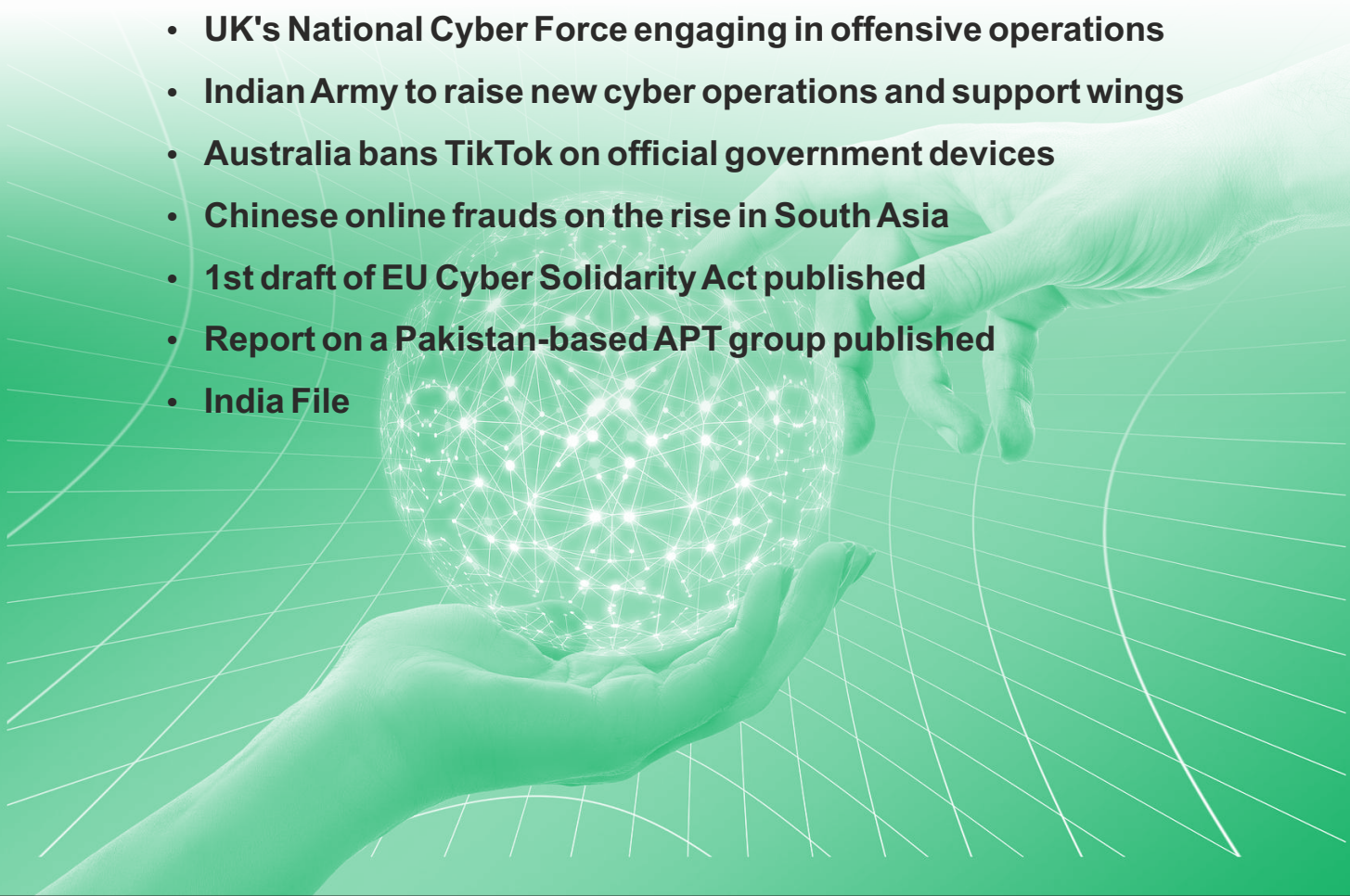
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

May 2023

- KillNet targeting health infrastructure in the US
- Pro-Russian hackers target European air-traffic control
- Software manufacturers urged to release secure products
- UK's National Cyber Force engaging in offensive operations
- Indian Army to raise new cyber operations and support wings
- Australia bans TikTok on official government devices
- Chinese online frauds on the rise in South Asia
- 1st draft of EU Cyber Solidarity Act published
- Report on a Pakistan-based APT group published
- India File



KillNet targeting infrastructure in the US and elsewhere

The US Department of Health and Human Services has published a report on KillNet, a pro-Kremlin hacktivist group which details KillNet's targeting of the Health and Public Health Sector from December 2022-March 2023.[1] The report elaborates on how the group uses its signature distributed denial-of-service (DDoS) attacks on critical infrastructure sectors, causing service outages lasting several hours to days. Since January 2022, KillNet has been known for conducting DDoS campaigns against multiple critical infrastructure sectors in countries supporting Ukraine in the ongoing conflict. In March 2023, Microsoft Security also reported on the waves of attacks by KillNet against Western countries targeting governments and companies focusing on the healthcare sector.[2]

Killnet affiliate Anonymous Sudan also conducted attacks around the world, including India and Israel. It conducted a series of DDoS attacks against Israeli targets such as government sites and universities.[3] The group also claimed responsibility for other online assaults, including the Haifa Port website and that of the Israel Ports Development & Assets Company that manages Israel's ports. The attacks coincided with the marking of Quds Day, an Iran-promoted event featuring anti-Israel marches in Tehran. According to some speculations, 'Anonymous Sudan may be linked to Russia's KillNet hacking group rather than Sudan.

In India, six major Indian airports including Delhi, Mumbai, Hyderabad, Goa and Kochi, were subject to DDoS attack by Anonymous Sudan, which rendered their websites inaccesible for varying periods of time on April 8. [4]

Pro-Russian hackers target European air-traffic control

Europe's air-traffic control agency Eurocontrol confirmed that pro-Russian hackers attacked and caused interruptions in service of its communications systems and its website.[5] Eurocontrol coordinates commercial traffic between 41 states, including the EU, and their national air-traffic control entities. The outage reportedly jammed the agency's communication systems forcing airlines to use older technology to manage flight schedules. However, the spokesperson for the Eurocontrol declined to comment on the effected systems while acknowledging attack on its website.

Software manufacturers urged to release secure products

An international coalition of government cybersecurity organisations published a joint statement and guidance asking software vendors to release future products that are secure by design and secure by default.[6] The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Australia, Canada, the United Kingdom, Germany, the Netherlands, and New Zealand in the report titled "Shifting the Balance of Cybersecurity Risks: Principles and Approaches for Security-by-Design and -Default" urged software manufacturers to take urgent steps to address the issue. The guidance includes specific technical

recommendations and core principles to guide software manufacturers in building software security into their design processes before developing, configuring, and shipping their products. Previously, CISA's Director Jen Easterly had flagged issues related to unsafe software and absence of liability on vendors as she stressed on the utility of secure by design to address vulnerabilities in technology products.[7]

UK's National Cyber Force engaging in offensive operations

The UK government has formally confirmed that its National Cyber Force (NCF) agency is active and has conducted several offensive operations.[8] Britain's newly created offensive hacking unit said that it is engaged in operations to disrupt terrorist groups, distributors of child sexual abuse material, and opponents of the UK. An official paper, *Responsible Cyber Power in Practice*, also the body's first policy statement, describes its response to growing organized online threats. Formally established in 2020, the NCF is a joint operation between GCHQ, the UK's main intelligence agency, and the Ministry of Defence.[9]

The UK government also announced the launch of a new program GovAssure, that introduces several changes in how the government protects itself from cyber threats.[10] Through this new program, the government security teams will carry out annual security audits of government departments and key public services. Third parties will also assess departments to increase standardization and validate results and help government organizations identify best practices.

Indian Army to raise new cyber operations and support wings

The Indian army has decided to raise Command Cyber Operations and Support Wings (CCOSW) to help the forces counter enemy capabilities, with cyber warfare as a critical focus. Army commanders decided during their annual conference held from 17-21 April.[11] The conference participants acknowledged cyberspace's growing significance in the military domain in grey zone warfare and conventional operations. Within the Ministry of Defence, the recently operationalized Defence Cyber Agency (DCA) acts a principal agency for all cybersecurity related issues for the three services.

Australia joins countries banning TikTok on official government devices

The Australian government has banned the use of the TikTok app on official government devices.[12] With the recent ban, all Five Eyes Intelligence sharing alliance members have formally banned the app on government devices. The ban means that government employees who have installed the app on their government-owned phones must delete it as soon as possible. The direction from the government states that TikTok poses significant security and privacy risks arising from "extensive collection of user data and exposure to extrajudicial directions from a foreign government that conflicts with Australian law.

Chinese online frauds on the rise in South Asia

Sri Lankan authorities have detained 39 Chinese nationals on charges of hacking

and stealing money from the bank accounts of people living in different countries.[13] According to the police, the group had been staying in a tourist resort and was arrested based on complaints from several embassies. The arrest in Sri Lanka was the second incident within a week of Chinese nationals being arrested from another country for online fraud. Earlier in March, Nepal police arrested 9 Chinese nationals on online fraud charges for swindling Rs 100 million from Nepali people.[14] In October 2022, a number of Chinese nationals were arrested in Andhra Pradesh[15] and Uttar Pradesh for carrying out online fraud activities.[16] The *Dawn* newspaper reported in November 2022 that nine bank accounts of Chinese firms and individuals had been frozen in Pakistan for similar activities.[17]

1st draft of EU Cyber Solidarity Act published

The European Commission has published the first draft of its EU Cyber Solidarity Act, a legislative effort to improve cybersecurity across the EU member states that will enable a common incident response.[18] The underlying reason behind the law is to improve the preparedness, detection, and response to cybersecurity incidents across the EU. According to the European Commission, implementation of the EU Cyber Solidarity Act would cost €1.1 billion, of which two-thirds will be provided from the EU's budget. At the same time, the rest will come from member states.

Report on a Pakistan-based APT group published

Team Cymru has published a report uncovering new infrastructure operated by SideCopy, a Pakistan-based APT group.[19] SideCopy has been active since 2019, primarily targeting South Asian countries, with a focus on India and Afghanistan. The report also provides specific evidence to demonstrate that the Action Rat infrastructure connected to SideCopy is managed by users accessing the internet from Pakistan.

India File

- The Insurance Regulatory and Development Authority of India (IRDAI) has issued new guidelines on information and cybersecurity for insurers to boost their defenses and other institutional arrangements.[20] The guidelines are expected to enable the industry to strengthen its defenses and improve its governance mechanisms to deal with emerging cyber threats. The initial guidelines covering information and cybersecurity practices for insurers were issued in 2017. They aimed to ensure that insurers are adequately prepared to manage any cyber threat to their systems.
- The Fifth Session of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of ICTs for Criminal Purposes was held in Vienna from 11-21 April 2023 in hybrid mode. Muanpuii Saiawi, Joint Secretary (CD) led the Indian delegation to Vienna. During the Session, provisions on international cooperation, technical assistance, preventive measures, mechanism of implementation, final provisions and preamble were discussed.
- The Indian government has updated its 2021 IT rules to add a clause requiring

online platforms such as Meta and Twitter to take down government related mis-information that an Indian government body has fact-checked.[21] The Ministry of Electronics and IT notified amendments to the Information Technology Rules, 2021, which allows the ministry to appoint a fact-checking body to decide whether online information related to the central government is accurate.

- MEA participated in the second meeting of the Working Group on Ransomware Cooperation and Diplomacy and Working Group on Ransomware Awareness and Capacity Building and National Counter Ransomware Task Force (NCRTF) established by Ministry of Home Affairs on 24th April 2023.
- The ICICI bank leaked millions of records with sensitive data, including financial information and personal documents of the bank's clients, due to the misconfiguration of their systems.[22] However, in its 4-point statement, ICICI has categorically denied the data breach incident.[23] The bank advised its customers to ignore reports of the breach and assured them of data security. The bank also warned that it will take "legal action against any entity spreading false news about data breaches or trying to damage its reputation."
- "11th ASEAN Regional Forum (ARF) Open-Ended Study Group (OESG) on Confidence Building Measures (CBM) to reduce the risk of conflict stemming from ICTs" and "5th Inter-sessional meeting on security of and in the use of ICTs" were held in Moscow, Russia during 27-28 April 2023 in hybrid mode. Shri Ravi Shanker Goel, Director (CD) represented India in these meetings in Moscow, Russia.

---

[1] US Department of Health and Human Services, Health Sector Cybersecurity Coordination Center- Analyst Note, 5 April 2023, https://www.hhs.gov/sites/default/files/202304051200-killnet-analyst-note-tlpwhite.pdf

[2] Microsoft Security, KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks, 17 March 2023,https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/

[3] The Times of Israel, Websites of Israeli port hacked; Sudanese group said to claim responsibility, 26 April 2023, https://www.timesofisrael.com/websites-of-israeli-port-hacked-sudanese-group-said-to-claim-responsibility/

[4] The Hindu, CIAL website comes under attack, 8 April 2023, https://www.thehindu.com/news/cities/Kochi/cial-website-comes-under-attack/article66714841.ece

[5] The Register, European air traffic control confirms website 'under attack' by pro-Russia hackers, 22 April 2023, https://www.theregister.com/2023/04/22/eurocontrol_russia_attack/

[6] Cybersecurity & Infrastructure Security Agency (CISA), U.S. and International Partners Publish Secure-by-Design and -Default Principles and Approaches, 13 April 2023, https://www.cisa.gov/news-events/news/us-and-international-partners-publish-secure-design-and-default-principles-and-approaches

[7] The Register, US cybersecurity chief: Software makers shouldn't lawyer their way out of security responsibilities, 28 February 2023, https://www.theregister.com/2023/02/28/cisa_easterly_secure_software/

[8] The Guardian, UK's offensive hacking unit takes on military opponents and terrorist groups, 3 April 2023, https://www.theguardian.com/technology/2023/apr/03/uks-offensive-hacking-unit-takes-on-military-opponents-and-terrorist-groups

[9] The Guardian, UK unveils National Cyber Force of hackers to target foes digitally, 19 November 2020, https://www.theguardian.com/technology/2020/nov/19/uk-unveils-national-cyber-force-of-hackers-to-target-foes-digitally

[10] UK Government, Government launches new cyber security measures to tackle ever growing threats, 20 April 2023, https://www.gov.uk/government/news/government-launches-new-cyber-security-measures-to-tackle-ever-growing-threats--2

[11] The Print, With eye on China & Pakistan, Army to raise new cyber operations and support wings, 27 April 2023, https://theprint.in/defence/with-eye-on-china-pakistan-army-to-raise-new-cyber-operations-and-support-wings/1542112/

[12] The Guardian, What does TikTok's ban from Australian government devices mean for its future?, 4 April 2023, https://www.theguardian.com/technology/2023/apr/04/what-does-tiktoks-ban-on-australian-government-devices-mean-for-its-future,

[13] Daily Mirror, Concern sparks over online frauds involving Chinese in Sri Lanka, 5 April 2023, https://www.dailymirror.lk/international/Concern-sparks-over-online-frauds-involving-Chinese-in-Sri-Lanka/107-257184.

[14] The Himalayan, Nine Chinese online racketeers arrested on fraud charges, 30 March 2023, https://thehimalayantimes.com/nepal/nine-chinese-online-racketeers-arrested-on-fraud-charges

[15] Times of India, Hyderabad: Chinese nationals among 10 held for cyber fraud, 12 October 2022, https://timesofindia.indiatimes.com/city/hyderabad/hyderabad-chinese-nationals-among-10-held-for-cyber-fraud/articleshow/94797431.cms

[16] Hindustan Times, GB Nagar police arrest two Chinese nationals for online fraud, 18 October 2022, https://www.hindustantimes.com/cities/noida-news/gbnagar-police-arrest-two-chinese-nationals-for-online-fraud-101666032445759.html

[17] Dawn, Nine bank accounts of Chinese firms, individuals frozen for 'fraud', 10 November 2022, https://www.dawn.com/news/1720071

[18] European Commission, Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience, 18 April 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243

[19] Team Cymru, Identifying Connected Infrastructure and Management Activities, 20 April 2023, https://www.team-cymru.com/post/allakore-d-the-sidecopy-train

[20] Outlook, IRDAI Issues Information & Cybersecurity Guidelines For Insurers: All You Need To Know, 25 April 2023, https://www.outlookindia.com/business/irdai-issues-information-cybersecurity-guidelines-for-insurers-all-you-need-to-know-news-281201

[21] The Indian Express, Govt-appointed fact-check body: What it will do, concerns around it, 7 April 2023, https://indianexpress.com/article/explained/govt-appointed-fact-check-body-what-it-will-do-concerns-around-it-8543723/

[22] Cybernews, Multinational bank leaks passports and credit card numbers, 24 April 2023, https://cybernews.com/security/icici-bank-leaked-passports-credit-card-numbers/

[23] Economic Times, ICICI Bank refutes data breach allegation; here's what we know so far, 22 April 2023, https://ciso.economictimes.indiatimes.com/news/data-breaches/icici-bank-refutes-data-breach-allegation-heres-what-we-know-so-far/99674205