June 2025 Cyber News

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 June 2025.

June 2 – UK Established Cyber Command as Part of Long-Term Defence Roadmap – UK Prime Minister Keir Starmer has presented the Strategic Defence Review (SDR), outlining initiatives to strengthen national security by 2035 through technological innovation and collaboration across government, academia, and industry. A key initiative is the creation of a new Cyber and Electromagnetic Command (CyberEM Command) under the Ministry of Defence's Strategic Command (StratCom). The command will define requirements for offensive cyber operations—executed by the National Cyber Force (NCF)—and lead defence policy for protecting military networks. It will also serve as the UK military's main liaison with foreign governments and NATO on cyber and electromagnetic warfare. The strategy further calls for integrating artificial intelligence and other advanced technologies into military operations. By July 2026, a Digital Warfare Group is to be established, employing AI, drones, and additional advanced tools for real-time battlefield data analysis, threat detection, and improved combat coordination.

June 6 – Trump Signed Executive Order Rolling Back Biden-Era Cybersecurity Mandates – President Donald Trump signed an executive order altering key cybersecurity policies set by former Presidents Obama and Biden. The order revokes a January 2025 mandate requiring federal software vendors to certify compliance with Secure-by-Design principles developed by the National Institute of Standards and Technology (NIST). Instead, NIST is now directed to work with the private sector to develop voluntary guidelines for secure software development. In the area of AI, Trump's order requires federal agencies to incorporate AI vulnerability management into existing systems, including internal databases and inter-agency information sharing. The order also narrows the scope of cyber-related sanctions introduced in 2015, restricting them to foreign actors and explicitly excluding election-related cyberattacks. The move reflects the administration's broader approach to strengthening federal cybersecurity by limiting government oversight and favoring market-based solutions over regulation.

June 11 – Morocco Introduced National Cybersecurity Strategy 2030 – The Moroccan government launched its National Cybersecurity Strategy 2030, aimed at strengthening national information system security. The strategy focuses on proactive risk management, systematic cybersecurity audits, and embedding security standards early in digital project design. Public sector cybersecurity awareness will be enhanced through training programs led by the General Directorate for Information Systems Security (DGSSI). The government also plans to bolster critical infrastructure protection by mapping interdependencies and encouraging the establishment of organizational SOCs. Morocco will also invest in cybersecurity R&D at academic institutions, including the Cybersecurity Innovation Center launched in June 2025 at Mohammed V University. In parallel, the government will strengthen inter-agency coordination by establishing communication channels between key national stakeholders for sharing threat intelligence and responding to cyber incidents.

June 17 – Recorded Future Report Reveals PLA Use of Generative AI in Intelligence Operations – Cybersecurity firm Recorded Future published a report analyzing the use of generative AI by the People's Liberation Army (PLA) and Chinese defense contractors in the context of intelligence operations. According to the authors, the PLA is leveraging commercial large language models (LLMs)—developed by both Chinese and foreign companies—including Meta's Llama 13B and DeepSeek's V3 model, to perform a range of intelligence-related tasks. These include information collection, content analysis, report summarization, alert generation, and decision support. One of the key entities identified in the report is the Chinese tech company TRS, which in June 2023 released the TuoTian model. TuoTian is used for open-source intelligence (OSINT) gathering and intelligence assessment, including for institutions such as the PLA's National Defense University in Beijing. The report further suggests that Chinese intelligence agencies may also apply generative AI for influence operations, such as producing falsified open-source content to disrupt the work of Western intelligence services. At the same time, the authors note that there is growing concern within China over the potential use of similar AI-based influence capabilities by Western agencies targeting China.

June 20 – US FCC to Review Cyber Trust Mark Program Amid National Security Concerns – Federal Communications Commission (FCC) Chairman Brendan Carr announced that he had instructed the Commission's Council for National Security to reevaluate the implementation of the U.S. Cyber Trust Mark program—a voluntary initiative launched by the Biden administration in January 2025 to help consumers identify secure IoT devices. As part of the program, UL Solutions—a U.S.-based company specializing in certification and technical assessment—was selected to oversee the testing of participating IoT products. However, an internal FCC document has raised concerns over the company's continued role due to its operation of 18 laboratories in China. The document warns that this arrangement could enable Chinese manufacturers to obtain U.S. cybersecurity labels despite potential vulnerabilities, which may be exploited by China for cyber espionage targeting the United States.
