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

CYBER *Digest*

October 2023

- **Key takeaways from G20 New Delhi Leaders' declaration**
- **China bans iPhones for government employees**
- **Bangladesh enacts Cybersecurity law**
- **Government networks face Ransomware Attacks**
- **China investing in reshaping global information environment**
- **UK says it is conducting hunt forward operations**
- **ICC contemplates cyberwar crime prosecutions**
- **India File and Cyber Diplomacy Round-up**

Key takeaways from G20 New Delhi Leaders' declaration

At the 18th G20 Summit, held on September 9-10, 2023, in New Delhi under the presidency of India, member nations made a range of commitments. Acknowledging the significance of a secure, inclusive digital public infrastructure (DPI) that upholds human rights, personal data protection, and privacy, the declaration welcomed the G20 Framework for Systems of Digital Public Infrastructure.[1] This framework is voluntary and serves as a recommended guideline for the development, implementation, and governance of DPI. The declaration also embraced India's proposal to establish and maintain a Global Digital Public Infrastructure Repository (GDPIR), which would serve as a virtual repository for DPI.

Intending to enhance cybersecurity in the digital economy through information exchange, the countries welcomed the G20 Toolkit on Cyber Education and Cyber Awareness of Children and Youth. The toolkit aims to share best practices cultivated by multiple G20 member nations and guest countries to promote cyber education and awareness among children and youth.[2] The declaration also reiterated the commitment to the G20 AI Principles (2019) and pledged to collaborate in sharing information regarding the usage of AI to facilitate solutions within the digital economy. Furthermore, there was a commitment to promote the responsible use of AI to advance progress towards achieving the Sustainable Development Goals (SDGs).

China bans iPhones for government employees

According to reports, the Chinese government has instructed its officials to refrain from using Apple iPhones for official purposes and discourage them from bringing these devices into the workplace.[3] This action aims to reduce China's dependence on foreign technology to prevent sensitive data from being exposed to foreign governments. Although the initiative primarily encompasses foreign-made smartphones, Apple is particularly notable in this context due to its significant presence in China, where it maintains one of its largest markets.

Bangladesh enacts Cybersecurity law

The Cyber Security Bill of 2023 was passed in Bangladesh's Parliament, keeping offenses under four sections non-bailable.[4] The new law seeks to replace the widely discussed Digital Security Act, which had made offenses under fourteen sections non-bailable. According to the provisions of the Bill, police inspectors are granted the authority to conduct searches and make arrests without requiring a warrant. Nevertheless, the Bill also includes provisions for punishing those who file false cases. Opposition party members have criticized several clauses of the Bill, arguing that the constitution guarantees freedom of thought and expression as well as the recognition of independent media.

Government networks face Ransomware Attacks

Sri Lanka's government email network experienced a ransomware attack that resulted in the deletion of several months' worth of data from numerous email accounts, including those belonging to high-ranking government officials.[5] The government authorities officially confirmed this incident. The attack impacted nearly 5,000 email addresses linked to the gov.lk email domain. Among the victims were members of Sri Lanka's Council of ministers. The targeted system, known as Lanka Government Cloud (LGC), was compromised and had its backups encrypted as part of the attack. It is believed that the breach occurred sometime between May 17 and August 26, rendering the backups of that period also unusable. The identity of the ransomware group responsible for the incident remains unknown though it is believed to have been carried out by the LockBit or BlackCat ransomware group.[6] According to Sri Lanka's Information and Communication Technology Agency (ICTA), the attackers may have accessed the targeted system by utilizing malicious links sent to government employees.

In another similar incident in Colombia, the Ministry of Health and Social Protection, along with the country's Judiciary Branch and the Superintendency of Industry and Commerce, have jointly disclosed that a cyberattack on the technology provider IFX Networks Colombia has resulted in a series of issues that have hampered the functioning of these government departments.[7] The IT team in the ministry confirmed that IFX Networks reported a ransomware attack affecting several machines. No ransomware gang has publicly taken credit for the incident.

China investing in reshaping global information environment

According to the US Department of State's report, China is investing heavily in reshaping the global information environment to its advantage.[8] Beijing has allocated substantial financial resources, amounting to billions of dollars, to establish a worldwide information ecosystem that advances its propaganda efforts, enables censorship, and fosters the dissemination of disinformation. The report identifies five key components of the People's Republic of China's (PRC) information manipulation efforts: "leveraging propaganda and censorship, promoting digital authoritarianism, exploiting international organizations and bilateral partnerships, pairing co-optation and pressure, and exercising control over Chinese-language media".

UK says it is conducting hunt forward operations

In a recent interview, the Deputy Commander of the United Kingdom's Strategic Command, who oversees the Ministry of Defence's offensive and defensive cyber capabilities, admitted that the UK has engaged in hunt forward operations.[9] Hunt forward operations involve military cyber experts deploying to

a foreign nation to identify and counter malicious activities on the host nation's networks. U.S. Cyber Command originally developed this approach. The National Cyber Force (NCF) is an entity that brings together various British offensive cyber capabilities. It comprises personnel from different organizations, including the signals intelligence agency GCHQ (Government Communications Headquarters), the Secret Intelligence Service, and the Ministry of Defence (MoD).

ICC contemplates cyberwar crime prosecutions

For the first time, the lead prosecutor of the International Criminal Court in The Hague has made a clear declaration that the Court will investigate and prosecute cybercrimes that breach established international law, akin to its handling of war crimes occurring in the physical realm.[10] His office will investigate cybercrimes that have the potential to contravene the Rome Statute, which is the treaty that outlines the court's jurisdiction to prosecute unlawful acts, encompassing war crimes, crimes against humanity, and genocide. A spokesperson for the Office of the Prosecutor has additionally verified that this is now the official position of their office.

India File and Cyber Diplomacy Round-up

- The Insurance Regulatory and Development Authority of India (IRDAI) has established a standing committee dedicated to cyber security. This committee will conduct regular reviews of the risks associated with current and emerging technologies.[11] Additionally, the committee will propose suitable modifications to the framework to enhance the cybersecurity readiness and resilience of the insurance industry.

- The Crime and Criminal Tracking Network and Systems (CCTNS) website of the Tamil Nadu police was reportedly hacked by individuals believed to be operating from South Korea.[12] The hackers allegedly demanded a $20,000 ransom to restore the site. In response, the State police notified the Electronics Corporation of Tamil Nadu (ELCOT) to remove the compromised links and safeguard the data. A preliminary investigation has unveiled that the suspects successfully breached the website by identifying two logins with insufficiently strong passwords.

- The Fifth edition of the India -Japan Cyber Dialogue was held in Tokyo on 14 September 2023. Led respectively by Smt.Muanpuii Saiawi, Joint Secretary (CD) and Mr Ishizuki Hideo, Ambassador in-charge of Cyber Policy, Ministry of Foreign Affairs (MOFA) of Japan, the two sides discussed areas of bilateral cyber cooperation and exchanged views on latest developments in cyber domain and mutual cooperation at the United Nations and other multilateral and regional fora, including under the Quad framework.

- The National Security Council Secretariat coordinated the fourth India-Russia Bilateral Inter-agency Consultations on cooperation in ensuring security of the use of Information and Communication technologies (ICT) which was held in New Delhi from 14-15 September 2023.

[1] Government of India (GoI), Ministry of External Affairs (MEA), G20 New Delhi Leaders' Declaration, 2023, https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf

[2] G20, G20 Toolkit on Cyber Education and Cyber Awareness for Children and Youth, https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/Toolkit_Cyber_Edu_and_Cyber_Awareness.pdf

[3] The Verge, China bans iPhone use for government work, 6 September 2023, https://www.theverge.com/2023/9/6/23861353/china-bans-iphones-foreign-smartphones-government-officials-us-tiktok-restrictions

[4] Dhaka Tribune, Parliament passes Cyber Security Bill 2023, 13 September 2023, https://www.dhakatribune.com/bangladesh/325228/parliament-passes-cyber-security-bill-2023

[5] The Record, Sri Lankan government loses months of data following ransomware attack, 11 September 2023, https://therecord.media/sri-lanka-loses-months-of-government-data-in-ransomware-attack

[6] TEISS, Sri Lanka government loses vital email data in a major ransomware attack, 14 September 2023 https://www.teiss.co.uk/news/sri-lanka-government-loses-vital-email-data-in-a-major-ransomware-attack-12845

[7] The Record, Several Colombian government ministries hampered by ransomware attack, 15 September 2023, https://therecord.media/colombia-government-ministries-cyberattack

[8] U.S. Department of State, How the People's Republic of China Seeks to Reshape the Global Information Environment, 28 September 2023, https://www.state.gov/how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/

[9] The Record, British Army general says UK now conducting 'hunt forward' operations, 25 September 2023, https://therecord.media/uk-hunt-forward-operations-lt-gen-tom-copinger-symes

[10] Wired, The International Criminal Court Will Now Prosecute Cyberwar Crimes, 7 September 2023, https://www.wired.com/story/icc-cyberwar-crimes/

[11] The Hindu, IRDAI sets up inter-disciplinary standing committee on cyber security, 16 September 2023, https://www.thehindubusinessline.com/money-and-banking/irdai-sets-up-inter-disciplinary-standing-committee-on-cyber-security/article67315500.ece

[12] The Hindu, Tamil Nadu police website hacked by cyber criminals, 12 September 2023, https://www.thehindu.com/news/national/tamil-nadu/tamil-nadu-police-website-hacked-by-cyber-criminals/article67296670.ece