Cyber News November 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 November 2024

November 4 – Meta Opens Llama AI to U.S. National Security Agencies Amid Policy Shift – Meta announced that it would permit U.S. national security agencies and defense contractors to utilize its Llama language models. This marks a shift from its previous policy, which prohibited the model's use in military missions to avoid potential harm to human life. According to Meta, the latest Llama models offer enhanced capabilities, including improved reasoning, code generation, and more diverse responses, comparing models with similar parameter counts, such as Gemini Pro 1.5. Meta also revealed partnerships with prominent security and technology firms, including Lockheed Martin and IBM, to facilitate government adoption of Llama. As part of this initiative, Microsoft and AWS now host Llama in their secure cloud environments, enabling the handling of sensitive information for government agencies.

November 7 – Germany Drafts Legal Changes to Protect Security Researchers – The German Federal Ministry of Justice has released a draft amendment to the German Criminal Code for public consultation. The proposed changes aim to protect cybersecurity professionals who identify and report security vulnerabilities from criminal prosecution. The amendment seeks to revise Sections 202a, 202b, and 303a of the law, establishing clear conditions under which researchers can identify and report vulnerabilities in IT systems that might impact critical infrastructure, such as healthcare, transportation, and energy supply. The proposal also introduces stricter penalties for cases involving espionage or the disruption of data transmission, particularly when these actions pose risks to Germany's national security, the functioning of critical public infrastructure, or involve cybercriminal groups. Offenders could face prison sentences ranging from three months to five years in such instances. Cybersecurity firms, legal experts, and public sector representatives are invited to submit feedback on the draft bill by December 13, 2024, before it is presented to the Bundestag, Germany's parliament, for further deliberation.

November 8 – Cyber Attacks on South Korea Escalate Over North Korea's Role in Ukraine Conflict – The Office of the President of South Korea has issued a warning regarding a surge in cyberattacks launched by groups linked to the Russian government. This follows reports of approximately 11,000 North Korean soldiers allegedly deployed in Russia's western Kursk region to support its ongoing war efforts. The observed cyber activities included DDoS attacks by unnamed pro-Russian hacktivist groups, targeting government websites and private companies, which caused temporary service disruptions. The warning came after an emergency meeting held on November 7, 2024, led by Shin Yong-seok, South Korea's Cybersecurity Secretary, and attended by national security agencies and other governmental bodies. The meeting focused on enhancing readiness to counter Russian cyber threats. The presidential office announced that The National Cyber Crisis Management Team of the National Intelligence Service (NIS) will monitor pro-Russian hacktivist activities and share intelligence with domestic cybersecurity agencies to strengthen the nation's defense against potential attacks.

November 11 – Biden Administration Announces Support for First International Cybercrime Treaty – The Biden administration has announced its support for adopting the first international treaty on combating cybercrime, which is set to be voted on by the United Nations General Assembly in December 2024. The treaty, based on a Russian proposal despite opposition from the U.S. and European nations, focuses on preventing online child exploitation and money laundering and was approved in August 2024 by the UN Cybercrime Committee. According to a senior Biden administration official speaking on anonymity, the decision to back the treaty stems from the U.S.'s desire to influence its implementation to uphold human rights and strengthen cooperation with allies, including in cybercriminal arrests and extraditions to the United States. However, Democratic senators, civil society and human rights organizations from the U.S. and Europe have raised concerns about the treaty's vague language. They warn it could empower governments such as Russia and China to suppress freedom of expression, as well as target journalists, activists, security researchers, and citizens under the guise of combating cybercrime. The senior official stated that the administration intends to develop a plan to monitor the treaty's implementation and mitigate its risks in collaboration with the private sector and human rights organizations.

November 28 – Australia Passed a Bill to Ban Social Media for Minors Under 16 – Australia's parliament passed the legislation banning minors under the age of 16 from using social media platforms, presented by the Australian Communications Minister Michelle Rowland. The proposal directs social media companies to prevent minors' access, potentially through biometric verification or ID checks to confirm their age. The restriction will apply to minors with existing accounts, not just those attempting to create new ones, even if parental consent is provided. Social media platforms may face penalties of up to 50 million Australian Dollars (33 million USD) for noncompliance, though parents and minors will not be punished. Following the proceedings, the Australian nonprofit Digital Industry Group, which represents social media platforms in the country, including TikTok and Meta, warned that the ban is a disproportionate measure to address the risks posed by social media. The group also expressed concern that such a policy could drive young people to use unregulated platforms. The legislation will take effect within 12 months, allowing social media platforms to prepare for its implementation.

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