August 2025 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 August 2025.

August 1 – New East-European Cybersecurity Alliance Proposed to Counter Russian Threats – Ukraine's National Coordination Center for Cybersecurity (NCCC) announced it is exploring the creation of a regional cyber alliance with Romania and Moldova. The alliance would aim to strengthen the resilience of its members against cyber and hybrid threats—particularly those originating from Russia—and to enable coordinated responses to cyberattacks that threaten their national security. The alliance is envisioned as a platform for sharing knowledge on cyber threats, developing and implementing AI-based security solutions, training experts for joint cyber defense operations, and enhancing the resilience of critical infrastructure. The initiative was advanced by the Chernivtsi Regional Military Administration, which proposed hosting the alliance's central hub to provide the organizational infrastructure. The formation of the alliance would represent the implementation of agreements reached by the leaders of the three countries during the IV Ukraine–Southeast Europe Summit, held on June 11, 2025 in Odesa, which focused on strengthening Ukraine's ties with Eastern and South-Eastern European states. Ukraine's National Security and Defense Council (NSDC) emphasized that the alliance will remain open to the future participation of additional countries that share the democratic values and strategic objectives of its members.

August 2 – New Provisions of the EU AI Act Took Effect – Additional provisions of the European Union's AI Act entered into force, marking another step toward full implementation by August 2026. The first provision to take effect is Chapter V, which sets out obligations related to the development and marketing of general-purpose AI models. Under this chapter, providers of such models are required to maintain up-to-date technical documentation and make it available to the European Commission's AI Office or to designated national authorities responsible for enforcement. However, this obligation does not apply to providers of open-source AI models, provided they publicly disclose key information—such as the model's architecture. In addition, all providers are required to report on the data used to train their models, in line with a template that will be issued by the EU AI Office. The second provision now in force is Chapter VII, which defines the national authorities and the EU-level body tasked with enforcement. At the EU level, the European Artificial Intelligence Board has now begun operating in full and will advise both the European Commission and member states on the law's implementation. Furthermore, each EU member state was required by this date to appoint two types of national authorities: notifying authorities, empowered to conduct pre-market conformity assessments of models, and market surveillance authorities, responsible for enforcement and oversight of models once placed on the market.

August 5 – New Report Reveals Iranian Cyber Warfare Tactics During Israel-Iran War – The U.S. cybersecurity firm SecurityScorecard released a report on cyber warfare tactics employed by Iranian state-linked groups, as well as pro-Iranian hacktivists and proxies, primarily targeting Israel during the Israel-Iran war. According to the report's authors, all of these actors engaged in cyber warfare throughout the conflict that unfolded across three distinct tiers of activity, differentiated by both the attack methods employed and the perpetrators themselves. At the basic tier, pro-Iranian hacktivist groups carried out website defacements and claimed to have leaked a variety of stolen data repositories. At the intermediate tier, the Cyber Fattah Team—linked to Iran's Islamic Revolutionary Guard Corps (IRGC)—targeted small- to mid-sized Israeli news outlets using SQL injection and other techniques. At the advanced tier, Imperial Kitten, an IRGC-linked group, ran a phishing campaign targeting pro-Israeli users through pro-Israel–themed domains, ultimately infecting them with the RemCos remote access trojan (RAT). The report highlights Telegram's central role, serving as a hub for recruitment, attacker coordination, and propaganda, favored for its wide reach and anonymity.

August 12 – U.S. Air Force Seeks AI Solutions for High-Intensity Conflict Training – The U.S. Air Force issued a Request for Information (RFI) seeking input from the private sector on AI–based solutions for the design and execution of wargames aimed at assessing personnel readiness in high-intensity conflict scenarios. The Air Force intends to develop a Software-as-a-Service (SaaS) platform enhanced with machine learning algorithms to generate realistic combat scenarios, track participants' decision-making, and produce after-action insights. This platform will be used to design scenarios that test two critical capabilities: 1) rapid expansion of training and accession pipelines in wartime; and 2) sustaining readiness in prolonged, high-attrition conflicts. Key platform requirements include the ability to generate complex scenarios that adapt dynamically to participant decisions; integration of two-factor authentication (2FA) using time-based one-time passwords (TOTP); and incorporation of open-source content, such as news reports, into gameplay. In addition, the platform must comply with U.S. Department of Defense cybersecurity standards, operate within a secure cloud environment, and allow the government to replay scenarios without vendor support.

Make sure you don't miss the latest on cyber research

Join our mailing list