
# October 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 October 2025.*

**October 9 – Ukraine Advanced Legislation to Establish Cyber Forces Command** – The Verkhovna Rada of Ukraine has approved on first reading a bill to establish a Cyber Forces Command within the country's armed forces. The new command will operate under Commander-in-Chief Oleksandr Syrskyi and the supreme authority of President Volodymyr Zelenskyy. According to the proposal, the new command will recruit personnel from existing army units, lead intelligence-gathering efforts, conduct offensive cyber operations, and defend military information infrastructure, while also developing a secure communications network for the Ukrainian Armed Forces. The legislation also envisions the creation of a Cyber Reserve - a pool of civilian technology experts who can be mobilized to support cyber defense efforts without formally enlisting in the military. This marks the first time Ukraine is establishing a dedicated military command for managing cyber operations, including potential cyberattacks against adversarial military infrastructure. Until now, such activities have been carried out primarily by the Security Service of Ukraine (SBU), the Main Directorate of Intelligence (HUR), and various hacktivist groups.

**October 15 – Thailand Established a National Committee to Combat Technology-Related Crime** – Thailand's Prime Minister, Anutin Charnvirakul, has signed an executive order establishing a 23-member government committee to coordinate national efforts against technology-related crime, with a focus on online fraud and money laundering involving digital assets. The Prime Minister will chair the committee, which brings together

representatives from key government ministries and regulatory agencies, including the Ministries of Finance, Foreign Affairs, and Digital Economy and Society (DES), as well as the Royal Thai Police and the Bank of Thailand. Under its mandate, the committee will develop policy principles and guidelines for preventing technology-driven crime, oversee the work of law enforcement agencies, and enhance operational effectiveness. It will report its findings and progress to the national cabinet on a regular basis.

**October 22 – India Proposed Draft Guidelines to Address Deepfake Misinformation** – India's Ministry of Electronics and Information Technology (MeitY) has released a draft proposal for new regulations governing the publication of AI-generated content, aiming to address the growing spread of deepfake-based misinformation. Under the proposal, social media platforms—as well as major technology companies such as Google and OpenAI—would be required to visibly label AI-generated visual content with a clear disclaimer covering at least 10% of the display area. For AI-generated audio content, a corresponding audio disclaimer would need to play during the first 10% of the recording's duration. The proposed rules also mandate that social media platforms collect user declarations when AI-based content is uploaded and implement technical measures to detect and verify AI-generated material either prior to or during its publication.

**October 25 – UN Opened the First Global Cybercrime Convention for Signature** – The United Nations Convention against Cybercrime, the first global treaty aimed at preventing and responding to cybercrime, opened for signature in Hanoi, Viet Nam. A total of 72 states signed the Convention, which will enter into force 90 days after the 40th ratification, acceptance, or accession. Adopted by the UN General Assembly in December 2024, the Convention establishes a comprehensive international framework to combat the misuse of information and communication technologies in crimes such as terrorism, financial fraud, and online exploitation. It seeks to enhance global cooperation, technical assistance, and capacity building, particularly for developing countries. The treaty criminalizes a broad spectrum of cyber-dependent and cyber-enabled offences, including online fraud, child sexual exploitation, and online grooming. Once in force, the Convention will guide cooperation among member states through a Conference of the States Parties, tasked with monitoring implementation, fostering collaboration, and advancing collective cyber resilience.

---