Cyber News September 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 September 2024

September 2 – Scottish Government Published New Strategy for Bolstering Public Sector Cybersecurity – The Scottish government unveiled a strategic plan for 2024-2027 aimed at operating the SC3 Center, a dedicated facility for coordinating cyber security operations. This initiative seeks to enhance the cyber security posture of Scotland's public sector by assessing and evaluating various facets of cyber resilience among public institutions. SC3 will also provide critical insights into current and emerging cyber threats, ensuring that public sector entities are well-prepared to respond effectively, including thoroughly reviewing their response strategies. Additionally, it will develop and implement principles and recommendations for cyber and information security across the public sector. To achieve these objectives, SC3 will spearhead initiatives such as research into mitigating security vulnerabilities within supply chains for public bodies. Operating under the Scottish Government's Cyber Resilience Unit (CRU), the center will collaborate closely with other public entities, including Police Scotland and NHS National Services Scotland.

September 4 – New Document Reveals New Russian Tactics to Influence U.S. Elections and Manipulate Israeli Public Opinion – The U.S. Department of Justice (DOJ) has released a document detailing Russian influence operations that are aimed at promoting pro-Russian narratives among target audiences in the United States and other countries, including Germany and Mexico, as part of its campaign in the Ukraine. This initiative involved multiple influence strategies intended to sway American public opinion while meddling in the Presidential elections. One notable scheme involved creating a network of 200 accounts on social media platforms, with four accounts in each U.S. State, designed to impersonate Republican Party activists and advocate for a pro-Russian foreign policy. Additionally, Russia launched the "Good Old USA" project, aimed at persuading American voters that the U.S. is providing excessive support to Ukraine and that the conflict should be resolved through territorial concessions between Russia and Ukraine. These narratives were strategically targeted at voters in swing states, such as Michigan and Pennsylvania, as well as among American Jewish and Hispanic communities.

The document also reveals new details about Russia's influence operations aimed at shaping public opinion in Israel over an unspecified timeframe. According to the report, the Russian government sought to bolster support for its military actions against Ukraine among the Israeli public by capitalizing on the internal controversies surrounding proposed changes to Israel's judicial system. Russia believed that swaying Israeli public sentiment could also impact Jewish voters in the U.S. ahead of the presidential elections. To achieve this, Russia launched an influence campaign in Russian, English, and Hebrew, disseminating content with a right-wing, anti-Ukrainian perspective across various platforms, including Telegram, X, Facebook, Instagram, and YouTube.

September 7 – United Arab Emirates Completed Cyber Security Training for Government Staff – The United Arab Emirates Cyber Security Council (UAE-CSC) announced the successful completion of a new series of training courses as part of its Cyber Sniper initiative, launched in 2023 in collaboration with the Federal Authority for Government Human Resources (FAHR) and global organizations such as the SANS Institute. This initiative provided government employees with advanced training in ethical hacking, equipping them with essential knowledge about various cyber-attack types and techniques for assessing security vulnerabilities in information systems and networks. The initiative is a key component of the UAE-CSC's efforts to implement the "We the UAE 2031" vision, introduced in November 2022, which aims to safeguard the country's digital infrastructure and enhance the preparedness and capabilities of government entities in addressing cyber threats.

September 9 – Singapore Introduced Bill to Combat Deepfakes and Misinformation in Elections – Singapore's Ministry of Digital Development and Information (MDDI) has proposed the Elections (Integrity of Online Advertising) (Amendment) Bill, aimed at curbing the spread of deepfake videos and other deceptive content intended to damage the reputation of election candidates. Under the proposed legislation, the Supervisor of Elections (the Returning Officer) would have the authority to direct social media platforms, internet service providers, and individuals who disseminate misleading information to either remove such content or restrict access to it during the election period.

Non-compliance by social media companies could result in fines of up to one million Singapore Dollars (approximately $775,000), while individual violators may face penalties of up to 1,000 Singapore Dollars (around $775) and a potential prison sentence of up to 12 months. Additionally, electoral candidates would have the right to request that the Supervisor of Elections review potentially unlawful content and issue directives for its correction.

The proposed amendments would not apply to private conversations between users, except in cases involving large WhatsApp group chats. Similarly, the law would exempt satirical or unrealistic entertainment content, such as memes or news agency reports of false information. The Infocomm Media Development Authority (IMDA) also announced plans to introduce new regulations requiring certain social media platforms to prevent the misuse of AI-generated content. IMDA will engage with social networks to finalize the details of these upcoming rules.

September 10 – USCYBERCOM Unveiled AI Integration Roadmap to Bolster Cyber Defense Capabilities – Michael Clark, the Deputy Director of Plans and Policy at U.S. Cyber Command (USCYBERCOM), has outlined a strategic plan for integrating artificial intelligence (AI) technology within the command to enhance its capabilities in analyzing and countering cyber threats. As part of this initiative, a specialized team will be established under the Cyber National Mission Force (CNMF) to oversee the roadmap's execution and address challenges related to infrastructure development, procurement, policy, and workforce integration. According to the command's statement, the roadmap's implementation will extend through 2029 and involve approximately 60 pilot programs and 26 AI-focused initiatives.

Make sure you don't miss the latest on cyber research

Join our mailing list