and execute cyber operations while ensuring interoperability with NATO forces. Additionally, the command will oversee the implementation of strategic and operational IT and communication systems within Lithuania. The Ministry of Defense spearheaded the establishment of LTCYBERCOM, which was made possible by a July 2024 amendment to the law defining the principal structure of the Lithuanian Armed Forces, which the Seimas, Lithuania's parliament, approved.

January 2 – MITRE and Japan's NICT Partnered to Advance AI-Driven Cyber Defense Research – The MITRE Corporation and Japan's National Institute of Information and Communications Technology (NICT), under the Ministry of Internal Affairs and Communications (MIC), will launch a joint research initiative in April 2025 to enhance cybersecurity defenses against AI-driven attacks. The research aims to bolster protections against cyberattacks launched by hacker groups backed by the Chinese government and position Japan as a strategic partner to the U.S. in addressing cyber threats in the Asia-Pacific region. As part of the collaboration, NICT will establish a research center in Washington, D.C., to gather data on AI-driven cyberattacks, such as advanced DDoS and ransomware operations, originating from non-English-speaking regions and nations. This effort addresses a gap in U.S. cybersecurity research, which traditionally concentrates on English-speaking regions. Additionally, in 2025, the Japanese government will draft guidelines for leveraging artificial intelligence in mitigating cyberattacks and launch a dedicated website to showcase real-time examples of AI-driven cyber threats.

January 7 – Tech Giants Meta and Google Move Away from Fact-Checking, Embrace User-Driven and AI Detection Solutions – On January 7, Mark Zuckerberg, founder and CEO of Meta, announced that the company will discontinue its fact-checking program aimed at countering disinformation across its platforms and replace it with a Community Notes system, similar to that used on the X platform. Through the program, Meta collaborated with third-party fact-checkers accredited by the International Fact-Checking Network (IFCN), who assessed the credibility of content, limited its reach when necessary, and provided clarifications. In contrast, the Community Notes system will allow users to add clarifications to posts rather than remove them, suggest counterclaims, or identify and report misleading information. According to Zuckerberg, Meta will continue to use automated systems to remove content related to terrorism, online fraud, and drug trafficking.

Additionally, on January 16, Kent Walker, Google's President for Global Affairs, informed Renate Nikolay, Deputy Director-General of the European Commission's Directorate-General for Communications, Networks, Content, and Technology (DG CONNECT), that the company will not implement its fact-checking program across its platforms and content ranking and removal systems. According to Walker, implementing the fact-checking program on Google services has proven ineffective, and the company now intends to enhance existing tools, such as digital watermarking, to identify AI-generated content.

January 8 – Turkey Launched Cybersecurity Directorate and Proposed New Legal Framework – On January 8, the Turkish government announced the enactment of Presidential Decree No. 177, which established the Cybersecurity Directorate (also referred to as the Cybersecurity Presidency). The Cybersecurity Directorate will develop national cybersecurity policies, strategies, and legislation while coordinating and monitoring their implementation. It will also draft emergency response plans, establish joint operation centers for crisis management, and promote collaboration among the public, private, and academic sectors.

Moreover, on January 16, it was revealed that Turkey's Parliament is reviewing a draft Cybersecurity Law to define the Cybersecurity Directorate's authority, including creating policies to protect critical infrastructure and private companies. The law grants officials the power to seize electronic devices without judicial oversight and impose prison sentences ranging from two to five years for data leaks. The law also outlines that the Cybersecurity Council will oversee the Directorate's actions and may impose restrictions on digital services. Proponents argue that this law addresses gaps left by the 2022 Disinformation Law in combating cyber threats and cybercrime.

January 14 – UK Government Launched Public Consultation on Ransomware Legislation – The UK Home Office has published a public consultation document to advance legislation to tackle the growing threat of ransomware attacks. The document proposes a ban on all public sector organizations and operators of critical infrastructure from paying ransom demands to attackers. Additionally, the document calls for establishing a mechanism to prevent ransom payments, which would require organizations to notify the Home Office before making any ransom payments and guide them in responding to such attacks. Furthermore, the document mandates the creation of a reporting mechanism for ransomware attacks, aiming to impose a reporting duty on such incidents within 72 hours. Following the public consultation period, the government will publish an official response on April 8, 2025, ahead of introducing the legislation for parliamentary discussion.

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