Cyber News June 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 June 2024

June 3 – Poland Announced Allocating $760 Million to Boost Cybersecurity After Alleged Russian Attack – The Polish Minister of Digitization, and Deputy Prime Minister Krzysztof Gawkowski, has unveiled plans to allocate 3 billion zloty (approximately $760 million) towards bolstering cybersecurity measures and fostering closer collaboration between the public and private sectors. This initiative directly responded to a cyberattack in late May 2024 targeting the Polish news agency PAP, which governmental authorities attributed to Russia. The attack was allegedly intended to sway the outcomes of the early June 2024 European Parliament elections. The incident involved the dissemination of fabricated news on the PAP website, falsely claiming that Poland had mobilized 200,000 troops for an invasion of Ukraine.

June 4 – Report: TikTok Failed to Remove False Information Regarding the 2024 European Parliament Elections in Ireland – An examination conducted by the non-profit organization Global Witness in May 2024 uncovered that TikTok had failed to prevent the dissemination of false political content aimed at influencing public opinion in Ireland ahead of the European Parliament elections. The investigation scrutinized the adherence of various social media platforms, including X and YouTube, to EU regulations such as the Digital Services Act (DSA), which mandates actions to combat the spread of disinformation. Global Witness examined this by submitting sixteen pieces of false content for publication, including claims about the closure of polling stations due to outbreaks of infectious diseases. The findings revealed that the platforms reviewed the content before publication. While X blocked all submissions and suspended the associated account, TikTok published all pieces of false content, and YouTube published two out of the sixteen submissions.

June 4 – South Korea Forms Advisory Panel for Promoting Cybersecurity of Satellites – The National Intelligence Service (NIS) of South Korea has introduced an advisory panel to bolster cybersecurity measures for satellite systems. This initiative, led by the NIS, will include representatives from diverse government agencies. The advisory panel's mission is to safeguard satellites from cyber threats at every stage of their lifecycle, from initial design to operational deployment. This effort is pivotal in fortifying the security of space assets domestically and globally.

June 7 – German Scholars Found Chatbots Provide Unreliable Information About EU Elections – The German NGO DRI has released a study investigating the accuracy of information provided by four chatbots, such as ChatGPT4 and Copilot, regarding the June 2024 European Parliament elections. This study builds on a prior DRI report from April 2024 that revealed these chatbots frequently gave inaccurate election information. In their latest research, the researchers posed five voting procedure questions in ten languages, including French and English. They discovered that Google had restricted its chatbot Gemini from addressing any election-related queries, a move researchers saw as a step to curb misinformation. Conversely, ChatGPT4 and ChatGPT4o chatbots managed to respond to most election questions, but often with unreliable information and broken links. The study's authors recommended that OpenAI consider training its models to avoid addressing election-related inquiries, among other suggestions.

June 7 - Japan Promotes Active Cyber Defense Policy for Protecting Critical Infrastructures – The Japanese Minister for Digital Transformation, Taro Kono, has convened a team of seventeen experts, including cybersecurity specialists and legal professionals, to compile a report on advancing the government's adoption of active cyber defense strategies to safeguard critical infrastructure. This report will form the basis for drafting a legislative proposal to enhance national capabilities in active defense, scheduled for presentation to the Japanese parliament as early as autumn 2024. The experts are tasked with advising the government on promoting information sharing between the public and private sectors, monitoring cyber threats, and providing necessary governmental authorities to implement active defense measures. Additionally, on June 9th, it was announced that the government plans to establish an independent organization to monitor data traffic across communication networks to detect potential cyber threats against critical infrastructure. Should this information indicate an imminent attack, the government will seek to disrupt it by penetrating the infrastructure used by hackers to execute such attacks.

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