March 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 March 2026.

March 1 – Vietnam's Artificial Intelligence Law Came into Force – The law on Artificial Intelligence, approved by the National Assembly of Vietnam on December 10, 2025, applies to government entities, private companies, and individuals involved in the development, commercialization, or use of AI systems in Vietnam. It establishes four core principles, including ensuring human oversight at all stages of system operation and preventing discrimination or bias in their functioning. At the same time, the law defines a list of prohibited uses of AI systems, including actions that may harm public order. It introduces a three-tier classification of AI systems—low, medium, and high risk—based on the potential harm to human rights or national security that may arise from their development or deployment, and accordingly imposes differentiated obligations on developers and users. In parallel, the law is also intended to advance Vietnam's AI ecosystem. As part of this effort, Vietnam will establish regulatory sandboxes to test new AI developments and launch funding mechanisms to support research, development, and implementation initiatives in AI.

March 4 – Flashpoint Published Findings on Cyberattacks Conducted During Epic Fury Operation – According to the blog post, on March 2, U.S. cybersecurity researchers identified a cyber campaign known as #OpIsrael, during which pro-Iranian and pro-Russian hacker groups claimed to have targeted entities in Israel, the United States, and the Gulf states, including Elbit systems and Israeli defense organizations. On March 5, Flashpoint identified a

renewed increase in the scope of activity associated with the campaign. Among other developments, the Iranian-affiliated group Handala claimed to have carried out a doxxing operation targeting individuals it alleged to be connected to the Israeli intelligence community. In the post, the authors recommended that organizations operating industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems segregate industrial networks from corporate IT networks and from public internet access, and implement multi-factor authentication (MFA) for privileged accounts.

March 6 – The White House Released President Trump's Cyber Strategy – The strategy aims to ensure the United States' ability to proactively and rapidly neutralize cyber threats, while promoting coordinated action across all federal government branches and strengthening cooperation with international allies, the private sector, and academia. The strategy outlines six policy principles: (1) shaping adversary behavior, including by leveraging the full range of U.S. national power to impose costs on malicious actors; (2) advancing balanced cybersecurity regulation by reducing regulatory burdens and improving international coordination between regulators and the private sector; (3) promoting modernization and strengthening the resilience of federal information systems; (4) enhancing the protection of critical infrastructure and their supply chains by reducing dependence on suppliers and products from adversarial states; (5) maintaining U.S. leadership in critical and emerging technologies, including through the securing the data, infrastructure, and models underpinning U.S. leadership in AI; (6) developing cyber workforce and capabilities by promoting collaboration among the private sector, government, and academia.

March 9 – The UK Government Published a Strategy to Combat Online Fraud and Cybercrime – The strategy is allocated a budget of at least £250 million (approximately $331 million) and is structured around three pillars. First, with regard to the proactive and effective disruption of crime in the UK, the government intends to launch an Online Crime Centre (OCC) in April 2026, which will operate in cooperation with the National Cyber Security Centre (NCSC), cybersecurity companies, and additional stakeholders to facilitate data and capability sharing and to coordinate efforts against fraud. Second, in strengthening the resilience of citizens and businesses against fraud, the Home Office will work in cooperation with the City of London Police throughout 2026 to coordinate and enhance the activities of the Fraud and Cyber PROTECT networks. Finally, in improving response measures to fraud and support for victims, the Home Office will collaborate with the Economic and Cyber Crime Academy (ECCA) of the City of London Police and the College of Policing (CoP) to implement, by 2028, recommendations from a professional skills review aimed at enhancing police capabilities in addressing fraud, economic crime, and cybercrime.

March 15 – Egypt Released National AI Policy – Egypt's National Council for Artificial Intelligence, Quantum Computing and Emerging Technologies (NCAI) published three documents outlining policy principles for AI and guidance for its safe adoption. The first document presents a vision aimed at positioning Egypt as a regional hub for responsible AI innovation, while strengthening national capabilities and promoting the development of AI systems that advance human

well-being. Among other elements, the document identifies the bodies responsible for shaping AI policy in Egypt and defines their authorities, including the National Telecom Regulatory Authority (NTRA), which is tasked with approving and licensing AI-enabled hardware and IoT devices. The document also addresses investment in key components required for the development of the national AI ecosystem. In this context, NCAI, in cooperation with the Ministry of Communications and Information Technology, is set to introduce mandatory training in AI governance for public sector employees responsible for procurement and oversight processes, with the aim of equipping them with the skills needed to manage AI procurement contracts and conduct relevant impact assessments. Alongside this document, NCAI published two complementary papers. The first outlines practical steps to promote the safe use of AI, presenting a three-stage model for its trustworthy development and deployment, while the second sets out principles for advancing the safe development and use of generative AI.
