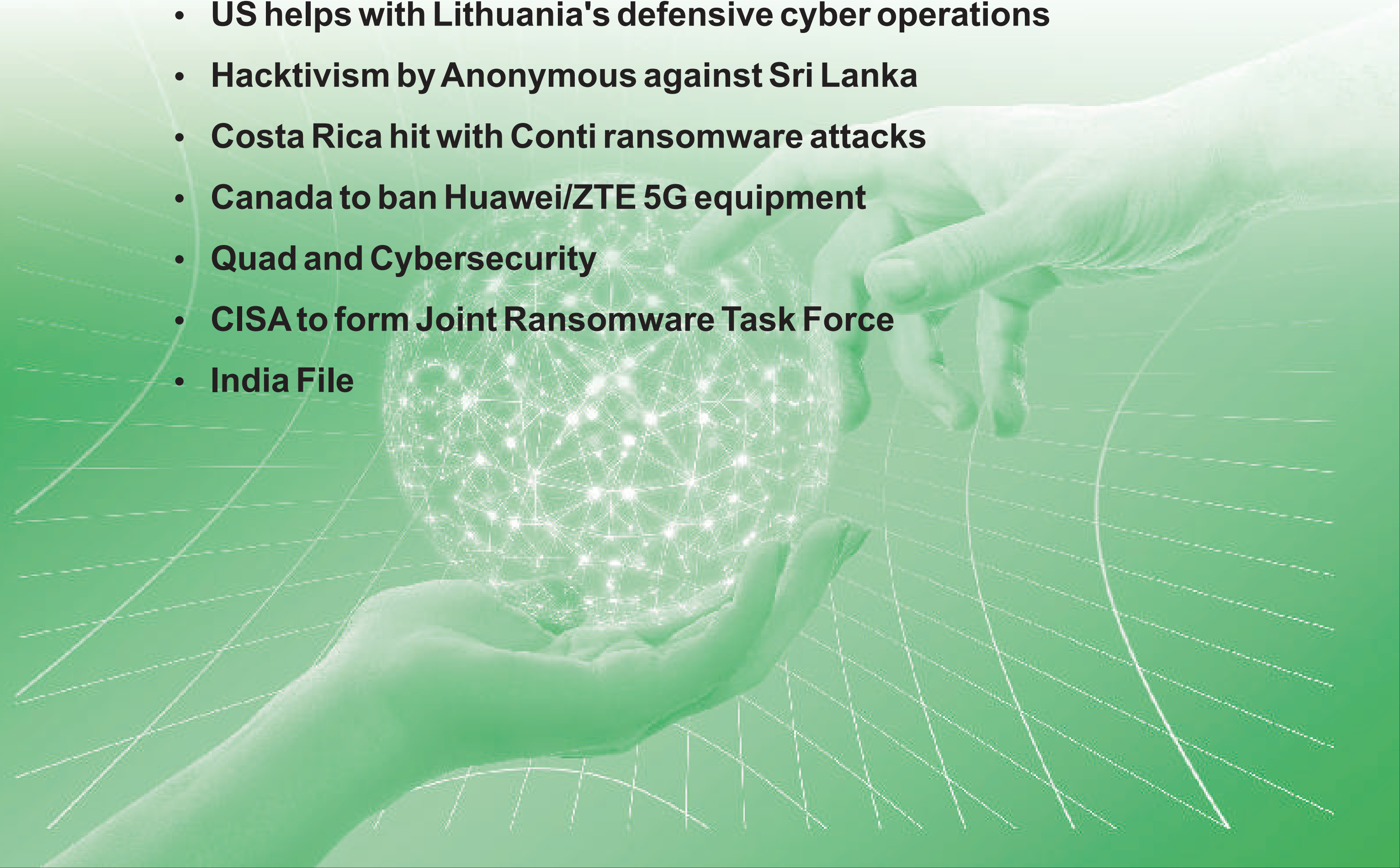
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER
Digest

June 2022



- South Korea joins NATO's Cyber Defense Unit
- UNDP and Bangladesh to launch a Cyber Security Campaign
- UK to reform spy laws to combat cybercrimes
- US helps with Lithuania's defensive cyber operations
- Hacktivism by Anonymous against Sri Lanka
- Costa Rica hit with Conti ransomware attacks
- Canada to ban Huawei/ZTE 5G equipment
- Quad and Cybersecurity
- CISA to form Joint Ransomware Task Force
- India File

South Korea joins NATO's Cyber Defense Unit

The National Intelligence Service (NIS) of South Korea has been accepted as a contributing participant for the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the first in Asia. South Korea's admission to the group comes against the backdrop of Russia's invasion of Ukraine, indicating a hardening of commitment among US allies in reaction to Russian and Chinese threats. However, it is unclear whether the events in Ukraine influenced NATO's decision to approve South Korea's membership. The NIS applied to join the organisation in 2019 and has since taken part in two Locked Shields exercises, the world's largest international live-fire cyberdefense exercise. The CCDCOE now includes 27 NATO member countries as well as five non-NATO contributing participants, the others being Austria, Finland, Sweden, and Switzerland.

UNDP and Bangladesh to launch a Cyber Security Campaign

The UN Development Programme (UNDP) and the government of Bangladesh's ICT Division have signed an agreement to launch a Cyber Security campaign for youth and children in select Least Developed Countries (LDC) countries. The ICT Division will provide USD 5 million to implement the Cyber Security campaign over 5 years. Money was raised from the 'Golden Jubilee Bangladesh Concert' that took place on May 6 at the Madison Square Garden in New York. Under this partnership UNDP-Bangladesh Bangabandhu Sheikh Mujibur Rahman International Award on Cyber Security Awareness would be presented to encourage and inspire the youth to combat cyber security challenges.

UK to reform spy laws to combat cyberattacks

According to the UK's Home Secretary Priti Patel, the country's spy laws will be overhauled in the wake of risks to national security ranging from cyber-attacks to 'nefarious' lobbying. The reforms would include the creation of a new Foreign Influence Registration Scheme, similar to ones in the United States and Australia, to reduce the risk of foreign governments damaging Britain's interests. The new legislation would make it illegal to be an undeclared foreign spy, create a new foreign interference offence, and broaden the response to drone and cyberattacks on critical infrastructure and other targets. It will also allow courts to impose longer sentences for crimes committed with the support of a foreign state, according to the interior ministry. People convicted of terror offences would also be denied access to civil legal aid under the proposed reforms.

US helps with Lithuania's defensive cyber operations

The US Cyber Command's Cyber National Mission Force (CNMF) deployed a hunt forward team to undertake defensive cyber operations alongside partner cyber forces at the invitation of the Lithuanian government. Along with its allies, the US cyber operators searched for harmful cyber activity on important Lithuanian national defence systems and Ministry of Foreign Affairs networks. This was the first shared defensive cyber operation between Lithuanian cyber forces and CNMF in that country.

Hacktivism by Anonymous against Sri Lanka

Anonymous employed distributed denial-of-service (DDoS) attacks on the websites of the Ceylon Electricity Board, the Sri Lanka Police, and the Department of Immigration and Emigration on April 20. Anonymous claimed to have established the #OpSriLanka hashtag in favour of the people and was "declaring cyberwar against the government" on Twitter. Many Sri Lankans had been calling for the group to step in, using the hashtag #AnonymousSaveSriLanka on social media. But as part of the attack, Anonymous hackers publicly shared thousands of usernames, passwords, and email addresses from the database of Sri Lanka Scholar, a private portal that connects students to various higher education institutions and uses the official ".lk" domain. This has raised questions amongst both cybersecurity professionals and the broader public, as to whether Anonymous is doing more harm than good while showing its support for the anti-government protests.

Costa Rica hit with Conti ransomware attacks

The newly elected President of Costa Rica, Chaves, proclaimed a national emergency on May 8th, citing ongoing Conti ransomware attacks as the reason. Conti ransomware had originally claimed the ransomware attack against Costa Rican government entities in April. Conti made public the majority of the 672 GB dump, which appears to contain information from Costa Rican government agencies. Conti's leak site presently lists Costa Rican Finance Ministry (Ministerio de Hacienda), Ministry of Labor and Social Security (MTSS), Social Development and Family Allowances Fund (FODESAF), Interuniversity Headquarters of Alajuela (SIUA) as government organisations that Conti attacked.

Canada to ban Huawei/ZTE 5G equipment

To defend national security, Canada plans to prohibit the use of Huawei Technologies Co Ltd (HWT.UL) and ZTE Corp (000063.SZ) 5G equipment, joining the rest of the so-called Five Eyes intelligence-sharing network. Companies will be required to remove their 5G gear by June, 2024, and would not be reimbursed. Companies using Huawei 4G equipment must have them removed by the end of 2027. In September 2018, Canada first announced it would review the possible threats to national security in adopting Huawei equipment. In addition to the ban, Public Safety Minister Marco Mendicino said Canada would draft new legislation to protect critical financial, telecommunications, energy and transport infrastructure from cyber threats.

Quad and Cybersecurity

US President Biden, Australian Prime Minister Anthony Albanese, Indian Prime Minister Narendra Modi, and Japanese Prime Minister Yoshihide Kishida advanced the Quad's ambitious and diverse agenda in Tokyo, including a substantial new initiative to boost marine domain awareness across the Indo-Pacific. The leaders met for the fourth and second time in person on May 24, 2022 in Tokyo. In terms of cybersecurity, the Quad Cybersecurity Partnership seeks to build resilience across the four countries in response to cybersecurity vulnerabilities and cyber threats. Its areas of focus are critical-infrastructure protection, led by Australia; supply-chain resilience and security, led by

India; workforce development and talent, led by Japan; and software security standards, led by the United States. Its work is guided by new joint cyber principles to improve cyber resilience in a rapidly changing threat environment.

Furthermore, the Quad will strengthen information-sharing among Quad country Computer Emergency Response Teams (CERTs), including exchanges on lessons learned and best practices. The Quad will also improve software and Managed Service Provider (MSP) security by coordinating cybersecurity standards for Quad governments' procurement of software. Finally, Quad partners will launch a Cybersecurity Day campaign, open to countries across the Indo-Pacific and beyond, as part of continuing efforts to strengthen cybersecurity awareness and action.

CISA to form Joint Ransomware Task Force

The US Cybersecurity and Infrastructure Security Agency (CISA), announced the formation of a joint ransomware task force, as provided for in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA, which was passed as part of the omnibus spending bill in March, focuses on critical infrastructure organisations, such as financial services firms and energy companies, as well as other entities where a cybersecurity event would have an economic or public health and safety impact. CIRCIA would require these organisations to notify the federal government within 72 and 24 hours, respectively, of any significant cybersecurity incidents or ransom payments.

India File

- **Cyberattacks on Indian companies**

Two Indian companies faced major cyberattacks in the month of May. According to a police complaint filed by the payment gateway company, Razorpay, hackers and fraudulent clients stole 7.3 crore by interfering with and manipulating the authorisation process of Razorpay Software to authenticate 831 unsuccessful transactions. Additionally, hundreds of passengers were stuck at airports and on planes following a recent attempted ransomware attack on SpiceJet, a domestic airline. After aeroplane departures slowed, aviation operations were disrupted for almost four hours.

- **Rs 515 cr allocated for cyber programs by GOI**

MoS for Electronics and Information Technology (MEITY) Rajeev Chandrasekhar noted at a news conference that the government of India has spent Rs 809.58 crore during 2019-20 to 2021-22 for online safety, online trust and online accountability programs. Also, an amount of Rs 515 crore has been allocated for cybersecurity programs for the year 2022-23.

- **India proposes panel on misuse of emerging tech at UNSC**

India has proposed holding a meeting of the Security Council's Counter-Terrorism Committee (CTC) in India to discuss measures to combat the threat of terrorists exploiting emerging digital technologies such as cryptocurrencies and NFTs, as well as 3D printing and artificial intelligence.

- **India attends ARF meetings on ICT**

9th ARF Open Ended Study Group (OESG) on Confidence Building Measures to reduce the risk of conflict stemming from the use of ICTs was held on 10.5.2022 and 4th ARF Inter Sessional Meeting on Security of and in the use of ICTs was held on 13.5.2022 on virtual mode. India actively participated in both the meetings.

- **8th BRICS Working Group Meet on ICT Security**

The Eighth Meeting of the BRICS Working Group on Security in the Use of Information and Communication Technologies (ICTs) was held on 24th May 2022 in virtual mode under the Chairmanship of China. Senior Officials from relevant Ministries, Departments and agencies from BRICS countries participated in the Meeting.

- **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 is being held in Vienna from 30th May 2022 to 10 June 2022 on Hybrid mode. Smt. Muanpuii Saiawi, Joint Secretary (CD) is leading the Indian delegation to Vienna for representing India in the Meeting.