Cyber News October 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 October 2024

October 1 – Singapore Introduced the Smart Nation 2.0 Strategy – Singapore's Prime Minister, Lawrence Wong, announced the launch of the Smart Nation 2.0 Strategy, led by the Ministry of Digital Development and Information (MDDI). The new strategy addresses threats like deepfakes, online scams, and data center disruptions. A key part of the initiative includes establishing a dedicated agency focused on combating online bullying and sexual harassment and improving reporting and support services for victims. Additionally, the government will mandate social media platforms to prevent the spread of harmful content and take action against offenders. The initiative also includes an allocation of 120 million Singapore dollars (approximately 90 million USD) to promote the use of AI for scientific research and train educators to utilize this technology through the Smart Nation Educator Fellowship. Finally, Wong announced that in 2025, the government will introduce the Digital Infrastructure Act to enhance the resilience and security of critical digital infrastructure and services.

October 3 – The U.S. Hosted the Annual International Counter Ransomware Conference – From September 30 to October 3, Washington hosted the fourth annual international summit of the Counter Ransomware Initiative (CRI), with 68 countries participating, including Israel. During the summit, the White House issued a joint statement on the efforts of the CRI's member states to combat ransomware attacks. In the policy pillar, France and the Netherlands led a workshop with cyber insurance companies, focusing on the industry's ability to support organizations affected by ransomware attacks. The U.S. also announced the launch of the CRI Fund, designed to strengthen member states' cybersecurity capabilities by providing rapid technical support during incidents, training skilled personnel, and the development of security protocols. Additionally, member states participated in a groundbreaking meeting exploring the use of AI in preventing cyberattacks, focusing on enhancing the security of healthcare institutions and monitoring hostile cyber activities.

October 5 – The Netherlands and Ukraine have Signed a Memorandum to Advance Cyber Security Collaboration – During the international annual ONE Conference held in The Hague, the Cyber Security Coordination Center of Ukraine (NCSCC) and the National Cyber Security Center of the Netherlands (NCSC) signed a memorandum of understanding aimed at enhancing cooperation in the field of cyber security. Under this memorandum, both countries committed to bolstering their cyber defense capabilities against global cyber threats and sharing expertise and knowledge. This memorandum builds upon the bilateral security agreement signed in March 2024, which mandates the Dutch government to provide military and security assistance to Ukraine until 2034.

October 6 – Chinese Hackers Infiltrated U.S. Telecom Networks, Targeting Presidential Campaigns – The FBI, the U.S. Department of Homeland Security, and other intelligence and government agencies have launched an investigation into cyberattacks reportedly conducted by Chinese agents against three major U.S. telecommunications companies: AT&T, Verizon, and Lumen Technologies. U.S. officials suggest the attacks may be linked to a group known as Salt Typhoon, allegedly affiliated with China's Ministry of State Security (MSS) and reportedly have remained undetected for several months. According to U.S. officials, the attacks were likely intended to gather information on potential American surveillance conducted on Chinese targets. On October 25, it was revealed that hackers targeting Verizon attempted to breach phones or systems used by former President Donald Trump, Sen. JD Vance, and members of Vice President Kamala Harris' presidential campaign. These incidents are part of a broader cyber-espionage effort aimed at political figures from both parties.

Make sure you don't miss the latest on cyber research
Join our mailing list