April 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 April 2026.

April 3 – Cambodia's Law on Combating Online Fraud Entered into Force – Cambodia's Law on Combating Online Fraud entered into force after being approved by the country's National Assembly. The law aims to address online fraud conducted through the use of technology as a means of committing offenses, both within Cambodia and abroad when such activities involve Cambodian citizens or when assets or proceeds related to the offense are transferred into Cambodian territory. The law assigns responsibility for combating fraud to judicial police investigators, while allowing the government to establish a dedicated mechanism for addressing online fraud, responsible for leading, coordinating, and overseeing prevention, suppression, and enforcement activities. The law establishes penalties ranging from two to five years of imprisonment and fines between 200,000,000 and 500,000,000 riel (approximately USD 50,000–125,000). It further introduces aggravated penalties of five to ten years of imprisonment and fines between 500,000,000 and 1,000,000,000 riel (approximately USD 125,000–250,000) when offenses are committed by organized crime groups or against multiple victims. Finally, the law regulates international cooperation with foreign states on extradition and mutual legal assistance, including investigation, information collection and sharing, suspect identification, and asset tracking.

April 7 – Anthropic Introduced Claude Mythos Preview Model – Anthropic introduced the Claude Mythos Preview model, a frontier model belonging to the category of general-purpose AI models. Claude Mythos Preview is capable of identifying zero-day vulnerabilities that are difficult to detect using existing security measures, including vulnerabilities that had remained undiscovered for extended periods, with the oldest identified vulnerability having gone undetected for 27 years. However, the company stated that the model developed exploitation methods for identified vulnerabilities within a matter of hours, whereas penetration testing experts estimated that such processes would typically require several weeks. In light of these

capabilities, Anthropic limited access to the model to a small group of private sector companies, including Microsoft and companies participating in the Glasswing project, with the aim of enabling them to use the model to identify zero-day vulnerabilities in major operating systems and web browsers.

April 14 – NIST Released Draft Guidance to Help Sole Proprietors Manage Cybersecurity Risks – The U.S. National Institute of Standards and Technology published a draft document for public comment intended to assist self-employed individuals in managing their cybersecurity risks. The document supports the implementation of version 2.0 of the Cybersecurity Framework, published by the institute in February 2024. As part of applying the Protect function of the framework, NIST outlined recommended measures for defending against ransomware attacks, including configuring operating systems and third-party software to allow only authorized applications to run, and prioritizing the use of standard user accounts with multi-factor authentication over accounts with administrative privileges. In addition, to facilitate implementation of the framework, the document includes various annexes, including examples of how small business owners across different sectors can apply the framework's principles, as well as a template for documenting and assessing cybersecurity risks across business assets.

April 15 – UK Institute for Strategic Dialogue Reported Coordinated Pro-Iranian Networks on X – The UK-based Institute for Strategic Dialogue published a study examining the activity of two pro-Iranian networks, BRICS4CLICKS and Verified4War, which operated in coordination on the X platform during the first month of Operation "Rising Lion." According to the findings, content published by the networks generated more than one billion views and around 3.5 million shares, through the dissemination of false information, while leveraging the platform's "For You" algorithmic amplification mechanism. The networks' accounts presented themselves as international news sources, parody accounts, or commentary profiles associated with political figures or national militaries, and purchased paid Premium subscriptions to obtain verification badges. The networks disseminated false information, including AI-generated content that amplified Iran's perceived achievements while undermining the image of the United States and Israel, including claims of kidnapped U.S. soldiers, downed US aircraft, and strikes on Israeli cities. While the BRICS4CLICKS network primarily relied on promoting content from several central accounts, Verified4War depended largely on a single dominant account, "Times of Iran News," which accounted for a significant share of the network's overall engagement. The networks achieved broad reach and engagement by adopting a casual tone, characteristic of the post-truth era, with activity aimed not at persuasion or deception but at entertainment, including through the use of clickbait-style questions, such as those relating to support for Iran becoming a nuclear state.
