



Cyber News December 2024

On behalf of the Yuval Ne'eman Workshop for Science, Technology and Security, we are happy to share some of the most interesting events and developments that took place in December 2024

December 11 – Hong Kong Legislative Council Approved First Reading of Critical Systems Protection Bill – The Hong Kong Legislative Council **has passed** the Protection of Critical Infrastructures (Computer Systems) **Bill** in its first reading. This proposed legislation is designed to protect computer systems within eight categories of critical infrastructure, such as energy supply and transportation networks. The bill outlines the creation of a Commissioner of Critical Infrastructure (Computer-system Security) protection, to be appointed by the Chief Executive of Hong Kong. The commissioner will oversee efforts to detect and address security threats targeting these systems. Additionally, all entities managing critical infrastructure will be required to develop a comprehensive plan to enhance the protection of their computer systems. These plans must include guiding principles for identifying, assessing, and mitigating potential security threats. Organizations that fail to present such plans may face fines of HK\$300,000 (US\$38,500) or HK\$500,000 (US\$64,300), depending on the extent of non-compliance. In cases where the commissioner identifies a significant security incident affecting a critical infrastructure's computer system, their office will be authorized to initiate an investigation to determine its causes, assess its impacts, and recommend measures to mitigate future risks. The Legislative Council is **expected to proceed** with the second and third readings of the bill in 2025.

December 11 – BRICS Nations Launched AI Alliance Network to Drive Collaborative AI Innovation – Russian President Vladimir Putin **announced** the establishment of the AI Alliance Network, a collaborative **initiative** within BRICS nations, which include Brazil, Russia, India, China, South Africa and others, aimed at advancing research, regulation, and the adoption of artificial intelligence products across member states. The alliance held **its inaugural meeting** on December 13 in Moscow as part of the annual international conference, AI Journey, which took place from December 11–13. The meeting, led by Russian Deputy Prime Minister Dmitry Chernyshenko, brought together AI system developers from Brazil, India, Indonesia, Azerbaijan, and other nations to discuss core aspects of AI development and explore potential collaborative opportunities. During the meeting, Chernyshenko called on alliance members to participate in the 2025 conference, which will focus on selecting and prioritizing AI research initiatives for accelerated development.

December 12 – U.S. Department of Defense Launches AI Readiness Cell to Accelerate Responsible AI Adoption – The Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO) has **announced** the establishment of the Artificial Intelligence Rapid Capabilities Cell (AI RCC) to accelerate the responsible adoption of artificial intelligence for combat and administrative purposes. This initiative coincides with the conclusion of **Task Force Lima**, which was launched in August 2023 to guide the department's implementation of responsible AI practices. The AI RCC will focus on executing recommendations issued by Task Force Lima across 15 operational and administrative domains, including command and control, personnel management and procurement processes.

December 17 – UC Berkeley Kicked off Collaborative Initiative to Combat AI-Driven Cybercrime – The Center for Long-Term Cybersecurity (CLTC) and the Berkeley Risk and Security Lab (BRSL) at the University of California, Berkeley, have **launched** a joint initiative titled "AI-Enabled Cybercrime: Exploring Risks, Building Awareness, and Guiding Policy Responses," to tackle the growing threat of AI-driven cybercrime. The initiative aims to explore the impact of artificial intelligence on cybercrime, focusing on the rise in scale and sophistication of phishing scams, identity theft, and the emergence of new types of cyberattacks. It will also provide policymakers and the private sector with future-oriented tools and strategies to tackle these evolving threats. The initiative is led by Dr. Gil Baram, a senior researcher and lecturer at Bar-Ilan University and UC Berkeley, who previously served as the Head of the Cyber & Space Research Program at the Yuval Ne'eman Workshop for Science, Technology, and Security at Tel Aviv University. The launch event included a simulation exercise conducted in collaboration with Fortinet at UC Berkeley. In 2025, the initiative will hold interviews and workshops in Singapore and Israel, featuring technology experts from Silicon Valley. Additionally, a report summarizing the initiative's activities and offering recommendations will be published in the summer of 2025.

Make sure you don't miss the latest on cyber research
[Join our mailing list](#)

