March 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 March 2025.

March 9 – North Korea Established 'Research Center 227' to Enhance AI-Powered Cyber Capabilities – Under the direction of North Korean leader Kim Jong-Un, North Korea's military intelligence agency (Reconnaissance General Bureau – RGB) has begun establishing a new research center named Research Center 227 in the capital city of Pyongyang. The center is dedicated to developing advanced technologies for attacking the cybersecurity systems of Western countries and global computing networks. The center's primary objectives include researching and developing advanced hacking techniques, creating AI-powered technologies for stealing sensitive information and financial assets, and producing automated data collection and analysis software. As part of its establishment, the RGB plans to recruit approximately 90 top-tier experts specializing in software development, automated systems, and information security.

March 11 – NIST Selected HQC as Fifth Algorithm for Post-Quantum Encryption Standard – The U.S. National Institute of Standards and Technology (NIST) announced the selection of the HQC algorithm as the fifth algorithm to be used for drafting a post-quantum encryption standard. HQC was chosen as part of the fourth round of NIST's project to standardize algorithms for preparing the shift to post-quantum asymmetric encryption, which was launched in December 2016. As part of the project, NIST selected the CRYSTALS-Kyber algorithm for encryption and the CRYSTALS-Dilithium, FALCON, and SPHINCS+ algorithms for digital signatures in July 2022. According to NIST, HQC will serve as a backup to the ML-KEM algorithm, based on the CRYSTALS-Kyber algorithm, and used for encrypting data in public networks. NIST plans to release a draft standard for the use of HQC for public comment within a year, with the final standard expected to be published in 2027.

March 13 – FCC Formed National Security Council to Address Cyber Threats to U.S. Communications Sector – The Chairman of the American Federal Communications Commission (FCC), Brendan Carr, launched the FCC's National Security Council, designed to address threats to the U.S. communications sector, including cyberattacks, primarily from U.S. rivals, with China at the forefront. The council, led by FCC National Security Advisor Adam Chan, will include representatives from eight departments and offices within the FCC. Its mission is to reduce the dependence of U.S. communications and technology sectors on trade and supply chains from foreign adversaries. In addition, the council will work to address vulnerabilities that expose the U.S. to cyberattacks, espionage, and surveillance activities from foreign rivals. Furthermore, the council will focus on advancing U.S. technological superiority, particularly in areas such as 5G networks, IoT systems, and quantum computing.

March 18 – Singapore Introduced New Military Units to Enhance National Cyber Defense – As part of a reorganization aimed at addressing sophisticated and evolving cyber threats, the Digital and Intelligence Service (DIS) of the Singapore Armed Forces (SAF) launched two new structural initiatives. First, DIS established the Cyber Defense Command (DCCOM), which will operate as a unified command to protect the Ministry of Defense and the Singapore Armed Forces (SAF) from cyber threats, enhance operational and defensive capabilities, and promote collaboration with the entire government sector and industry in Singapore as part of the national cybersecurity defense. DCCOM will integrate existing units and create two new ones: the Cyber Protection Group (CPG) and the Cyber Threat Intelligence Group (CTG). The CPG will collaborate with the Singapore Cyber Security Agency (CSA) and other relevant agencies to enhance the protection and resilience of critical information infrastructures. The CTG will focus on early threat detection and conducting cyber threat intelligence assessments. Additionally, the SAF C4 Command has been expanded into the SAF C4 & Digitalisation Command (SAFC4DC). In its role, SAFC4DC will consolidate and manage all software and hardware capabilities, aiming to accelerate and integrate digitization processes within the Singapore Armed Forces. It will also lead the development of the operational digital framework, developing and managing IT systems for operational support and expanding the adoption of artificial intelligence technologies.
