



July 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 July 2026.

July 3 – Thailand Launched International Intelligence-Sharing Platform to Combat

Cyber Fraud – The Royal Thai Police **launched** SHIELD, a centralized web-based platform for international intelligence sharing. The platform aims to support the dismantling of transnational cyber fraud and human trafficking networks. Operational since July 2, 2026, SHIELD was jointly developed by the Thai Police and Thailand's Ministry of Foreign Affairs. Several countries, including the United States, China, and India, as well as international organizations such as the United Nations Office on Drugs and Crime (UNODC), participate in the initiative. SHIELD enables participating countries to securely exchange real-time intelligence on criminal networks, victim identification, and financial transactions. **In addition**, the platform promotes common standards for information sharing in four areas: cybercrime investigations; tracking IP addresses and internet service providers; analyzing IP address activity patterns and usage frequency; and visualizing the density of connections between IP addresses through color-coded visualization.

July 7 – The European Commission Published an Action Plan on Cybersecurity and Artificial Intelligence – The [plan](#) aims to help EU member states and organizations harness the opportunities offered by AI while addressing the new cybersecurity risks it introduces. Building on the EU's existing regulatory and policy framework, the plan is structured around three pillars: (1) promoting secure, accessible, and usable frontier AI for European cybersecurity; (2) preparing the EU cybersecurity ecosystem for the AI era, including by supporting the use of AI-based tools by critical sectors and SMEs to remediate the most significant security vulnerabilities; (3) expanding European AI capabilities for cybersecurity through investment in advanced AI technologies and the development of the skills needed to deploy them across sectors. As part of the plan's implementation, the Commission announced several key actions, including the development of a European framework for providing controlled access to advanced AI capabilities for cybersecurity purposes. The framework, scheduled for completion by the fourth quarter of 2026, will establish criteria and mechanisms for providing secure and timely access to such capabilities for European entities while ensuring that access does not create irreversible security risks.

July 15 – Australia Announced Establishment of Office of AI – Australian Prime Minister Anthony Albanese [unveiled](#) the Office of AI within the Department of the Prime Minister and Cabinet. The new office aims to develop a national standards framework that will establish new mandatory requirements for the operation of large-scale data centers and AI training in Australia. The framework, expected to be published in early 2027, will require operators of large data centers to finance the new electricity generation capacity needed to support their operations, cover the costs of connecting their facilities to the electricity grid, and reduce electricity consumption when necessary to help maintain grid stability.

July 21 – US Senator Proposed Legislative Framework for Responsible AI Leadership – US Senator Mark Warner, Vice Chair of the Senate Select Committee on Intelligence, [released](#) a legislative framework aimed at strengthening the United States' global leadership in AI while promoting its responsible development. The framework includes several legislative proposals, including the Secure AI Development Act. Under the proposal, the Secretary of Commerce would, within 90 days of the bill's enactment,

establish an AI Risk Management Board at the National Institute of Standards and Technology to develop a technical process for evaluating AI model capabilities. The process would help determine which capabilities, or combinations of capabilities, indicate that a model has reached a level of performance that could pose risks to national security, economic security, or public safety. The framework also includes the SAFE AI Act, which seeks to reduce the creation of harmful sexually explicit deepfake content targeting both minors and adults. Within 90 days of the law's entry into force, the Director of NIST would be required to develop evaluation benchmarks, to assess the ability of AI models to generate such content.

July 24 – China Reviewed Cybersecurity and AI Measures Implemented Under the 14th Five-Year Plan

– China's Cyberspace Administration (CAC) [published](#) a report reviewing the cybersecurity and AI measures implemented during 2025 to advance informatization under the country's 14th Five-Year Plan. According to the report, China enacted more than 180 cybersecurity-related legislative instruments by the end of 2025. Among these, the Standing Committee of the National People's Congress approved amendments to the Cybersecurity Law in October 2025, formally establishing the development of China into a global cyber power as an official government objective. In November 2025, regulations issued by CAC entered into force, requiring cybersecurity incidents affecting critical information infrastructure to be reported within one hour of their discovery. In the field of AI, China published 29 national standards during 2025. Among them, CAC and other government authorities issued regulations in March 2025 establishing legal obligations for online information service providers to apply both visible and invisible labeling to AI-generated content.

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

[**Join our mailing list**](#)

