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

CYBER Digest

April 2022

- Update on Ukraine-Russia Cyber Conflict
- Second Session of UN Working Group held in New York
- US bill requiring mandatory cyber reporting passed into law
- Russian Hackers charged by the US for cyberattacks
- Singapore to establish a Digital Intelligence Unit
- Japan's Self-Defense Force forms a new cyber defense unit
- New cyber facility to boost Australian capabilities
- Largest-ever attack on Israeli Government sites reported
- Bangladesh Cyber Security Strategy in final stages
- $600 Million stolen in cryptocurrency hack
- India File

Update on Ukraine-Russia Cyber Conflict

As the Russian-Ukrainian conflict slid into the second month, unlike in the 2015 where Ukrainian power grids witnessed massive cyberattacks from Russia, in this conflict, the cyberwar has been largely focussed on wiper and denial-of-service attacks.[1] Two malware tools are being used to target Ukraine- IssacWiper and HermeticWizard which are a strain of wiper and worm respectively.[2] Also, a malware-as-a-service platform DanaBot is being used to run a distributed denial-of-service attack against the Ukrainian Ministry of Defense and there have also been reports of "local" Russian jamming of GPS in and around Ukraine. The Ukrainians, with help from allies, have been better prepared to deter Russian cyberattacks this time around. Companies such as Microsoft have also been pro-active in releasing patches to seal vulnerabilities.

Many hactivists have responded to Ukraine's call for help in targeting Russian networks and multiple instances have come to light of such attacks. Hacktivists claiming to be supporters of the Anonymous collective have taken down or defaced Russian media and government websites of TASS, RIA Novosti, Kommersant, and Izvestiya. Furthermore, Anonymous claims to have hacked into Russian television feeds and interrupted their programming with footage of the war against Ukraine. They also claim control over four-hundred Russian camera feeds.[3]

Ukraine's Defense Intelligence Service Cyber Operations Unit penetrated networks at Russia's Beloyarsk Nuclear Power Plant.[4] Ukraine's Centre for Defence Strategies released or doxxed a database of the names of 120,000 Russian servicemen who are fighting in Ukraine.[5]

ICANN, the Internet Corporation for Assigned Names and Numbers, the agency in charge of the domain numbering system informed the Ukrainian government in response to its request to shut down Russia's access to the Internet that such a step was unfeasible, both technically and as a matter of policy, as the Internet is a decentralised system and no one actor has the ability to control it or shut it down.[6]

However, many western companies have not shied away from taking actions against Russia. YouTube has banned Russian media outlets from its platform across Europe. [7] Meta, Facebook's corporate parent, has taken two steps: it has declassified Russian media content as possible disinformation, and it is experimenting with an encrypted Instagram messaging service to ensure user safety.[8] Also, In turn, Moscow has also blocked online access to the BBC and the Voice of America and aims to bring a new law that imposes penalties of up to fifteen years for intentionally disseminating "fake" news about the Russian military.[9]

There were also reports of Huawei helping Russia defend its networks. Australian Defence Minister Dutton has criticised Huawei for working on behalf of Russia, and accused Moscow and Beijing of having concluded an "unholy alliance."[10]

Second Session of UN Working Group held in New York

The Second 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 at New York from 28 March 2022 to 1 April 2022.

Smt. Muanpuii Saiawi, Joint Secretary (NEST & CD) led a two-member Indian delegation which delivered substantive statements on issues covered in the OEWG, viz., emerging cyber threats and cooperative measures to prevent and counter such threats, application of international law to the use of ICTs by States, confidence-building measures, cyber capacity building and the possibility of establishing a regular institutional dialogue under the auspices of the UN for all matters related to the use and security of ICTs.[11]

The Russia-Ukraine conflict found its way into many of the country statements, particularly pointing out that the OEWG was a Russian initiative and but was itself seen to be flouting many of the norms put forward in the OEWG. The Russian delegation complained that that its head of delegation had been denied a visa to attend the sessions and many unfounded accusations had been made against Russia in the sessions.

Through resolution 73/27, the General Assembly had established an Open-Ended Working Group (OEWG), in which all UN Member States are invited to participate. The Group was convened for the first time in 2019 and reported back to the General Assembly in 2020. The OEWG process also provides the possibility of holding inter-sessional consultative meetings with industry, non-governmental organizations and academia, although the modalities of doing so are still under discussion.

US bill requiring mandatory cyber reporting passed into law

President Joe Biden signed the Cyber Incident Reporting for Critical Infrastructure Act, which was included in an omnibus appropriations bill, into law on March 15, 2022. After failing to pass similar legislation in recent years, the House unanimously approved the bipartisan legislation on March 9 and the Senate unanimously approved the legislation on March 11 against the backdrop of high-profile cyberattacks on critical infrastructure providers and growing concerns about retaliatory cyberattacks relating to Russia and Ukraine conflict.

The White House had endorsed the bill that would require hospitals, power plants, water utilities, airports, and other key infrastructure to notify the Department of Homeland Security within 72 hours of a cyberattack. The decision came amid the escalating conflict in Ukraine and fears of Russian cyber threats to the United States. The FBI, and the Justice Department had sought modifications to assure that the FBI was also kept informed of cyberattacks. In a nod to concerns from private companies over liability, the agencies also called for such information to be kept out of the purview of the Freedom of Information Act, which permits the public to request records.

Russian Hackers charged by the US for cyberattacks

The US has filed criminal charges against four Russian government officials, alleging that between 2012 and 2018, they were involved in two massive hacking campaigns that targeted the global energy sector and impacted thousands of systems in 135 countries. The three alleged hackers from Russia's Federal Security Service (FSB) carried out cyberattacks on the computer networks of oil and gas companies, nuclear power plants, utility and power transmission companies around the world, according to a now-unsealed indictment from August 2021.

The Department of Justice accused Evgeny Viktorovich Gladkikh, a 36-year-old Russian ministry of defence research institute employee, of conspiring with others between May and September 2017 to hack a foreign refinery's systems and install malware known as "Triton" on a Schneider Electric safety system, according to a second unsealed indictment from June 2021. The two cases were unsealed just days after US President Joe Biden warned about "evolving intelligence," implying that the Russian government is considering methods for future cyber-attacks.[12]

Singapore to establish a Digital Intelligence Unit

Singapore is establishing a new digital intelligence branch inside the armed forces to strengthen the country's cyber defences. The government has described the move as vital, citing the rise in the number and sophistication of online threats, as well as attacks that target both physical and digital domains. The new Singapore Armed Forces (SAF) digital and intelligence service (DIS) branch will be entrusted with fighting online attacks. It is designed to aid the army's ability to fight as a unit.

The DIS, which is expected to be operational by the end of 2022, will allow the SAF to deal with current and future cyber threats, according to Singapore's Defence Minister Ng Eng Hen. He pointed out that cyber-threats were already spilling over into the physical realm, and that such threats were only going to get worse. DIS would also dedicate "special effort" to realising the "full potential" of emerging digital technologies such as cloud, AI, and data science. SAF's next-generation transformation initiatives would be accelerated as a result of this.[13]

Japan’s Self-Defense Force forms a new cyber defense unit

The Self-Defense Forces of Japan have formed a newly reorganised cyber-defense organisation to improve the country's response to cyber-attacks, a security arena that has become increasingly crucial in global conflicts. The 540-strong unit is in charge of human resources training, practical training support, and information and communication network management. Outer space, cyberspace, and the electromagnetic spectrum, according to the Japanese government, are critical pillars in maintaining the military balance among states and bolstering Japan's defence capabilities. The creation of a new cyber section at the Defense Ministry's Tokyo headquarters indicates the urgent need to boost the SDF's cyber capabilities. The new organisation would consolidate cyber countermeasures by bringing together cyber departments that were previously dispersed among the Ground, Maritime, and Air self-defense forces.[14]

New cyber facility to boost Australian capabilities

The Australian Signals Directorate (ASD) has opened a new cyber and foreign intelligence centre in Canberra. The new site will boost ASD's capabilities while also opening up new prospects for intelligence analysts, cyber operators, technology researchers, and corporate enablers. ASD is a member of the national security community that supports the Australian Defence Force (ADF) and the government with signals intelligence, cybersecurity, and offensive cyber operations. ASD and its Australian Cyber Security Centre will be able to better identify threats and disrupt potential adversaries through the new centre. It will also make collaboration between the private and public sectors easier in order to combat cyber threats and safeguard the country's interests.[15]

Largest-ever attack on Israeli Government sites reported

According to Israel's National Cyber Directorate, the country was subjected to a cyberattack that temporarily brought down a number of official websites. "A denial of service (DDoS) attack has been identified on a communications provider in the last few hours," the government-funded directorate wrote on Twitter. "As a result, for a brief period, access to a number of sites, including government sites, had been prevented." However, while Israel's government network is now accessible within Israel, web monitoring firm NetBlocks said that it remained "unreachable abroad." According to the Israeli newspaper Haaretz, a source in the country's defence establishment believes it was the country's largest-ever cyberattack.

Following this, Israel's Ministry of Communications undertook an "evaluation of the situation with the emergency services in the Ministry of Communications." It was not immediately clear who carried out the hack. Previous hacks on Israeli web sites have been attributed to attackers linked to Iran. Iran and Israel have been locked in a shadow war that includes cyberattacks as well as targeting of physical sites.[16]

Bangladesh Cyber Security Strategy in final stages

Bangladesh is preparing to implement a cybersecurity plan aimed at ensuring the proper functioning of cyberspace by increasing resilience to the growing threat of cyberattacks. The Digital Security Agency under the Information and Communication Technology (ICT) Division has already drafted the Bangladesh Cybersecurity Strategy for 2021-2025. The ICT Division will place the strategy before the cabinet for approval soon, after making necessary changes, if any, to it based on recommendations from other stakeholders.

The proposed cybersecurity policy, which is the first of its kind in Bangladesh, specifies that all ministries will be equipped with particular software and qualified staff to safeguard themselves against cyber-attacks. According to ICT Division officials, the draft strategy focuses on 10 points to confront future cyber challenges and improve the country's capacity in cyberspace. The major targets set in the draft document include enhancing national cybersecurity governance and ecosystem, improving organisational management and business operation, strengthening cybersecurity incident management and active cyber defence, enhancing national cybersecurity capacity, nourishing cybersecurity knowledge through education, and promoting a competitive local industry and ecology.[17]

$600 Million stolen in cryptocurrency hack

Hackers allegedly broke into gaming-focused blockchain network Ronin Network and stole coins worth more than $600 million, making it the second-largest cryptocurrency hack ever. 173,600 ether tokens and 25.5 million USD coins—worth nearly $620 million—were drained from its platform after an attacker used hacked private keys to forge two fake withdrawals. The platform discovered the attack after a user reported being unable to withdraw 5,000 ether tokens, worth $17 million, from the network.

The hack on Ronin marks one of the biggest hacks in cryptocurrency history and is even bigger than the $460 million hack on cryptocurrency exchange Mt. Gox that led to the company’s bankruptcy and heightened regulation in the nascent space about seven years ago. $14 billion worth of illicit money were received into cryptocurrency addresses last year, climbing 79% from one year prior and marking an all-time high for cryptocurrency-based crime, according to blockchain analytics firm Chainalysis, which cited the explosion in mainstream cryptocurrency adoption as a main catalyst.[18]

India File

- **New infrastructure to fight cybercrime in major cities**

Mumbai Police has decided to set up six state-of-the-art cybercrime investigation and forensic laboratories, as well as a first-of-its-kind Social Media Analytics lab and a Cyber Crime Analytics lab, to combat the growing number of cases of cybercrime in the city using advanced technological tools and expertise. The cyber laboratories will be set up at all five regions of the city — South, Central, East, West and North along with the Mumbai police headquarters' crime branch and will work on the lines of Forensic Science Laboratories, allowing the police to collect digital evidences, store them and use them to crack difficult cybercrime cases. [19]

Rakesh Asthana, Commissioner of Police, Delhi inaugurated the new premises of cyber police station North-West District at PS Model Town Complex, for detection and prevention of cyber crimes.

The aim is to deal with the complaints related to cyber crime with alacrity, swift response and professionalism, ensuring quality investigations of such crimes.[20] The Chandigarh Police are also working on setting up a cyber directorate, which will be equipped with all infrastructure to investigate cyber crimes under one roof and catch the elusive online fraudsters.[21]

- **India to establish a CSIRT to protect its power grids**

According to two government officials, the growing threat of cyberattacks on India's power system has spurred the government to consider forming a dedicated computer security incident response team (CSIRT) to counter any attempt to cripple the country's critical power infrastructure. The team, comprising trained professionals, including domain experts from the private sector, will be housed under India's apex power sector planning body, Central Electricity Authority (CEA). The officers will be recruited through the Combined Engineering Services Examination conducted by the Union Public Service Commission.[22]

- **India-Indonesia Security Dialogue**

National Security Advisor (NSA) Ajit Doval led the second India-Indonesia security dialogue with Coordinating Minister for Political, Legal, and Security Affairs of Indonesia Mohammad Mahfud. They discussed issues including cooperation in counter-terrorism, maritime, defence and cyber.[23]

- **660 technologies developed under National Mission on Interdisciplinary Cyber-Physical Systems**

Union minister Jitendra Singh told the Lok Sabha that 660 innovations have been developed under the National Mission on Interdisciplinary Cyber-Physical Systems, compared to a target of 6,824 technologies. The National Mission on Interdisciplinary Cyber-Physical Systems aims to address the technological requirements of the society, taking into account international trends and road maps of leading countries for the next generation technologies. Out of the mission target of 30,694 Human Resource Development, as many as 3,145 have been achieved, the Minister of State (Independent Charge) of the Ministry of Science and Technology and Earth Sciences added.[24]

- **Updates on Ad Hoc Committee On Cyber Crime**

The First Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in New York from 28 February 2022 to 11 March 2022 in Hybrid mode. Smt. Muanpuii Saiawi, Joint Secretary (CD) led the Indian delegation and delivered a statement on February 28, 2022. The Indian Statements and interventions can be seen at:

(i) https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/India.pdf

(ii) https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/India_-_Intervention.pdf

The AHC adopted the Agenda, Structure and mode of work during its 1st Session. The Second Session of AHC will be held in Vienna in May-June 2022.[25]

[1] The dire predictions about a Russian cyber onslaught haven't come true in Ukraine. At least not yet. At https://www.washingtonpost.com/technology/2022/02/28/internet-war-cyber-russia-ukraine/

[2] IssacWiper and HermeticWizard: New wiper and worm targeting Ukraine at https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[3] More Than 5 Million Anti-Propaganda Text Messages Sent to Russians in Anonymous Information Warfare at https://www.hstoday.us/featured/more-than-5-million-anti-propaganda-text-messages-sent-to-russians-in-anonymous-information-warfare/

[4] Russia's Beloyarsk Nuclear Power Plant has been breached by a GURMO Cyber unit at

https://jeffreycarr.substack.com/p/russias-beloyarsk-nuclear-power-plant

[5]Personal data of 120,000 Russian servicemen fighting in Ukraine at https://www.pravda.com.ua/eng/news/2022/03/1/7327081/

[6] Ukraine's request to cut off Russia from the global internet has been rejected at https://www.cnn.com/2022/03/03/tech/ukraine-russia-internet-icann/

[7] YouTube bans Russian media outlets across Europe at https://www.politico.eu/article/youtube-bans-russian-media-outlets-across-europe/

[8] Meta rolls out encrypted Instagram DMs in Russia and Ukraine at https://www.protocol.com/bulletins/encrypted-instagram-dms-russia-ukraine

[9] Russia fights back in information war with jail warning at https://www.reuters.com/world/europe/russia-introduce-jail-terms-spreading-fake-information-about-army-2022-03-04/

[10] Chinese telecom giant Huawei reportedly helping Russia to stabilise internet network at https://www.wionews.com/world/chinese-telecom-giant-huawei-reportedly-helping-russia-to-stabilise-internet-network-459936

[11] Initial Indian statement at 00:11:00 https://media.un.org/en/asset/k14/k1438emnab

Subsequent statements at 02:11:00 https://media.un.org/en/asset/k1l/k1l7rcax4f

and at 01:21:00 https://media.un.org/en/asset/k17/k17m9pt3k0

[12] US charges four Russian hackers over cyber-attacks on global energy sector at

https://www.theguardian.com/world/2022/mar/24/us-charges-russian-hackers-cyber-attacks

[13] Singapore to set up digital intelligence unit as cyber threats intensify at https://www.zdnet.com/article/singapore-to-set-up-digital-intelligence-unit-as-cyber-threats-intensify/

[14] Japan's SDF launches new cyber-defense unit at https://english.kyodonews.net/news/2022/03/2009b0fac163-japans-sdf-launches-new-cyber-defense-unit.html

[15] Australia's ASD unveils new cyber and foreign intelligence facility at

https://www.army-technology.com/news/australia-asd-cyber-intelligence-facility/

[16] Israel Says Government Sites Targeted by Hack at

https://www.securityweek.com/israel-says-government-sites-targeted-hack#:~:text=Israel's%20National%20Cyber%20Directorate%20said,number%20of%20government%20web%20sites.

[17] Bangladesh in final stages of clearing cyber security strategy at https://www.tbsnews.net/bangladesh/bangladesh-final-stages-clearing-cyber-security-strategy-376933

[18]Second Biggest Crypto Hack Ever: $600 Million In Ether Stolen From NFT Gaming Blockchain at https://www.forbes.com/sites/jonathanponciano/2022/03/29/second-biggest-crypto-hack-ever-600-million-in-ethereum-stolen-from-nft-gaming-blockchain/?sh=62e6a9da2686

[19] Coming soon: Six state-of-the-art cybercrime labs, social media lab to help Mumbai police tackle cyber crime at https://indianexpress.com/article/cities/mumbai/coming-soon-six-state-of-the-art-cyber-crime-labs-social-media-lab-to-help-mumbai-police-tackle-cyber-crime-7828655/

[20] Delhi Police Chief inaugurates new premises of cyber police station to curb crime at https://www.indiatoday.in/cities/delhi/story/delhi-police-chief-rakesh-asthana-hi-tech-cyber-police-station-1928878-2022-03-24

[21] Chandigarh to get robust cyber directorate: DGP at https://www.hindustantimes.com/cities/chandigarh-news/chandigarh-to-get-robust-cyber-directorate-dgp-101647200009351.html

[22] India is assembling an ace team of cyber sleuths to protect its power grids at https://www.livemint.com/industry/energy/india-plans-specialized-cyber-unit-to-protect-its-power-grid-11647452534052.html

[23]India, Indonesia hold second security dialogue, vow to combat terror at https://www.hindustantimes.com/world-news/india-indonesia-hold-second-security-dialogue-vow-to-combat-terror-101647526214000.html

[24] 660 technologies developed under cyber scheme against target of 6,824: Govt at https://www.business-standard.com/article/economy-policy/660-technologies-developed-under-cyber-scheme-against-target-of-6-824-govt-122031601257_1.html

[25] First session of the Ad Hoc Committee at https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html