Cyber News February 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 February 2024

February 1 - South Korea Unveiled New Cybersecurity Strategy to Actively Counter North Korea's Cyber Operations - The new strategy, published by the National Security Office of the Republic of Korea (ROK), aims to promote a proactive approach to countering North Korea's malicious cyber activities, marking a shift from the 2019 cybersecurity strategy that focused on passive defensive measures. Under the new strategy, South Korea seeks to develop offensive cyber capabilities and utilize emerging technologies, such as AI, to identify the sources of cyberattacks by monitoring malevolent activities on the dark web. The strategy also emphasizes international cooperation, particularly with NATO and Asia-Pacific countries, as crucial for countering malicious cyber activities. Additionally, the strategy addresses influence operations posed by North Korea and other countries and calls for the formulation of technical and diplomatic response measures, as well as the strengthening of the cooperation between government ministries and the private sector.

February 6 – Governments and Industry Partners Initiated the Pall Mall Process for Countering the Proliferation of Offensive Cyber Capabilities – Officials from 35 countries, including the United States, Italy, and Australia, launched the Pall Mall Process alongside representatives from the private sector and civil society, including Meta and Microsoft. The process aims to regulate the production, use, and distribution of advanced offensive cyber capabilities. According to the declaration signed by the participants, the use of these capabilities should be subject to four principles: (1) Responsible use in accordance with the norms of responsible state behavior in cyberspace and international law; (2) Minimizing the likelihood of unintended and unwanted consequences; (3) Assessment of use and compliance with the principles of legality and necessity by state and private actors; (4) Transparency regarding the activities of production and marketing of advanced cyber capabilities. In addition, the members decided to hold a follow-up conference in 2025 to review the progress made in implementing the principles.

February 7 – Five Eyes States Published a Joint Advisory on Chinese State Hacking Group Targeting U.S. Critical Infrastructure – Intelligence, cyber, and law enforcement agencies from the Five Eyes countries (The US, Australia, Canada, New Zealand, and the UK), including the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Centre (NCSC) of the United Kingdom, issued a joint advisory about risks to U.S. critical infrastructure posed by the Chinese government-affiliated hacking group Volt Typhoon. According to the document, the group has breached organizational IT networks of critical infrastructure in multiple sectors in the U.S., including communications, energy, and water, after gathering preliminary information on key IT staff and exploiting zero-day vulnerabilities in public-facing network appliances. Concurrently, the hackers used stolen administrator credentials and implemented LOTL techniques to move laterally within the networks and attempt to disrupt the operation of OT systems. The agencies recommended critical infrastructure entities monitor logs in communication channels between IT and OT networks to detect anomalous behavior and avoid storing credentials on edge appliances and devices. Additionally, in an accompanying guidance document, the agencies suggested methods for hunting LOTL activity, such as using automation to detect anomalous activity in domain controllers and other critical assets.

February 7 – Two American Senators Introduced a Bill to Improve Cybersecurity of Drones Used by the Federal Administration – Senators Mark Warner and John Thune introduced the bipartisan bill, Drone Evaluation to Eliminate Cyber Threats Act of 2024 (DETECT Act). The bill aims to direct the National Institute of Standards and Technology (NIST) to develop cybersecurity principles for using drones by Federal agencies. First, the Office of Management and Budget (OMB) will introduce a pilot program for evaluating the implementation of the principles in one selected agency. Afterward, The OMB will direct all Federal agencies to implement the NIST principles and draft guidelines for reporting drone security vulnerabilities. In addition, the OMB will prohibit agencies from acquiring drones that do not meet NIST's principles.

February 21 – The Biden Administration issued an Executive Order for Bolstering the Cybersecurity of U.S. Ports – Under the order, the Coast Guard will be able to direct owners and operators of vessels and ports to improve their cybersecurity measures and will be able to control the entry of vessels into the United States that pose an actual or potential threat to national cybersecurity. Additionally, by April 2024, the Coast Guard will publish a proposal for public comment to develop minimum security standards for vessels and ports, including mandatory requirements for reporting security incidents to the FBI and other federal agencies. Following the publication of the order, the Coast Guard directed American entities operating Chinese-made maritime cranes to contact the Coast Guard to receive new guidance on managing security risks associated with using the cranes. According to the Coast Guard, these cranes, which make up 80% of all maritime cranes in the U.S., can be remotely controlled and reprogrammed by malicious actors, potentially endangering the ports where they are located.