January 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 January 2026.

January 7 – US President Directed Withdrawal from International Organizations and Treaties – U.S. President Donald Trump issued a memorandum instructing the federal government to pursue withdrawal from 66 international organizations and conventions. The move aims to reassess U.S. participation in international bodies deemed not to advance national interests. As part of the memorandum, the administration was directed to advance the U.S.' withdrawal from the European Centre of Excellence for Countering Hybrid Threats, the Freedom Online Coalition, and the Global Forum on Cyber Expertise.

January 12 – Morocco Launched the "AI Made in Morocco" National Initiative – The Minister of Digital Transition and Administrative Reform, Amal El Fallah Seghrouchni, announced the launch of the national "AI Made in Morocco" initiative, to advance Morocco's AI ecosystem. Serving as a national roadmap, the initiative aims to create around 50,000 new jobs in the field of AI, and train 200,000 graduates in relevant skills. The initiative is built around three core pillars: (1) strengthening digital sovereignty and building trust in the use of AI, with a focus on governance, regulation, and infrastructure; (2) promoting local innovation and competitiveness, with an emphasis on industrial development, human capital, and research; (3) deepening the adoption and impact of AI systems to enhance Morocco's international positioning in the field. In addition, the initiative includes the establishment of a national data factory to regulate and manage public sector data, alongside a

national software factory to consolidate government-developed AI components and algorithms, as well as the development of sovereign cloud infrastructure. The initiative was launched as part of Morocco's national AI strategy, which the country planned to publish in January 2026.

January 12 – U.S. Department of War Released New Strategy to Expand Military Use of AI – The U.S. Department of War published a new AI strategy, with the aim of expanding the use of AI across all branches of the US Armed Forces and reinforcing its position as a global leader in the field. The strategy advances initiatives across three main domains. In the warfighting domain, elite combat units and technology companies will jointly develop, test, and refine new principles for integrating AI systems on the battlefield, alongside the formulation of principles for countering adversaries' AI-enabled systems. In the intelligence domain, the strategy seeks not only to enhance capabilities for the collection and use of military intelligence but also to promote its optimal use to support dynamic deterrence against adversaries, evolving based on real-time developments. Finally, the strategy promotes access to advanced AI models developed in the private sector, to streamline work processes across the Department and the military. In parallel, the strategy sets out implementation guidance: each initiative will be led by a designated program manager, who will report monthly on progress to the Deputy Secretary of War and the Under Secretary of War for Research and Engineering. At the same time, the Department of War's Chief Digital and AI Office will be required to establish clear metrics on the speed of deployment of AI systems within the military and to report on these metrics monthly to the Under Secretary of War for Research and Engineering.

January 20 – European Commission Published Updates to Two EU Cybersecurity Regulations – First, the Commission published an updated version of the Cybersecurity Act, introducing changes to the European Cybersecurity Certification Framework. The proposed amendments expand the scope of the framework beyond information and communications technology products and services, introducing a new certification scheme that would allow organizations to assess their cybersecurity posture and demonstrate compliance with requirements set out in the NIS2 Directive and other relevant regulations. In addition, the proposal instructs the European Union Agency for Cybersecurity (ENISA) to establish a dedicated helpdesk to support operators of critical infrastructure in responding to ransomware attacks. Second, the Commission proposed amendments to the NIS2 Directive, extending its scope to include organizations operating subsea data transmission infrastructure for telecommunications companies. The proposed changes would enter into force immediately upon approval by the European Parliament and the Council of the European Union. EU member states would then be given one year to implement the updated directive.

January 23 – Angola's Parliament Approved National Cybersecurity Bill in First Reading –Angola's parliament, the National Assembly, approved the National Cybersecurity Bill in its first reading to address existing regulatory gaps in cybersecurity, notably the absence of

enforcement mechanisms to sanction non-compliant entities. The bill provides for the establishment of three bodies: (1) a National Cyber System; (2) a National Cybersecurity Council, which would serve as an advisory body to the President of Angola and coordinate among public and private sector entities responsible for protecting the national cyberspace; (3) a National Cybersecurity Center, which would be granted supervisory authorities and empowered to impose sanctions.

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

Join our mailing list