



August 2026 Cyber News

On behalf of the Yuval Ne'eman Workshop for Science, Technology, and Security, we are pleased to share with you some of the most notable events and developments that occurred in August 2026.

August 3 – INTERPOL Identified AI as a Key Driver of Cybercrime Across

Africa – According to the INTERPOL African Cyberthreat

Assessment [Report](#) 2026, in 2025 ransomware shifted from financial extortion toward disrupting critical infrastructure. The financial sector was the most heavily targeted, accounting for approximately 40% of such attacks. INTERPOL also found that in 2025, artificial intelligence was used in 55% of all cybercrimes committed that year, including to create synthetic identities capable of bypassing Know Your Customer (KYC) mechanisms. Additionally, INTERPOL presented recommendations for strengthening responses to cybercrime. At the national level, it recommended establishing formal information-sharing channels with telecommunications companies, financial institutions, and fintech companies through memoranda of understanding.

At the regional level, it recommended a continent-wide portal linking national CERTs, financial institutions, and telecommunications providers for real-time cybercrime reporting, threat correlation, and automated alerts.

August 6 – CSIS: Iran Adapted Its Cyber Strategy to Support Wartime

Objectives – The Center for Strategic and International Studies (CSIS) published [an article](#), examining the evolution of Iran's use of cyber capabilities in its conflict with the United States and Israel since February 2026. The author identified three key strategic trends in Iran's cyber activity. First, Iran realigned its cyber apparatus to support wartime objectives, shifting from simple attacks and low-impact hacktivist operations to coordinated cyber espionage, including to help target kinetic attacks against U.S. forces in the Middle East.

Second, Iran used offensive cyber capabilities to shape the operational environment in its favor, particularly through information warfare, which enabled it to project power beyond its borders and gain strategic depth. Third, Iran employed its cyber capabilities to a relatively limited extent, following patterns from its 12-day conflict with Israel in June 2025 in both its targets and methods, including cyber espionage, camera hacking, and influence operations. The author concluded that while cyber capabilities played a vital role in supporting Iran's kinetic and economic activities, they provided more limited leverage than its use of drones, missiles, and economic tools.

August 10 – Challenges Remained to Broader AI Adoption Across the U.S.

Military – According to a [paper](#) by U.S.-based Carnegie Endowment for International Peace, several key barriers hinder broader AI adoption across the U.S. military. At the bureaucratic level, the Department of Defense appointed Portfolio Acquisition Executives ([PAEs](#)) to streamline military acquisition, while [dismantling](#) the Joint Capabilities Integration and Development System ([JCIDS](#)), which helped define military requirements. According to the author, this could create uncertainty over acquisition needs and the private sector's ability to meet them. The author also noted that human air traffic controllers could struggle to manage growing numbers of autonomous and crewed weapon systems. To enable broader adoption of AI-enabled systems, the Department should prioritize funding for the technological and physical infrastructure needed to manage and operate large numbers of autonomous systems simultaneously, including without access to cloud infrastructure or remote computing resources. In addition, the department should establish baseline standards for the technological maturity and

interoperability of autonomous weapon systems, with testing requirements tailored to their complexity.

August 12 – Chinese Cyberattacks Became a Key Tool in Beijing's Strategy

Toward Taiwan – According to the U.S.-based [Global Taiwan Institute](#) (GTI), Chinese cyberattacks have become a key tool in Beijing's efforts to advance unification with Taiwan. The growing use of cyberattacks reflects China's concerns over Taiwan's strengthening national identity, democratic status, and increasingly important semiconductor industry, while also serving to test Taiwan's resilience to a potential Chinese blockade ahead of a possible invasion. Furthermore, cyberattacks aim to undermine public trust in Taiwan's government by targeting public services and infrastructure, and to isolate Taiwan internationally through cyberattacks during diplomatic events in Taiwan and partner countries. Finally, as China's economic leverage over Taiwan weakened, it increasingly used cyberattacks to pressure Taiwanese companies, particularly in the semiconductor industry, and steal sensitive technological and business information. To address these cyber threats, Taiwan should increase cybersecurity funding, expand workforce training, and strengthen international cooperation with private-sector companies and other countries.

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

[Join our mailing list](#)

