MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

# CYBER *Digest*

September 2023

## Key takeaways from the BRICS Summit

The recent BRICS Summit convened in Johannesburg addressed a wide range of topics, with discussions encompassing matters related to cyber and technology, among others. The group welcomed the ongoing initiatives undertaken by the Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes.[1] This is in response to the evolving landscape of criminal activities and increasing sophistication in utilizing ICTs for such illicit purposes. The group also reaffirmed its support for an "open, secure, stable, accessible and peaceful ICT-environment" while intensifying cooperation in using ICTs and the internet. The declaration also supported the UN's leading role in "promoting constructive dialogue on ensuring ICT-security, including within the UN Open-Ended Working Group on the security of and in the use of ICTs 2021-2025".

## Pakistan's agencies bought Israeli spyware tools

According to reports, Pakistan's Federal Investigation Agency and multiple law enforcement agencies within the country have been using products developed by the Israeli cyber technology company, Cellebrite.[2] The hacking tool enables law enforcement agencies to conduct digital forensic investigations by accessing password-protected mobile devices and copying all the data stored on them, encompassing images, documents, text messages, call logs, and contact information. The Cellebrite's tools were sold to Pakistan via Singapore, as Pakistan has no diplomatic relations with Israel.

## Japan to build cyber defense network in Indo-Pacific

The Japanese government came out with its plan to build an information network in the Indo-Pacific region to counter cyberattacks and with a focus on providing support to Pacific island countries from threat actors.[3] The network will be used for information sharing to provide appropriate time to respond to a cyber incident. The Foreign Ministry has also earmarked strengthening cyber capabilities overseas in the fiscal 2024 draft budget. In addition, Japan also plans to provide capacity building through joint training sessions. Japan is also broadening its cyber capabilities within the Quad framework, comprising the United States, Australia, and India as its members, and through closer collaboration with the Association of Southeast Asian Nations (ASEAN).

## Huawei to install surveillance systems across Afghanistan

Afghanistan's Taliban led government has been working with Huawei technologies to install surveillance systems and tools across the country, according to reports.[4] The agreement to work together was reached in the month of August, to install advanced camera systems in every province of Afghanistan. However, the representatives from the Huawei technologies denied any meeting with Taliban officials. The recent collaboration on surveillance systems is seen as a response to growing threats posed by ISIS in the country. Huawei has several advanced camera systems for surveillance that also includes home video surveillance systems. The company is not new to Afghanistan and has been selling mobile phone products in the country through local distributors.[5]

## Ecuador's election disrupted by cyber attack

According to reports, Ecuador's national elections were disrupted by cyber attacks, which the country's election agency said, were found to be originating from seven different countries.[6] The disruption mostly effected the absentee voters as they were unable to access the voting system before the polls closed. The official website of the National Electoral Council was reportedly down on the day of elections, leading users to an error message. About 120,000 Ecuadoreans living outside the country were registered to vote in the elections, and many of them were unable to access the voting system before polls closed.

## Breach in Poland's rail network

According to Polish media, the country's intelligence services are investigating a hacking attack on railway network.[7] The threat actors broke into railway frequencies to disrupt traffic in the north-west of the country, and the signals were interspersed with recording of Russia's national anthem and speech by President Putin. The incident brought about 20 trains to standstill, but services were restored within hours. According to assessments, the intrusion is been seen as Russia-linked and saboteurs appear to have sent simple "radio-stop" commands via radio frequency to the targeted trains.[8]

## Space observatories go offline after cyber attack

Two of the world's most advanced astronomy observatories based in Hawaii and Chile were forced to halt operations following a cyberattack.[9] Following the detection of a cyber incident on its computer systems, the National Optical-Infrared Astronomy Research Laboratory (NOIRLab) suspended astronomical observations. The lab acknowledged the incident in its public statement and confirmed the ongoing investigation. Following the incident, the National Counterintelligence and Security Center warned about foreign actors' efforts to target and exploit the US space industry, affecting US commercial firms and broader US national and economic security.

## Bangladesh hacktivists target critical infrastructure

According to a report, a hacktivist group that goes by the name Mysterious Team Bangladesh, carried out over 750 DDoS attacks within a year, citing religious and political reasons.[10] The activities also include web defacements and the group has undertaken attacks against India and other countries. The group was founded by a threat actor named D4RK TSN. The report also analyzed the main targets of the group, which includes India, Israel, and Australia. The hackers primarily target logistics, government, and financial sector entities, launching multi-phased campaigns with a country-centric focus rather than singling out individual companies.

## India File

- On 9 August 2023, the Indian Parliament passed The Digital Personal Data Protection Act to address the issue of personal data and privacy.[11] The law will apply to handling digital personal data in India, whether gathered online or obtained offline and then digitized. It will also apply to data processing activities conducted outside of India if they pertain to offering goods or services within India. Data fiduciaries will be required to preserve data accuracy, security, and deletion upon fulfilling its purpose. The bill also empowers individuals with rights to access information, request corrections and erasure, and seek grievance resolution.

- Following a cyber security incident in the company, Granules India Ltd, the maker of paracetamol, ibuprofen and metformin, reported a 62.5% fall in first-quarter profit.[12] The ransomware attack on the company caused major disruptions in its operations and also affected its revenue and profitability for the quarter. The attack exemplifies a company's reputational and economic costs following a cyber incident.

- According to reports, future investigations into cyberattacks on India's critical infrastructure and other sensitive digital infrastructure will be led by a specialized anti-cyber terrorism unit (ACTU) created within the National Investigation Agency (NIA).[13] The ACTU, which is yet to be finalized was sanctioned by the Ministry of Home Affairs last year to investigate the role of terrorists or state actors seeking anonymity.

- India and Trinidad and Tobago have signed a Memorandum of Understanding (MoU) for the mutual sharing of INDIA STACK, which comprises a set of open APIs and digital public assets designed to streamline identity verification, data exchange, and payment services on a broad scale.[14] Both sides have also agreed to cooperate in digital transformation by means of capacity building, training programs, exchange of best practices, and other measures.

- Ministry of Electronics & Information Technology (MeitY) launched the Indian Web Browser Development Challenge (IWBDC) spearheaded by MeitY, CCA and C-DAC Bangalore.[15] The IWBDC is an open challenge competition seeking to encourage developers and innovators to create an indigenous web browser with cutting edge technologies and enhanced protection features. The proposed browser would also focus on accessibility and user friendliness and envisions the ability to digitally sign documents using crypto token, bolstering secure transactions and digital interactions.

- The sixth session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in New York from 21 August to 1 September 2023 in Hybrid mode. Shri Amit Agrawal, CEO, UIDAI, MeitY, and Shri Tarun Kumar, Joint Director, MHA, co-led the Indian delegation. MEA representatives provided diplomatic support and outreach during the sixth session. During the session, the draft text of the convention was also negotiated. The next session will take place in New York in January-February 2024.

- The Indian Ministry of Defence has decided to transition from Microsoft Windows to 'Maya', an Ubuntu-based operating system developed by Indian government agencies.[16] The Maya OS has been developed by Indian government agencies to enhance cybersecurity measures. The new operating system will be supported by a security framework called Chakravyuh. This endpoint security system is concurrently being implemented on computers equipped with the Maya OS. As of now, the new operating system is being introduced only in computers within the Defence Ministry. While the Navy has reportedly approved the deployment of Maya in its systems, the Army and the Air Force are currently in the process of evaluating the software.

[1] Government of India (GoI), Ministry of External Affairs (MEA), Johannesburg II Declaration- Brics and Africa: Partnership for Mutually Accelerated Growth,

Sustainable Development and Inclusive Multilateralism, 23 August 2023, https://mea.gov.in/Images/CPV/Declaration_2408.pdf

[2] Haaretz, Pakistan's Spy Agency Buys Israeli Cellphone Hacking Tech, 3 August 2023, https://www.haaretz.com/israel-news/security-aviation/2023-08-03/ty-article/.premium/pakistans-spy-agency-buys-israeli-cellphone-hacking-tech/00000189-b608-db5d-a5fd-b62979680000

[3] Nikkei Asia, Japan to set up cyberdefense network that includes Pacific islands, 13 August 2023, https://asia.nikkei.com/Politics/International-relations/Japan-to-set-up-cyberdefense-network-that-includes-Pacific-islands.

[4] The Times of India, Taliban says Huawei to install cameras to locate terrorists, 25 August 2023, https://timesofindia.indiatimes.com/world/south-asia/taliban-says-huawei-to-install-cameras-to-locate-terrorists/articleshow/103067834.cms

[5] Tech Wire Asia, Will the Taliban use Huawei's camera system to locate militants in Afghanistan?, 29 August 2023, https://techwireasia.com/2023/08/will-the-taliban-use-huaweis-camera-system-to-locate-militants-in-afghanistan/

[6] The Record, Ecuador's national election agency says cyberattacks caused absentee voting issues, 22 August 2023, https://therecord.media/ecuador-election-cyberattacks-absentee-voting

[7] BBC, Poland investigates cyber-attack on rail network, 26 August 2023, https://www.bbc.com/news/world-europe-66630260

[8] Wired, The Cheap Radio Hack That Disrupted Poland's Railway System, 27 August 2023, https://www.wired.com/story/poland-train-radio-stop-attack/

[9] Cybernews, Cyberattack blinded two of the most advanced telescopes in the world, 1 September 2023, https://cybernews.com/news/cyberattack-blinded-two-of-the-most-advanced-telescopes-in-the-world/

[10] Cybernews, Bangladesh hacktivists target critical infrastructure in India, Israel, and Australia, 3 August 2023, https://cybernews.com/news/mysterious-team-bangladesh-hacktivists-attack-india-israel-australia/

[11] PRS Legislative Research, The Digital Personal Data Protection Bill, 2023 , https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

[12] Reuters, Paracetamol maker Granules India' Q1 profit hurt by cyber attack disruptions, 9 August 2023, https://www.reuters.com/business/healthcare-pharmaceuticals/paracetamol-maker-granules-india-q1-profit-hurt-by-cyber-attack-disruptions-2023-08-09/

[13] Hindustan Times, Specialised unit within NIA to lead probes into cyberattacks, 13 August 2023, https://www.hindustantimes.com/india-news/specialised-unit-within-nia-to-lead-probes-into-cyberattacks-101691867415960.html

[14] Press Information Bureau (PIB), India Signs MoU with Trinidad and Tobago on sharing INDIA STACK, 17 August 2023, https://pib.gov.in/PressReleasePage.aspx?PRID=1949830

[15] PIB, Launch of Indian Web Browser Development Challenge (IWBDC), 9 August 2023, https://pib.gov.in/PressReleasePage.aspx?PRID=1947243

[16] The Hindu, Why is India's Defence Ministry ditching Microsoft Windows for Ubuntu-based Maya OS?, 13 August 2023, https://www.thehindu.com/sci-tech/technology/why-is-indias-defence-ministry-ditching-microsoft-windows-for-ubuntu-based-maya/article67187333.ece