MANOHAR PARRIKAR

idsa

MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES

मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

March 2022

- **Russia-Ukraine Cyber Conflict updates**
- **Indian Government bans another 54 Chinese Apps**
- **JNPCT crippled by suspected cyber-attack**
- **Toyota's factories in Japan suffer a cyber-attack**
- **Chinese Cyber Firm claims Indian Research Institutes hacked by NSA**
- **The India File**

Russia-Ukraine Cyber Conflict updates

Russia's 'special military operation' in Ukraine starting February 23 was preceded and accompanied by large cyberattacks, in what has been regarded as an example of "hybrid" warfare. Since then, Ukraine has witnessed a second round of DDoS attacks against its websites as well as wiper malware infections spreading across Ukrainian networks and possibly spilling over into Latvia and Lithuania. Although no threat actor has been formally recognised as the perpetrator of the second series of attacks, the United States and other agencies have identified Russia as the perpetrator of the first round of attacks. Experts in cybersecurity and government authorities appear to believe that Russia is to blame for the most recent events. Cyberattacks, believed to originate from Ukraine and elsewhere, have also targeted Russian websites and crucial information infrastructure.[1]

On 24th February, the infamous hacker's collective, Anonymous on twitter, @YourAnonOne, claimed that it was targeting Vladimir Putin's regime. The gang has claimed responsibility for hacking the Russian Ministry of Defense database, as well as hacking various state television outlets to broadcast pro-Ukraine information. In the days after, the organisation has claimed responsibility for a number of cyber-attacks. Hackers also attacked the website of the Russian Space Research Institute and published files they claim were taken from Roscosmos, Russia's space agency. Cryptocurrency donations have garnered millions of dollars for Ukraine. [2]

Indian Government bans 54 more Chinese Apps

On 14th February, citing concerns of privacy and national security, the Ministry of Electronics and Information Technology issued an interim order to block access of 54 apps that were "allegedly collecting sensitive user data, which were being misused and transmitted to servers located outside India". The list of banned apps includes- Rise of Kingdoms: Lost Crusade, Tencent Xriver, Nice Video baidu, Viva Video Editor, Beauty Camera: Sweet Selfie HD, Beauty Camera - Selfie Camera, Garena Free Fire – Illuminate, Astracraft, FancyU pro, MoonChat, Barcode Scanner - QR Code Scan, Lica Cam, etc. In 2020 and 2021 the government had banned over 200 and 59 Chinese mobile applications respectively like TikTok, Shareit, Mi Video Call, Club Factory, Cam Scanner, WeChat and Bigo Live citing reasons of threat to sovereignty, integrity and security of the country.[3]

Singapore-based developer Garena's Free Fire, a popular battle royale game was one of the 53 apps banned by the Ministry of Home Affairs. However, the higher-graphic version of the popular game, Free Fire MAX, is still available on the Play Store, seemingly untouched by the prohibition.[4] The Singapore government has raised concerns over the ban with Indian authorities.[5]

After a similar game, PlayerUnknown's Battlegrounds (PUBG). was banned in 2020, it was relaunched as Battlegrounds Mobile India (BGMI) by the South Korean game developer Krafton, which had earlier licensed the mobile rights to the Chinese company Tencent.[6]

JNPCT crippled by suspected cyber-attack

The state-owned port authority's container terminal at Jawaharlal Nehru Port has been crippled since 21st February due to a suspected cyber-attack on the management information system (MIS). The officials at JNPCT stated that the information system

had stopped working and they had to divert a vessel. It is still unclear as to when the system will be restored. Currently, JNPCT is not accepting vessels alongside due to outage of the system as documents are needed to berth the ship, all of which are now digitalised. JNPCT is the busiest state-owned container port in India with a capacity of 1.35 million twenty-foot equivalent units (TEUs). [7]

Toyota's factories in Japan suffer a cyber-attack

After a suspected cyber-attack on a supplier of plastic parts and electronic components, Toyota Motor Corp halted domestic plant operations, resulting in a production loss of about 13,000 cars. There was no clarity on who was behind the alleged attack or what the motivation was. A spokesperson from Toyota described it as a "supplier system failure."[8] The attack occurred just after Japan joined its Western allies in condemning Russia for invading Ukraine. However, it is unclear whether the two incidents were connected. Fumio Kishida, Japan's prime minister, said his government would look into the incident and see if Russia was involved.[9]

Chinese Cyber Firm claims Indian Research Institutes hacked by NSA

Hackers affiliated to the US National Security Agency (NSA) were found to have introduced "covert backdoors" that may have given them access to sensitive information in dozens of nations, including India, Russia, China, and Japan, according to a new analysis from Beijing-based cybersecurity firm, Pangu Labs. India's Institute of Microbial Technology (IMTech), the Indian Academy of Sciences in Bengaluru, and the Banaras Hindu University were among those organisations allegedly targeted. The Beijing-based cybersecurity firm produced a technical study outlining how it discovered the backdoors and linked them to "unique IDs in the operating manuals of the National Security Agency" that were discovered in the 2013 NSA file leak by Edward Snowden. The study named dozens of targets including colleges and scientific research organisations — that had allegedly been hacked in many countries, including India, Japan, China and Russia.

Last year, the Union Power Ministry reported that "state-sponsored" Chinese hacking groups had targeted numerous Indian power centres, but that the groups had been foiled after government cyber agencies alerted the government to their operations. This came after a study from a cyber security firm in the United States linked a significant power outage in Mumbai in 2020 to hacking activities related to China.[10]

The India File

- **1st Foreign Ministers' Cyber Framework Dialogue**

Dr. S. Jaishankar, Minister of External Affairs co-chaired the 12th Foreign Ministers' Framework Dialogue (FMFD) and the 1st Foreign Ministers Cyber Framework Dialogue, with Australian Foreign Minister Ms. Marise Payne, in Melbourne, Australia on 12 February 2022. The Ministers discussed the progress made towards implementation of the India-Australia Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation and the subsidiary Plan of Action which was signed in June 2020 on the side-lines of the Virtual Leaders' Summit held between Prime Minister Shri Narendra Modi and Australian Prime Minister Scott Morrison.[11]

- **National Crime Record Bureau (NCRB) 2020 data on Cyber**

According to the National Crime Record Bureau (NCRB), cybercrime in India increased by 11% in 2020. The statistics for 2020 was taken from the NCRB's report "Crime in India, 2020." In 2020, a total of 50,035 cases of cybercrime were reported, representing an increase of 11.8 percent over 2019. (44,735 cases). In this category, the crime rate climbed from 3.3 in 2019 to 3.7 in 2020. In 2020, fraud accounted for 60.2 percent of all cyber-crime cases (30,142 out of 50,035 reported), with sexual exploitation accounting for 6.6 percent (3,293 incidents) and extortion accounting for 4.9 percent (2,440 cases).

The Standing Committee on Home Affairs, was informed that law enforcement agencies in some states, such as Punjab, Rajasthan, Goa, and Assam, do not have a single cybercrime unit, while Andhra Pradesh, Karnataka, and Uttar Pradesh only have one or two cybercrime cells.[12]

- **Army launches its first hackathon to improve cyber warfare**

A first-of-its-kind Hackathon was held at the Military College of Telecommunication Engineering (MCTE), Mhow. Over 15000 students participated in the virtual "Sainya Ranakshetram" event, which was held from October 1 to December 31, 2021. The competition included a variety of challenges involving Secure Coding, Software Defined Radio exploitation, and Cyber Offensive skills. The event drew participants from all around the country, with a strong showing from rural and distant locations. At the concluding ceremony held online, Chief of the Army Staff General MM Naravane congratulated the Hackathon victors, noting that cyber threats from a variety of actors are one of the most pressing concerns facing the country today.[13]

- **UN AD HOC COMMITTEE on Cybercrime holds session in New York**

The First Session of The Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established by the General Assembly in its resolution 74/247 is being held in New York from 28 February 2022 to 11 March 2022 in hybrid mode. A two member delegation to New York representing India in the Meeting is being led by Ms. Muanpuii Saiawi, Joint Secretary (CD). [14]

In an earlier session on organizational matters held on Thursday, 24 February 2022 Mr. Eric Do Val Lacerda Sogocio (Brazilian) was elected as Vice Chair of the Ad Hoc Committee of GURLAC Countries. The Japanese candidate was elected with consensus from the Asia Pacific region as there was only one candidate from that region.

[1] Russia-linked cyberattacks on Ukraine: A timeline at **https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html**

[2] Hacktivists Stoke Pandemonium amid Russia's War in Ukraine at **https://www.wired.com/story/hacktivists-pandemonium-russia-war-ukraine/**

[3] MHA recommends ban on 54 Chinese apps citing security concerns at **https://www.thehindu.com/news/national/mha-recommends-ban-on-54-chinese-apps-citing-security-concerns/article65048256.ece**

[4] Free Fire banned in India: 'Working to address this situation,' says Garena at **https://indianexpress.com/article/technology/gaming/garena-free-fire-banned-in-india-company-statement-7776209/**

[5] Singapore hopes India ban on Sea's game can be resolved quickly at **https://www.reuters.com/world/asia-pacific/singapore-hopes-india-ban-seas-game-can-be-resolved-quickly-2022-03-02/**

[6] Spooked by India ban, PUBG parent revokes Tencent publishing rights at **https://www.techcircle.in/2020/09/08/tencent-publishing-rights-for-pubg-revoked-in-india**

[7] Suspected cyber-attack cripples box terminal run by Jawaharlal Nehru Port Authority at **https://www.thehindubusinessline.com/economy/logistics/suspected-cyber-attack-cripples-box-terminal-run-by-jawaharlal-nehru-port-authority/article65073293.ece**

[8] Toyota to restart all suspended Japan plants after supplier cyberattack at **https://www.japantimes.co.jp/news/2022/02/28/business/corporate-business/toyota-plants-close-cyberattack/**

[9] Toyota suspends domestic factory operations after suspected cyber-attack at **https://www.reuters.com/business/autos-transportation/toyota-suspends-all-domestic-factory-operations-after-suspected-cyber-attack-2022-02-28/**

[10]U.S. group hacked top research institutes in India, Russia and China, says Beijing cyber firm at **https://www.thehindu.com/news/international/us-group-hacked-top-research-institutes-in-india-russia-and-china-says-beijing-cyber-firm/article65079559.ece**

[11] Joint Statement on the Inaugural India-Australia Foreign Ministers' Cyber Framework Dialogue at **http://www.mea.gov.in/bilateral-documents.htm?dtl/34860/Joint+Statement+on+the+Inaugural+IndiaAustralia+Foreign+Ministers+Cyber+Framework+Dialogue**

[12] 11% jump in cybercrime in 2020, NCRB data in Home Panel report at **https://www.business-standard.com/article/current-affairs/11-jump-in-cyber-crime-in-2020-ncrb-data-in-home-panel-report-122021100189_1.html**

[13] Indian Army Conducts First Ever Hackathon at Military College of Telecommunication Engineering, Mhow at **https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1797235**

[14] Video of the first session First session, Ad Hoc Committee on Cybercrime, (Indian statement at 35:00) at **https://media.un.org/en/asset/k1c/k1cr4qjobl**