Cyber News January 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 January 2024

January 4 – Greece introduced a bill to establish a new national cybersecurity agency – The Greek Ministry of Digital Governance issued for public comments a draft law to found a new national cybersecurity authority, which the Ministry of Digital Governance will oversee. The new authority will be based on the current General Directorate of Cybersecurity and will include two directorates: one for staff planning and the other for operational activity. In addition, it will be responsible for coordinating and implementing the national cybersecurity strategy and will lead Greece's preparation for cyberattacks. The government of Greece will appoint a cybersecurity expert as the authority's head for five years, which may be extended.

-

January 7 – Philippines to work with black hat hackers to protect national infrastructures due to lack of cybersecurity professionals – According to the Department of Information and Communications Technology Undersecretary at the *Philippine Government*, Jeffrey Ian Dy, the state occasionally cooperates with black hat hackers, who may have formerly breached governmental systems, to counter cyber attacks launched by foreign hackers. Dy justified the decision as a means to increase the staff of the national cyber response team: it counts 35 members, while the requirement is for about 200 employees. He claimed that the shortage of funds for the recruitment and employment of professional workers is the primary obstacle to expanding the team's personnel.

January 9 – The U.S. harnessed AI technologies to detect advanced Chinese cyber operations against critical infrastructures – During the 10th International Conference on Cyber Security in New York, the National Security Agency (NSA) Director of Cybersecurity, Rob Joyce, stated that AI and machine learning technologies assist the NSA in detecting Chinese cyber attacks on U.S. critical infrastructures, including pipelines and transportation systems. Joyce estimated that traditional cybersecurity means may not have disclosed the attempts since AI-based tools are more effective in identifying abnormal activity patterns. This occurs as U.S. intelligence officials warned during 2023 that Chinese hacks against critical entities are becoming more sophisticated and elusive.

January 15 - OpenAI introduced steps to prevent malicious uses of AI technologies during elections – The ChatGPT's maker detailed, in a blog post, its actions to avoid disseminating AI-based disinformation ahead of elections in more than 50 countries during 2024. OpenAI will forbid using the image generator DALL-E 3 for political campaigns as part of its plan. The company also stated that it is developing tools to pinpoint ChatGPT-generated content and will provide users with a new means for identifying DALL-E 3-generated images. Furthermore, OpenAI announced that it blocks applications that may deter electorates from participation in democratic processes, and it will refer users to sources with reliable voting information.

January 16 – NATO unveiled its first quantum technologies strategy – NATO published the main principles of its first strategy for utilizing quantum technologies for defense following its approval by NATO Foreign Ministers in November 2023. As part of the strategy, NATO members will explore the use of quantum technologies for security purposes, such as providing precise positioning, navigation, and timing abilities, while preparing for threats arising from similar uses by NATO adversaries. To achieve these goals, NATO will protect its information systems by implementing quantum key distribution and migrating to post-quantum cryptography. NATO will also establish a transatlantic quantum community to promote cooperation among governments, companies, and academia. In addition, NATO will advance the responsible development of quantum technologies, considering data privacy, international norms development, and sustainability.

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