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

CYBER *Digest*

July 2022

- **Update on Russia-Ukraine Cyber Conflict**
- **Iran-Israel Cyberattacks**
- **CISA/ FBI Issue a Joint Warning Against Chinese Cyber Espionage**
- **INTERPOL's Operation Against Social Engineering Scams**
- **Slovenia's Cybersecurity Ex to Test Nuclear Safety Capabilities**
- **Canada Wants Firms To Report Cyberattacks**
- **Hacktivist Cyberattacks on Indian Government from Malaysia**
- **India File**

Update on Russia-Ukraine Cyber Conflict

According to Microsoft's latest report on the Russia-Ukraine Cyber Conflict, Russian targeting has been successful 29 percent of the time since the start of the conflict. Following are major cyber-related activities in the region for the month of June:

- Ukraine, a non-NATO member, joined the Atlantic Alliance's NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), formalising its membership during meetings in Tallinn, Estonia.
- DDoS attacks from Russia have disrupted connectivity in Ukrainian cities such as Kyiv, Luhansk, and Mariupol, as well as in countries sympathetic to Ukraine.
- General Paul Nakasone, the commander of US Cyber Command, stated in an interview that the US has conducted a series of offensive, defensive, and information operations against Russia in Ukraine.
- In a World Cup qualification match between Ukraine and Wales, Russian hackers replaced the game stream on OLL.TV with Russian coverage of the special military operation.
- Several dark web weapon marketplaces have listed military-grade firearms, such as Javelin anti-tank missiles, allegedly sent by Western countries to support the Ukrainian army in its fight against Russian invaders.
- Anonymous claims to have successfully hacked into Russia's drone suppliers, if not the actual drones. They also claim to have disrupted significant government activities in Belarus.
- Ukraine has begun to store sensitive data abroad in order to reduce its vulnerability to Russian physical or cyberattacks. The protection of "VIP" databases, or databases deemed critical to the operation of Ukraine's economy, has been prioritised.
- An attempt to hack the Urengoy Gas Pipeline in Russia has been attributed to a cyberattack by Ukraine's GUR intelligence service.
- Killnet, a Russia-based cyber threat group, operating as the Cyber Spetsnaz carried out DDoS attacks against Lithuania and Norway.

Iran-Israel Cyberattacks

In June, Israel and Iran were in the midst of many cyberattack allegations against each other. Microsoft announced that it had disrupted a cyber-operation against Israeli organisations carried out by the Lebanon-based group known as Polonium, which is linked to Iran's Ministry of Intelligence and Security. The campaign specifically targeted OneDrive users, and Microsoft claims to have suspended more than 20 malicious OneDrive apps created by Polonium actors. Researchers have described a complex spearphishing campaign targeting former Israeli officials as well as some American targets. Furthermore, on June 28, the hacktivist

group Gonjeshke Darande (Predatory Sparrow) targeted Khouzestan Steel Company, one of Iran's largest steel manufacturers.

CISA/ FBI Issue a Joint Warning Against Chinese Cyber Espionage

In Alert AA22-158A, the US Cybersecurity and Infrastructure Security Agency (CISA) and the FBI provided an overview of ongoing Chinese cyberespionage activity against US targets. According to the alert, Beijing's threat actors "continue to exploit publicly known vulnerabilities in order to establish a broad network of compromised infrastructure." Their typical approach, according to the warning, is to compromise unpatched network devices, particularly Small Office/Home Office (SOHO) routers and Network Attached Storage (NAS) devices. The advisory describes the targeting and compromise of major telecommunications companies and network service providers, as well as the top network device vulnerabilities routinely exploited by cyber actors since 2020.

INTERPOL's Operation Against Social Engineering Scams

Interpol has announced that its Operation First Light 2022, which targets telecommunications fraud, business email compromise, and money laundering, has resulted in significant criminal takedowns. Law enforcement agencies from 76 participating countries' raided national call centres suspected of telecommunications or scamming fraud, particularly telephone deception, romance scams, e-mail deception, and related financial crime.

Slovenia's Cybersecurity Ex to Test Nuclear Safety Capabilities

The Slovenian Nuclear Safety Administration (SNSA) conducted the Cyber Security Exercise to Test Nuclear Security Capabilities. This highly interactive exercise included hands-on examples and involved key Slovenian nuclear sector stakeholders. The scenario involved real operational technology systems with insider threats, external cyber-attacks, and physical intrusions into a fake nuclear facility, demonstrating the consequences of a computer security compromise of critical operational control systems leading to a nuclear security event.

Canada Wants Firms To Report Cyberattacks

Under a new law, Canadian firms operating in critical infrastructure sectors would be required to report cyberattacks to the federal government and strengthen their cyber systems. The legislation recognises the finance, telecommunications, energy, and transportation sectors as critical to national security and public safety. Designated companies would also be required to keep records of how they implement their cyber security programme, every cyber incident they are required to report, any steps taken to mitigate supply-chain or third-party risks, and any steps taken to implement a government-ordered action. While the proposed legislation only applies to federally regulated firms, the government hopes that provinces and territories will pass similar legislation to improve the cybersecurity of entities under their jurisdiction, particularly hospitals, police departments, and local governments.

Hacktivist Cyberattacks on Indian Government from Malaysia

Dragon Force, a Malaysian hacktivist group, called upon hackers all over the world to launch cyberattacks against the Indian government's information technology (IT) infrastructure. The group announced its plans on Twitter, calling the move a "special operation." Dragon Force has posted multiple instances of what they claim are breaches of various websites and departments in India since its announcement. The collective claims to have taken down the services of Hostnet India, a popular web hosting company in India, resulting in the shutdown of multiple companies' websites. Dragon Force also claimed to have published a list on Twitter that contained information belonging to members of the Indian government. However, the email addresses listed in the alleged database appeared to be personal addresses rather than official ones.

India File

- **7th Round of India-Bangladesh Joint Consultative Commission**

The seventh round of the India-Bangladesh Joint Consultative Commission (JCC) was held in New Delhi on 19 June. EAM S Jaishankar stated during the discussion that India is looking forward to working with Bangladesh on new areas of cooperation such as artificial intelligence, cybersecurity, start-ups, and fintech. A joint statement said the two ministers expressed satisfaction that despite challenges posed by the Covid-19 pandemic, both countries have worked closer than ever before in every sector, from security and border management to mutually beneficial trade and investment flows, as well as enhanced bilateral and sub-regional multimodal connectivity, greater power and energy cooperation, developmental assistance and capacity building exchanges, cultural and closer people-to-people ties.

- **India's Views on Cyber at ARF Senior Officials' Meeting**

Shri Saurabh Kumar, Secretary (East), virtually attended the ASEAN Regional Forum Senior Officials' Meeting (ARF SOM) on June 9, 2022. He also shared India's perspectives on the threat posed by terrorism and the challenges of cybersecurity. The meeting reviewed the 27-member ARF's activities and exchanges over the previous year and deliberated on its future plans and activities. Senior officials discussed regional and international developments, as well as the Covid-19 pandemic, terrorism, maritime security, and cybersecurity.

- **MeitY Republishes Proposed Changes to IT rules**

The Ministry of Electronics and Information Technology (MeitY) has republished a new draft of the IT Rules 2021 amendments. It has requested feedback from stakeholders within the next 30 days. The IT ministry said the proposed rule requires intermediaries to respect the rights guaranteed to users under the Constitution of India. This has been made necessary because a number of intermediaries have acted in violation of the constitutional rights of Indian citizens. It also proposed to create an appellate body 'Grievance Appellate Committee'. Users

will have the option to appeal against the grievance redressal process of the intermediaries before this new appellate body.

- **BRICS NSAs Discuss Challenges to National Security**

NSA Ajit Doval met with counterparts from China, Russia, Brazil, and South Africa during a virtual meeting on national security of the BRICS National Security Advisors and High Representatives hosted by China. The BRICS countries held an in-depth discussion and reached an agreement on issues such as strengthening multilateralism and global governance, as well as responding to new threats and challenges to national security. The meeting reviewed the work of the working group on counter-terrorism and cybersecurity, agreed to jointly promote plans and roadmaps for international counter-terrorism and cybersecurity cooperation, and uphold the central coordinating role of the United Nations in the global counter-terrorism cause.

- **CERT-In Extends Timeline for Cyber Security Rules**

To assist Micro, Small, and Medium Enterprises (MSMEs) in making the transition smoothly, the Indian Computer Emergency Response Team (CERT-In) extended the deadline for implementing the new cyber security rules until September 25, 2022. Aside from MSMEs, Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers, and Virtual Private Network Service (VPN Service) providers have been given an extension until September 25, according to a release from the Ministry of Electronics and IT (MeitY). CERT-In issued information security directions in April to promote an open, safe, trusted, and accountable Internet in the country. According to the new guidelines, data centres, VPS, and cloud service providers must keep a five-year record of customers' personal information.

- **India Hosts Fourth Indo-Japan Cyber Dialogue**

The Fourth India-Japan Cyber Dialogue was hosted by India virtually on 30 June 2022. The Indian Delegation was led by Smt. Muanpuii Saiawi, Joint Secretary, Cyber Diplomacy Division, Ministry of External Affairs (MEA), while the Japanese delegation was led by Mr Yutaka Arima, Ambassador in-charge of Cyber Policy, Ministry of Foreign Affairs (MOFA). Both sides discussed important areas of bilateral cyber cooperation and reviewed the progress achieved in the areas of cybersecurity and Information and Communication Technologies (ICTs) including 5G Technology.

- **Ad Hoc Committee On Cyber Crime**

The Second Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in Vienna from 30th May 2022 to 10 June 2022 on Hybrid mode. Smt. Muanpuii Saiawi, Joint Secretary (CD) led the Indian delegation to Vienna to represent India in the Meeting. The second inter-sessional consultations with other stakeholders was held on 13-14 June 2022 in Vienna, Austria in hybrid mode.