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

CYBER *Digest*

November 2022

- Update on Russia-Ukraine Cyber Conflict
- Chinese cyber offensive activities around the globe
- Cyber updates from the United States
- Lebanon-based hacking group attack Israeli networks
- Turkey passes law criminalising spread of 'disinformation'
- Tata Power hit by cyberattack
- Iran's Nuclear Agency alleges email server hacking
- S. Korea participates in US-led cyber exercise
- India File

Update on Russia-Ukraine Cyber Conflict

The Russia-Ukraine cyber conflict has shown two important lessons: the first is that Russian forces' performance has not met expectations, and the second is the expected avalanche of cyberattacks on par with the kinetic attacks never materialised. Following are major activities in the month of November:

- DNS (Digital Network System), Russia's second-largest retail chain, disclosed a data breach that exposed the personal information of customers and employees. The National Republican Army (NRA), an activist group of dissidents seeking to depose Putin, has been accused of carrying out this attack.
- Since December 2021, the US military Cyber Command team has been in Ukraine protecting its digital networks, according to a news report. This implies a new role for the US military, whose teams are engaged in "Hunt Forward" missions, examining partner countries' computer networks for evidence of intrusion.
- In an interview, Rob Joyce, the head of the NSA's Cybersecurity Directorate, outlined six lessons learned from Russia's invasion of Ukraine: In a conflict, both espionage and destructive attacks will occur simultaneously; Cybersecurity industry insights offer a distinct perspective on these conflicts; sensitive and timely intelligence makes a significant difference; work on and develop resiliency and acquire adequately skilled personnel; don't do it alone; and one can never plan adequately for contingencies.
- According to Digital Shadows, a British cybersecurity firm, the number of ransomware assaults has decreased overall. According to their analysis, a portion of the decline is due to Russian criminal gangs being co-opted into Russia's war effort, diverting them away from their usual criminal activities.
- A flourishing online underground market for goods and services meant to help Russian males evade military service has emerged. These services include claims to alter official databases in order to keep the customer's identity out of call-up sweeps, as well as "grey" SIM cards to aid in avoiding government surveillance.
- Anonymous Russia, a group of pro-Russian hackers, attacked MI5's public website, briefly taking it offline as the Ukrainian crisis raged on. The Security Service's website displayed a "website under maintenance" page for an hour before returning to normal operation.
- Starlink services are believed to have been disrupted as Ukrainian forces marched into formerly Russian-occupied territory. There has been no public explanation for the disruptions, though there has been much conjecture. Furthermore, Starlink has stated that it is finding it difficult to bear the costs of providing resilient Internet service to Ukraine. The company has requested funding from the US Department of Defense. Concerns have also been raised about Ukraine's reliance on a single company for communication.
- Arne Schönbohm, the chief of Germany's national cybersecurity agency, has been fired following claims of suspected ties to Russian intelligence.
- According to the Lithuanian Ministry of National Defense, Poland will become the fifth country to join the Regional Cyber Defense Center

(RCDC), which works as a branch of the National Cyber Security Center. The RCDC was established in July 2021 and serves as the primary forum for actual cooperation with the United States in the field of cyber defence.

- Hybrid and cyberattacks could be grounds for triggering NATO's Article 5, the alliance's Secretary-General Jens Stoltenberg warned, amid suspicions that Moscow planted explosives on underwater gas pipelines.

Chinese cyber offensive activities around the globe

- Suspected Chinese hackers tampered with widely used software provided by a small Canadian customer service company, another example of a "supply chain compromise" similar to the attack vector used in the SolarWinds incident.
- According to PricewaterhouseCoopers, an elite Chinese hacking group with ties to operatives charged by a US grand jury in 2020 has increased its activity this year, targeting sensitive data stored by firms and government agencies in the US and dozens of other nations.
- A newly detected cyberespionage group based in China has been using signed malware to attack IT service providers and telecoms companies. The operations of this advanced persistent threat (APT), known as WIP19 overlaps with Operation Shadow Force, although it is unclear whether this is a new iteration of the campaign or the work of a distinct, more sophisticated adversary employing new malware and methodologies. WIP19 is primarily targeting companies in the Middle East and Asia, and it employs stolen certificates to illegally sign many components that can be used for harmful effects.
- According to the Symantec Threat Hunter Team, a long-running Chinese-linked cyberespionage group targeted the network of a U.S. state legislature in July, marking the group's first confirmed attack against the US government in years. Since at least 2013, the group has been known to target a wide range of companies "in support of its political and military intelligence-collection objectives."
- In recent efforts, the Chinese state-sponsored threat group Winnti has been spotted attacking governmental entities in Sri Lanka and Hong Kong. The Winnti Group, active since at least 2007, and also known as APT41, Barium, Blackfly, Double Dragon, Wicked Panda, and Wicked Spider, is thought to be made up of many subgroups engaged in both cyberespionage and financially driven operations.

Cyber updates from the United States

- The Cybersecurity and Infrastructure Security Agency is rolling out a new service to help defend a broader range of agency systems from cyberattacks. After spending the previous year beta testing the tool, CISA is now rolling out a Protective Domain Name System (DNS) service to all federal agencies. CISA is also looking to potentially expand the tool beyond federal systems.
- The US has released its National Defense Strategy. The report underlines the danger posed by four US adversaries- China, Russia, North Korea, and Iran- all of whom have significant offensive cyber capabilities. The Strategy places a strong emphasis on deterrence, specifically deterrence through resilience in relation to cyberspace, which it contends is possible through a number of steps, including the adoption of zero-trust principles and encryption. The US will

also pursue deterrence by direct and collective cost imposition, which may include offensive cyber operations.

- A partnership between the United States and the United Kingdom to combat online and digital crime came into effect, marking another international bilateral agreement authorised by the Clarifying Lawful Overseas Use of Data, or CLOUD Act. The Department of Justice agreement will allow law enforcement in both countries to use critical data to combat crime while respecting civil rights and privacy standards.

  President Biden also signed an Executive Order (E.O.) on Enhancing Safeguards for US Signals Intelligence Activities directing the steps that the US will take to implement the US commitments under the European Union-US Data Privacy Framework (EU-US DPF) announced by President Biden and European Commission President von der Leyen in March 2022.

Lebanon-based hacking group attack Israeli networks

ESET researchers revealed their findings about POLONIUM, an advanced persistent threat (APT) group. POLONIUM is an operational group based in Lebanon, coordinating its activities with other actors affiliated with Iran's Ministry of Intelligence and Security (MOIS). POLONIUM has targeted more than a dozen organizations in Israel since at least September 2021, with the group's most recent actions being observed in September 2022. Verticals targeted by this group include engineering, information technology, law, communications, branding and marketing, media, insurance, and social services.

Turkey passes law criminalising spread of 'disinformation'

President Tayyip Erdogan's proposed law, which would jail journalists and social media users for up to three years for spreading "disinformation," was approved by Turkey's parliament. Despite opposition from opposition MPs, European countries, and media rights activists, lawmakers from Erdogan's ruling AK Party (AKP) and its nationalist allies MHP voted to approve the bill.

Tata Power hit by cyberattack

Tata Power Company Limited was hit by a cyberattack on its IT infrastructure impacting some of its IT systems. The company has taken steps to retrieve and restore the systems, it informed. A senior official from the Maharashtra Police's cyber wing said an intelligence input had been received about threat to Tata Power and other electricity companies.

Iran's Nuclear Agency alleges email server hacking

According to a statement on the Atomic Energy Organization of Iran's website, a number of emails from the IT unit of a subsidiary called the Nuclear Energy Production and Development Co., which is in charge of producing nuclear energy, were published online without authorization. On Friday, a group called Black Reward claimed in a series of tweets and messages on its Telegram channel that it had hacked the AEOI as part of a campaign to support Iran's anti-government protests.

S. Korea participates in US-led cyber exercise

South Korea's military took part in a multinational cyber exercise led by the United States. The South Korean military participated in the Cyber Flag exercise with eighteen personnel. This year, 25 countries participated in the exercise, which included both seminars and cyber field training.

Since 2011, the U.S. Cyber Command has conducted the exercise annually to enhance the readiness of Washington and its allies against malicious cyber activities.

India File

- **CERT-In and Power-CSIRTs conduct Cyber Security Exercise**

  Indian Computer Emergency Response Team (CERT-In) in collaboration with Power-CSIRTs (Computer Security Incident Response Teams in Power sector), successfully designed & conducted the Cyber Security Exercise "PowerEX" for 193 invited Power Sector Utilities. The Exercise Planner Team of Power-CSIRTs' officials worked along with the CERT-In team on the exercise day as Exercise Coordinators. The objective of the exercise was to "Recognize, Analyse & Respond to Cyber Incidents in IT & OT Systems".

- **26 cyber criminals arrested under CBI's "Operation Chakra"**

  Twenty-six alleged cyber criminals have been arrested so far under 'Operation Chakra' of the CBI to dismantle cybercrime gangs operating in the country. The operation has been launched in coordination with state police, Interpol and agencies of other countries. The CBI registered 11 cases against cyber criminals involved in financial fraud using the internet. While the agency conducted searches at 87 locations, 28 places were raided by the state police.

- **India offers cyber security training to Philippines military**

  As the two countries' defence engagements deepen, the Indian military is willing to provide operational and cyber-security training to the Armed Forces of the Philippines (AFP). This offer was made by India's ambassador to the Philippines, Shambhu Kumaran, during a courtesy call on DND officer-in-charge Undersecretary Jose Faustino Jr.

- **Open RAN international delegation from USA visits MEA**

  An Open RAN International delegation from US called on JS (CD, NEST & DISA). The delegation was briefed on the developments taking place in India in the field of new and emerging strategic technologies like 5G, fintech, etc. and how it has benefited the delivery of government services to the citizens of India.

- **Draft Telecommunication Bill 2022 open for comments**

  The Department of Telecom has made available for public comment the draft Indian Telecommunication Bill, 2022, which aims to reform existing telecom laws and regulations and make them "future ready."

- **Cyber Ambassadors meet with MEA**

  Cyber Ambassadors from Germany, Switzerland and Poland held dialogues with senior officials of the MEA, including Ms. Muanpuii Saiawi, JS (CD, NEST & DISA) over the course of the month. German Cyber Ambassador Dr. Regina Grienberger discussed issues of mutual interests and followed up on the discussions that took place during the India-Germany bilateral Cyber dialogue held in April 2022 in Germany. A Swiss delegation headed by Mr. Benedikt Wechsler, Ambassador, Head of Digitalisation Division, Swiss Federal Department of Foreign Affairs visited the Ministry to hold the India-Switzerland Cyber Dialogue.Other visitors included Mr. Tadeusz Chomicki, Ambassador for Cyber and Tech Affairs, Security Policy Department, Ministry of Foreign Affairs, Poland and Dr.Cecile Aptel, Deputy Director, UNIDIR who met with Shri Ravi Shanker Goel, DS (CD).