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

CYBER Digest

January 2024

- GPAI Ministerial Declaration 2023
- US, India, and Taiwan hold workshop on cybersecurity
- Brazil sets up cybersecurity policy
- Cyber attacks escalate around Israel-Hamas conflict
- Information security cooperation between Iran and Russia
- Cyber attack targets Ukrainian mobile operator
- India File

GPAI Ministerial Declaration 2023

This year's session of the Global Partnership on Artificial Intelligence (GPAI) took place in New Delhi, India. During this meeting, a ministerial declaration was issued, outlining key principles to guide the development of AI.[1] The declaration endorsed the trustworthy and responsible use of AI, reiterating its commitment to a range of broader principles. These principles encompass democratic values and human rights, the safeguarding of dignity and well-being, ensuring the protection of personal data, upholding applicable intellectual property rights, and maintaining privacy and security. Furthermore, the declaration highlights the importance of fostering innovation and advocates for the promotion of AI that is trustworthy, responsible, sustainable, and centred around human needs and values.

The declaration also reaffirmed its support for efforts to foster collaborative AI through global partnerships among GPAI members. This support is aimed at facilitating equitable access to essential resources for AI research and innovation. These resources include AI computing, high-quality and diverse datasets, algorithms, software, testbeds, and other AI-relevant resources. The declaration also acknowledged the significance of leveraging AI innovation in the realm of sustainable agriculture, identifying it as a new thematic priority for the GPAI.

US, India, and Taiwan hold workshop on cybersecurity

A joint workshop was held under the auspices of the Global Cooperation and Training Framework (GCTF), where representatives from the United States, India, and Taiwan convened.[2] The primary focus of this meeting was to deepen operational expertise and exchange shared best practices regarding cybersecurity issues. U.S. Ambassador to India Eric Garcetti, Taiwan's Representative to India Baushuan Ger, former National Cyber Security Coordinator of India Lt. Gen Rajesh Pant, and the United Service Institution of India co-hosted an event under the Global Cooperation and Training Framework (GCTF). This event marked the first in-person GCTF program to be held in India.

Since its inception in 2015, the Global Cooperation and Training Framework (GCTF) has conducted 70 international workshops, with participation from experts in over 120 countries. These workshops have been instrumental in strengthening connections among experts on a variety of topics, including public health, supply chains, humanitarian assistance, digital health, and other regional issues.

Brazil sets up cybersecurity policy

Brazilian President Luiz Inacio Lula da Silva has enacted Decree 11.856/2023, which establishes the National Cybersecurity Policy (PNCiber).[3] This initiative was proposed by the Office of Institutional Security (GSI). The decree additionally sets up the National Cybersecurity Committee, which is scheduled to meet quarterly. This committee will comprise representatives from various sectors, including government, civil society, academic institutions, and business organizations. Its primary responsibility will be to propose updates to the cybersecurity program. The committee will have the responsibility of developing a National Cyber Security

Strategy and a National Cyber Security Plan. They are also tasked with proposing strategies for engagement that aim to promote international technical cooperation in the field of cybersecurity.

Cyber attacks escalate around Israel-Hamas conflict

Resembling other contemporary conflicts, the Israel-Hamas confrontation has also escalated beyond the physical realm to cyberspace. The conflict has also seen the involvement of Iranian threat actors or hacktivists. Recent trends in cyber warfare indicate a change in the tactics of Iranian hacktivist proxies. While initially focusing on Israel, these groups have expanded their cyber operations to target other nations, especially focusing on the United States.[4] These hacktivist proxies, by strategically targeting U.S. entities that use Israeli technology allows them to simultaneously claim attacks on both Israel and the U.S.

In another major escalation in the cyber domain, the Israel-aligned hacktivist group known as Gonjeshke Darande also referred to as Predatory Sparrow, has reportedly claimed responsibility for a cyberattack on Iran's gas stations.[5] This attack has led to the disruption of approximately 70% of these stations, as per the reports. The cyberattack significantly disrupted Iran's fuel distribution system. It disabled smart cards used for accessing subsidized fuel, resulting in malfunctions across a wide range of gas stations. Consequently, some stations were forced to sell gasoline at non-subsidized prices. A similar attack had taken place in 2021, which Iran had accused Israel and the United States of orchestrating, Predatory Sparrow had claimed responsibility for that attack as well.[6]

Information security cooperation between Iran and Russia

Iran's parliament has approved a bill to enhance collaboration with Russia in the field of information security.[7] This development comes as both countries face accusations of conducting extensive cyber attacks. The bill, which enacts an agreement signed three years earlier has received approval from Iranian parliamentarians. The bill, containing nine articles, centres on addressing cyber threats, strengthening information security measures, and promoting cooperation between Iran and Russia. A significant aspect of this legislation includes a provision for the exchange of information and collaboration in prosecuting criminal offenses between the two countries.

In recent years, Tehran and Moscow have notably enhanced their ties in various domains, including political, military, communication, and cyber sectors. This strengthening of relations has raised concerns among Western countries and their allies.

Cyber attack targets Ukrainian mobile operator

Ukraine's largest mobile operator, Kyivstar, was hit by a significant cyber attack, which was the largest of its kind since the onset of the Ukrainian war. The cyber attack on Kyivstar, a mobile operator serving more than half of Ukraine's population, resulted in a service outage and damage to its IT infrastructure. This disruption put millions at risk by hindering their ability to receive warnings about potential Russian air assaults. Furthermore, the attack also disrupted the air raid alert systems in parts of Kyiv. Banking systems were also affected.

The Russian hacktivist group Killnet claimed responsibility for the attack on Kyivstar through a statement on the Telegram messaging app. However, they did not provide any evidence to support their claim. Kyivstar, boasting a substantial customer base, has 24.3 million mobile subscribers, along with over 1.1 million home internet subscribers.

Ukraine's cyber chief said that their investigation of the attack showed that Russian hackers had been inside Kviystar's systems for over 8 months. The attack wiped "almost everything", including thousands of virtual servers and PCs, he said, describing it as probably the first example of a destructive cyberattack that "completely destroyed the core of a telecoms operator."[8] In an apparent response to the strike, the Ukarainian military intelligence service posted on Telegram that Russia's Federal Tax service had been paralysed through a cyber attack.

India File

- Following a series of cyberattacks, a senior government official announced that the Centre has established a secure e-mail system for 10,000 users in critical ministries and departments.[9] This e-mail system, which operates on Zero Trust Authentication (ZTA), has been developed by the National Informatics Centre (NIC). The 10,000 email accounts are distributed across seventeen union ministries and departments.

- The Central Electricity Authority (CEA) of the Ministry of Power, Government of India, in collaboration with REC Limited and the Expert Group on Smart Metering (EGSM), organized a workshop focused on Cyber Security for Distribution Utilities in the Power Sector.[10] The workshop convened a diverse group of renowned experts, industry leaders, and cybersecurity enthusiasts. They gathered to engage in discussions about the latest trends, innovations, and strategies in the field of cybersecurity.

- A threat actor has reportedly claimed to possess "critical information" related to the users of Bharat Sanchar Nigam Ltd (BSNL), the state-owned telecom operator in India, suggesting a potential data breach at the company.[11] The data breach allegedly involves a range of sensitive information. This includes email addresses, billing details, contact numbers, and other critical data. Furthermore, the compromised data encompasses details about mobile outage records, network specifics, completed orders, and comprehensive customer information.

- The Sixth Substantive Session of the UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies (ICTs) 2021-2025 was held at UN Headquarters New York from 11-15 December 2023. Indian delegation attended the Session. During the Session, India made a detailed presentation on the Global Cyber Security Cooperation Portal (GCSCP). The presentation incorporated technical and design details for the proposed portal and also demonstrated how it was more comprehensive as compared to other existing information-sharing platforms.

[1] GPAI, 2023 Ministerial Declaration, https://gpai.ai/2023-GPAI-Ministerial-Declaration.pdf

[2] U.S. Embassy & Consulates in India, Representatives from the United States, India, and Taiwan collaborate on cybersecurity under the global cooperation and training framework, 11 December 2023, https://in.usembassy.gov/representatives-from-the-united-states-india-and-taiwan-collaborate-on-cybersecurity-under-the-global-cooperation-and-training-framework

[3] TV Brics, Lula da Silva signs a decree to develop a national cybersecurity policy, 28 December 2023,

Text copied from https://tvbrics.com/en/news/lula-da-silva-signs-a-decree-to-develop-a-national-cybersecurity-policy/

[4] Check Point, Check Point Research Report: Iranian Hacktivist Proxies Escalate Activities Beyond Israel, 4 December 2023, https://blog.checkpoint.com/research/check-point-research-report-shift-in-cyber-warfare-tactics-iranian-hacktivist-proxies-extend-activities-beyond-israel/

[5] CSO Online, Pro-Israel hacktivist group brings down 70% of gas stations in Iran, 19 December 2023, https://www.csoonline.com/article/1266704/pro-israel-hacktivist-group-brings-down-70-of-gas-stations-in-iran.html

[6] BBC, Iran blames foreign country for cyberattack on

petrol stations, 27 October 2021, https://www.bbc.com/news/worldmiddle-east-59062907

[7] Iran International, Iranian Parliament Approves Information Security Deal with Russia, 10 December 2023, https://www.iranintl.com/en/202312105187

[8] Reuters, Exclusive: Russian hackers were inside Ukraine telecoms giant for months, 5 January 2024, https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

[9] The Hindu, Centre sets up secure e-mail for 10,000 users in critical ministries, 17 December 2023, https://www.thehindu.com/news/national/centre-sets-up-secure-e-mail-for-10000-users-in-critical-ministries/article67648444.ece

[10] Press Information Bureau (PIB), Workshop on Cyber Security for Distribution Utilities in Power Sector organized by Central Electricity Authority, 15 December 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1986848

[11] The Economic Times, BSNL suffers data breach; sensitive info of users up for sale on dark web, 22 December 2023, https://telecom.economictimes.indiatimes.com/news/industry/bsnl-suffers-data-breach-sensitive-info-of-users-up-for-sale-on-dark-web/106197459