May 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 May 2026.

May 7 – Investigation Revealed Training of Hackers and Intelligence Officers for Russia's GRU at Moscow University – VSquare, a media organization bringing together journalists from the Visegrád countries, published an investigation into the training of hackers and intelligence officers for Russia's Main Intelligence Directorate (GRU) at Bauman Moscow State Technical University (BMSTU). The investigation is based on approximately 2,000 internal documents obtained by European media outlets. According to the report, the training is conducted within Department No. 4 at BMSTU, where students are exposed to detailed information regarding the operation of protected computer networks within the US Department of Defense. Students also receive extensive training in penetrating foreign computer systems, covering a range of attack methods from simple password-based attacks to the use of Trojan horses. In addition, one of the department's courses teaches the production of manipulated video content for dissemination on social media as part of influence operations. As part of their studies, students complete internships with organizations operating under the auspices of the Russian government, including the Gamma Research Center for Information Systems Protection.

May 10 – UAE Entities Signed Agreement to Accelerate Transition to Post-Quantum Cryptography – The UAE Cyber Security Council and the Advanced Technology Research Council signed an agreement to accelerate the country's transition to post-quantum cryptography and strengthen national cyber resilience. The agreement aims to support the deployment and expansion of cybersecurity solutions developed within the ATRC ecosystem that facilitate the transition, including a platform for cryptographic discovery, inventory management, and vulnerability assessment; an Entanglement-Based Quantum Key Distribution technology; and national cryptographic libraries incorporating both classical and post-quantum

cryptographic algorithms. In addition, the agreement includes national training and preparedness programs, as well as initiatives designed to assist organizations in carrying out the transition in accordance with standards developed by the US National Institute of Standards and Technology and other relevant standards.

May 13 – Two Leading AI Models Achieved High Success Rates in Complex Cybersecurity Tasks – The UK AI Security Institute published a blog post presenting an evaluation of the GPT-5.5 model and a new version of Claude Mythos Preview. The assessment aims to measure the models' ability to perform cybersecurity tasks at a success rate of at least 80% relative to the time required by human experts. The evaluation found that both models were capable of completing tasks that human cybersecurity experts typically perform over the course of several hours. In particular, both models completed the longest tasks with success rates approaching 100%, despite being subject to a limit of 2.5 million tokens per task. The assessment also found that the two models were the only ones able to complete all 32 stages of "The Last Ones" attack scenario, which simulates a breach of a corporate network. In addition, Mythos Preview successfully completed the "Cooling Water" attack scenario—a seven-stage attack against industrial control systems—an achievement not previously reached by any AI model.

May 14 – CrowdStrike Reported Rising Cyber Threats to the Global Financial Sector – CrowdStrike published a report reviewing the key trends, incidents, and operational patterns that shaped the cyber threat landscape targeting the global financial sector between April 2025 and March 2026. According to CrowdStrike, the attacks targeted, among other regions, on Canada, India, and Indonesia, reflecting a focus on major financial hubs and rapidly growing digital economies. The report also notes an increase in "Big Game Hunting" ransomware attacks during 2025, targeting large organizations perceived as more capable or likely to pay ransom demands. According to the findings, China-linked groups represented the most significant intelligence-gathering threat to financial institutions, particularly in South and Southeast Asia, likely seeking information on economic conditions, personally identifiable information, and data that could support future espionage operations. The report's authors recommended strengthening defenses against social engineering attacks and identity-based intrusions by enhancing identity verification procedures for password resets and multi-factor authentication, while prioritizing the remediation, monitoring, and rapid updating of perimeter security technologies and internet-facing services.

May 20 – USCYBERCOM and NSA Established Task Force to Accelerate AI Integration – US Cyber Command and the National Security Agency established a new task force dedicated to accelerating the integration of artificial intelligence tools for national security purposes. The initiative aims to examine how advanced AI models developed by private-sector companies, including Google and OpenAI, can be securely integrated into the organizations' missions and classified systems. The task force will be staffed primarily by technical experts from the NSA's Artificial Intelligence Security Center and will be led by a commander from US Cyber Command.
