Cyber News March 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 March 2024

March 8 – India Approved a Comprehensive Plan for Advancing the National Artificial Intelligence Ecosystem – The Indian government has initiated the IndiaAI Mission with the aim of bolstering indigenous AI capabilities and infrastructure, allocating a substantial budget of $1.24 billion for its execution through the Digital India Corporation. Central to this endeavor is the establishment of the IndiaAI Innovation Centre, dedicated to fostering the development of large local multimodal models (LMMs) and facilitating AI training initiatives. Moreover, the IndiaAI Startup Financing plan will extend financial support to homegrown startups, propelling the commercialization of AI breakthroughs. Complementing this, the IndiaAI Datasets Platform will serve as a vital resource hub, granting access to essential databases crucial for AI application development by both private enterprises and public institutions. Additionally, the program encompasses the ambitious IndiaAI Compute Capacity initiative, aimed at constructing a high-performance supercomputer equipped with no less than 10,000 Graphics Processing Units (GPUs), thus addressing the escalating computational demands of the national AI landscape.

March 13 – The European Parliament Approved the EU AI Act – Striving for a balance between innovation and safety, the EU AI Act aims to regulate the development and deployment of AI systems. The act prohibits harmful practices like mass scraping of facial recognition data from CCTV footage. It goes further than mere permission, establishing safeguards for high-risk systems. These include mandatory human oversight and the right for citizens affected by AI decisions to receive clear explanations. The European Council is expected to greenlight the act by May 2024, with a phased rollout over the next two years.

March 14 - The American Federal Communications Commission Approved a Voluntary IoT Cybersecurity Labeling Plan – The Federal Communications Commission (FCC) is launching the U.S. Cyber Trust Mark Program to help consumers identify secure Internet of Things (IoT) devices. Devices meeting cybersecurity criteria will display a QR code, linking to details about their security features. This empowers consumers to make informed choices. Building on the White House's July 2023 proposal, the FCC will select third-party administrators to verify security labeling applications from IoT manufacturers. Additionally, the FCC seeks public input on how software from adversarial nations might pose risks to U.S. national security.

March 17 - Iran Discussed with the Private Sector Promoting the Use of AI for Advancing Local Economy – The Iranian President, Ebrahim Raisi, engaged in a pivotal discussion with 15 representatives from the local private sector, as reported by the Iranian Tasnim news agency. The focus of the meeting was on delineating financial and regulatory strategies to bolster prosperity, foster innovation, and propel the digital economy. Additionally, deliberations revolved around initiatives aimed at equipping the youthful workforce with requisite skills and facilitating job creation. Notably, this significant gathering occurred approximately a week subsequent to the signing of a memorandum of understanding between Iran and Russia, delineating collaboration on AI ethics. Under the terms of this memorandum, the two nations will exchange vital insights and explore potential measures to integrate ethical considerations into the development and deployment phases of AI technologies.

March 18 – Six Countries Joined an International Initiative for Limiting Misuse of Spyware – During the third Summit for Democracy (S4D3) which convened in Seoul, South Korea, Secretary of State Antony Blinken unveiled a collaborative initiative led by the United States to combat the proliferation and misuse of commercial spyware, with Finland, Germany, Ireland, Japan, Poland, and the Republic of Korea joining in. Delegates at the summit engaged in extensive discussions centered on identifying best practices and extracting pertinent lessons for thwarting the misuse of spyware. Under this initiative, participating nations commit to actively engage in programs geared towards monitoring and exchanging crucial information concerning the spread and exploitation of spyware. Furthermore, a unanimous consensus was reached among the countries to enact measures aimed at curbing the export of software and technologies that could potentially be harnessed for malicious activities in cyberspace.