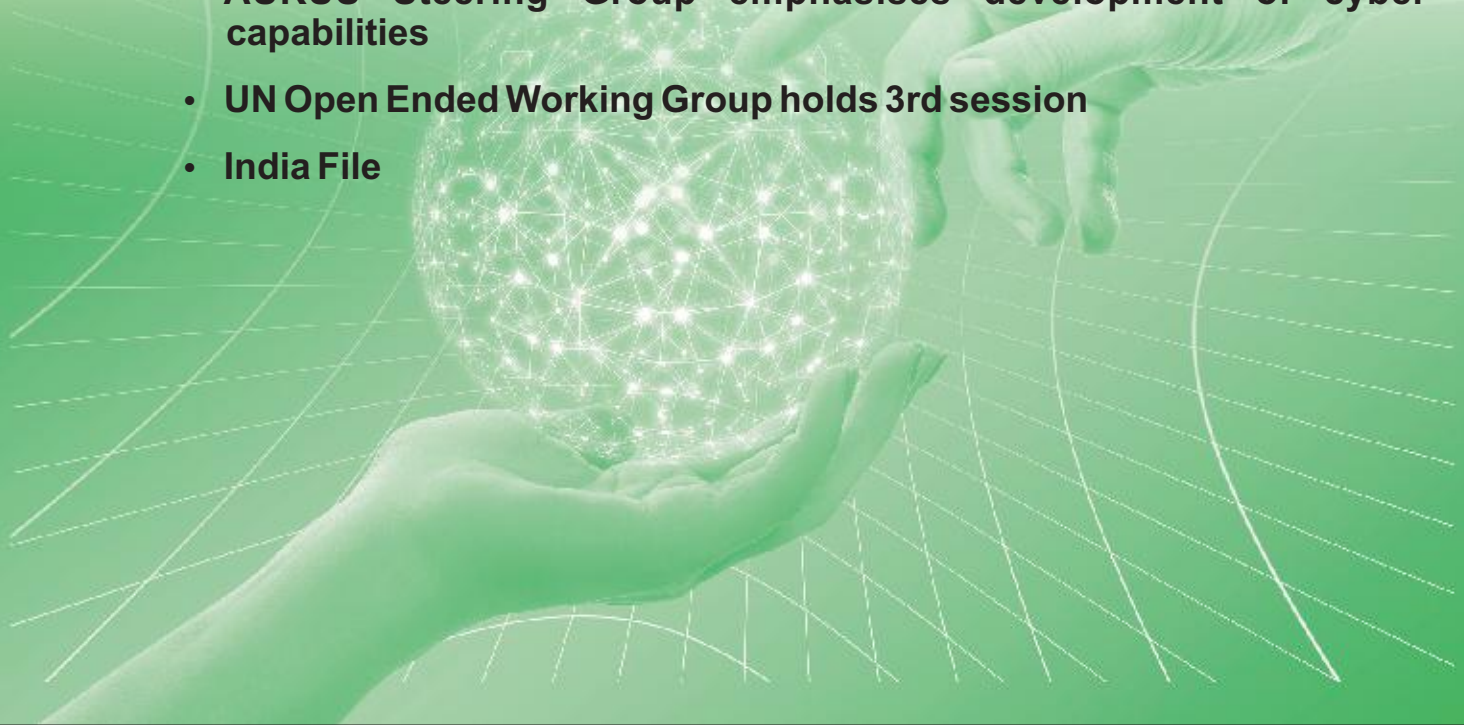
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

August 2022

- **Update on Russia-Ukraine Cyber Conflict**
- **Pro-China Digital Campaign found targeting Mining Companies**
- **North Korea and Cryptocurrency**
- **UK to amend its draft Online Safety law**
- **Telecom procurement rules modified on cybersecurity concerns**
- **Belgium cyberattacks traced to Chinese APT actors**
- **AUKUS Steering Group emphasises development of cyber capabilities**
- **UN Open Ended Working Group holds 3rd session**
- **India File**



Update on Russia-Ukraine Cyber Conflict

The cyber conflict between Russia and Ukraine has largely been limited to cyberespionage and influence operations, with some low-level, nuisance-level distributed denial-of-service (DDoS) attacks. The Ukrainian State Service for Special Communications and Information Protection (SSSCIP) released a report on the current state of the cyber phases of Russia's conflict. It believes Russia is primarily focused on espionage, network disruption, data wiping, and disinformation. Following are major cyber-related activities in the region for the month of July:

- Killnet, a Russian threat actor that poses as a hacktivist movement working in Russia's patriotic interest carried out several cyberattacks against Russia's adversaries. It carried out a DDoS attack against Lithuania's state and private institutions. They also claimed responsibility for a DDoS attack on the US Congress and Poland government websites. Furthermore, in its Telegram channel, the same group, also known as the Cyber Spetsnaz, announced a campaign against Norway.
- According to a report, Cozy Bear, a unit of Russia's Foreign Intelligence Service (SVR), is using Brute Ratel C4, a pentesting tool that has been in use since December 2020, in a variety of cyberespionage campaigns. The threat actor uses popular cloud storage services to avoid detection.
- There has also been an increase in Chinese cyberespionage activity directed against Russian targets using phishing emails to deliver office documents to exploit targets in order to deliver their RAT of choice, most commonly Bisonal.
- Turla, a Russian-aligned actor, has been found impersonating the Azov Regiment and offering malicious apps that misrepresent themselves as a type of do-it-yourself kit patriotic Ukrainians can use to launch DDoS attacks against Russian networks. The apps, in actuality, install malware on the devices to which they are downloaded.
- The US Cyber Command and the Ukrainian CERT have accused Russia of spear phishing Ukrainian entities by using evacuation and humanitarian documents.
- CERT-UA has warned that Windows systems in Ukraine were under attack by Russian operators deploying the Dark Crystal RAT (DCRat), a commercial .NET Remote Access Trojan (RAT).
- The Cyber National Mission Force of US Cyber Command has made available a sizable collection of indications of compromise (IOCs) collected from Ukrainian networks. The disclosure also shows how closely US Cyber Command is collaborating with its counterparts in the Ukrainian Security Service.
- The US Cybersecurity and Infrastructure Security Agency (CISA) and the State Service of Special Communications and Information Protection (SSSCIP) of Ukraine signed a Memorandum of Cooperation. According to CISA, the two agencies will collaborate "on shared cybersecurity priorities" in three areas: 1) Information exchanges and sharing of best practises on cyber incidents; 2) Critical infrastructure security technical exchanges; and 3) Cybersecurity training and joint exercises.

Pro-China Digital Campaign found targeting Mining Companies

According to the cybersecurity firm Mandiant, a pro-China propaganda campaign used sham social media accounts to incite opposition, including protests, against mining companies that challenge China's business interests. The digital campaign, called Dragonbridge, has flooded Twitter and Facebook in recent months with posts raising environmental and health concerns about the operations of three major mining companies: Australia's Lynas Rare Earths Ltd (LYC.AX), Canada's Appia Rare Earths and Uranium Corp (API.CD), and USA Rare Earth.

North Korea and Cryptocurrency

In an attempt to fund their weapons programme, North Korean state-sponsored threat actors laundered some $100 million looted from Harmony's Horizon blockchain bridge, a service that allows funds to be transferred from one blockchain to another. Furthermore, The US Department of Justice has seized $500,000 worth of Bitcoin from suspected North Korean hackers. In 2021, the hackers used a new strain of ransomware to target healthcare providers, extorting money from several organisations. Authorities in the United States say they have already returned ransom payments to two hospital groups. According to a report, North Korean hacker groups have generated more than $1 billion for their government through ransomware.

UK to amend its draft Online Safety law

The United Kingdom is amending its upcoming online safety law, which will require social media apps and search engines to combat "state-linked disinformation" or face fines. According to a statement from the Department for Digital, Culture, Media, and Sport, "social media platforms, search engines, and other apps and websites that allow people to post their own content will have a legal duty to take proactive, preventative action to identify and minimise people's exposure to state-sponsored or state-linked disinformation aimed at interfering with the UK."

Telecom equipment procurement rules modified on cybersecurity concerns

India has changed its telecom licensing rules to make it more difficult for Chinese vendors to sell to local operators. The Department of Telecommunications (DoT) announced that telecom licences will require operators to purchase network expansion and upgrade equipment from trustable vendors. India has begun laying the groundwork for 5G services, which, according to the Ministry of Communications and Electronics and Information Technology, will be operational before the year-end.

Belgium cyberattacks traced to Chinese APT actors

The Belgian government stated that it had detected three Chinese APT actors -UNSC 2814, GALLIUM, and SOFTCELL- attacking its government and armed forces. The statement doesn't give details on the nature of the attacks other than to describe them as "malicious cyber activities that significantly affected our sovereignty, democracy, security and society at large by targeting the FPS Interior and the Belgian Defence." Belgium's Foreign Ministry issued a press statement where it "strongly denounced these malicious cyber activities, which are undertaken in contradiction with the norms of responsible state behaviour as endorsed by all UN member states."

AUKUS Steering Group emphasises development of cyber capabilities

Australia, the United Kingdom, and the United States of America held meetings of the AUKUS Joint Steering Groups, which were established as part of the governance structure of the AUKUS partnership in September 2021. On July 28 and 29, the Joint Steering Group for Advanced Capabilities met to examine progress on key defence capabilities. The participants decided to increase near-term capabilities in cyber, counter-hypersonics, and hypersonics, as well as joint military capabilities.

UN Open Ended Working Group holds 3rd session

The Third Substantive Session of the new Open Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025 was held in New York from 25 to 29 July 2022. Smt.Muanpuii Saiawi, Joint Secretary (NEST & CD) led the Indian delegation. The Third Substantive Session of the OEWG adopted its First 'Annual Progress Report' on consensus basis. This marks an important milestone in the work of the OEWG to further discuss the six pillars of its mandate and build common understanding and consensus on the ICT security matters under the UN framework. India reiterated its call for creating a "permanent mechanism for exchanging views and ideas related to capacity-building in ICTs" in the form of an integrated and comprehensive portal. (Video timestamp at 29:47

India File

- **Panel to devise strategy to fight cyberattacks: MHA**

  Union home minister Amit Shah said a committee would be formed under the Union home secretary to formulate a strategy to combat cyberattacks, citing the grave national security implications. The cybercrime panel, which will include representatives from all state governments and departments involved, will develop a unified strategy to combat the threat.

- **MHA to analyse 'Phishing Havens'**

  The Ministry of Home Affairs (MHA) has launched an on-the-ground investigation, beginning in Jamtara, India's "phishing capital," to develop a roadmap for combating cybercrime. Senior ministry officials visited cities notorious for cyber crooks — Jamtara, Deoghar, Giridih, and Bokaro — and met with state officials.

- **8th BRICS Communications Ministers Meeting held**

  The 8th Meeting of BRICS Communications Ministers was held in virtual mode under the presidency of China. Minister of Railways, Communications, Electronics and Information Technology Ashwini Vaishnaw, participated in the meeting and highlighted achievements of India in the field of ICT. He also underlined the reforms undertaken by the Government in the Telecom sector. The Ministers decided to work in the field of ICTs in areas identified at the 14th BRICS Summit held on 23-24 June 2022. All Ministers appreciated the work-plans finalised for BRICS Institute for Future Networks (BIFN), Digital BRICS Task Force (DBTF) and hoped that these mechanisms will help in deepening Innovative cooperation among BRICS countries.

- **India, UK NSAs discuss Cyber Cooperation**

  Ajit Doval, national security adviser, met with Sir Stephen Lovegrove, his visiting counterpart from the United Kingdom where they talked about a wide range of bilateral and global issues. The key points

discussed included cybersecurity cooperation, maritime and Indo-Pacific security, regional security, and dealing with violent extremism.

- **UIDAI program to address Aadhaar biometric database vulnerabilities**

  The Unique Identification Authority of India (UIDAI) has established a bug bounty programme with the aim of enhancing security around the Central Identities Data Repository (CIDR), the database that houses the biometric data of over 1.3 billion holders of Aadhaar cards.

- **India-Australia Cyber Experts Meeting and JWG on ICT**

  First India-Australia Cyber Experts Meeting was held on 4 and 6 July 2022 in Canberra, Australia and 07 July 2022 in Sydney, Australia. First India-Australia Joint Working Group on ICT was held in Canberra, Australia on 5 July 2022. Smt.Muanpuii Saiawi, Joint Secretary (NEST & CD) led the Indian delegation consisting of officials of MEA and other line Ministries. Both sides discussed matters of mutual interest in cyberspace such as cyber governance, cybercrime, data protection and others.

- **SCO group of experts meeting held**

  A meeting of the Shanghai Cooperation Organisation (SCO) Group of Experts on International Information Security was held on 13 July 2022 in hybrid mode from Tashkent. The Working Group discussed the Plan of Cooperation adopted in the previous meetings along with cooperation in UN OEWG on Security of and in the use of ICTs and UN Ad Hoc Committee to develop a comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.