INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"CYBERCRIME IN THE DIGITAL AGE: RISKS, THREATS, AND GLOBAL COUNTERMEASURES"

AUTHOR - KOMAL KUMARI, LLB, UTTARANCHAL UNIVERSITY

BEST CITATION - KOMAL KUMARI, "CYBERCRIME IN THE DIGITAL AGE: RISKS, THREATS, AND GLOBAL COUNTERMEASURES", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (1) OF 2026, PG. 361-369, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/KSAU4282

ABSTRACT

The major purpose of the research paper is to convey knowledge about the cyber risks that countries around the world face. In Today's world, practically every device is connected to the internet and is at risk of being hacked. Every country is connected via the internet. Today, there is a slew of new criminal activities taking place on the internet which becomes a threat to national security. Cybercriminals commit cybercrime regardless of where they are located. Currently, Cybercrime is typically used to obtain sensitive information or to commit financial crimes. Numerous cyber activities aid in the battle against cybercrime. There are various international collaborations between countries to combat cybercrime, including seminars, collaborative workshops, and other activities. These factors help in the development of a nation's cyber-security team and provide their respective countries with a more secure cyber area.

Keywords: National security, cyberspace threats, vulnerability assessments, cyberspace security, cyber security policy.

INTRODUCTION

[960] Cyber security involves technology, methods, and policies to protect systems, networks, and data from cyberattacks and unauthorized access. Cyberspace is the interconnected space between networks of computer systems. William Gibson coined the word "cyberspace" in one of his short tales, "Burning Chrome." The threat to cyberspace has increased, necessitating government actions to defend it. With the internet's ability to connect people from all over the world, businesses and private users have increased their operations, and the internet has grown in popularity. Because everyone regularly uses the internet, it has also produced a social environment that has become a part of our daily life. Various governmental and non-governmental organizations use cyberspace to promote their countries. Then there are terrorist organizations who utilize the internet to recruit these terrorist organizations who use cyberspace to assault their target organizations and train their members, in a country where they are attempting to disable their intelligence services.

It was anticipated that by the early 1990s, a large number of countries would be using cyberspace, and that if war broke out in the twenty-first century, cyberwar would also break out. Twenty years into the twenty-first century, the threat of cyberwar has grown. There are a lot of people, services, and criminals that utilize the internet to annihilate their targets. Saving the country's security is what national security entails. Certain interests must be protected at any cost. For most of the country, it's integrity and national interests will be paramount institutions of fundamental governance. Numerous small- or large-scale threats could

[960] Log point, Cyber security: definition, importance and benefits of cyber security (December. 09, 2020), https://www.logpoint.com/en/blog/what-is-cyber-security/.

put a nation in danger. Nowadays, everything is connected to the internet, putting everyone at danger of hacking, which might be quite problematic for both individuals and small and large enterprises. Many countries now lack adequate cyber security, making them easy targets for hackers. Since most government and financial institutions, military groups, corporations,

hospitals, and other businesses store and process a large amount of confidential information on computers, network outages, computer viruses, data conceded by hackers, and other incidents affect our lives in ways that range from inconvenient to life-threatening. As a result, with the growing number and sophistication of cyberattacks, there is a greater need to defend personal information and sensitive business, as well as national security. Cybersecurity is becoming a more important aspect of national security policy.

Methodology

This paper is a qualitative study that is explanatory and descriptive based on secondary data for which its users are analysis, reports, journals, research papers, and newspaper articles.

Objectives

- To evaluate the threats to national security in cyberspace.
- To understand and examine the vulnerability of cyberspace.
- To elicit preventive measures by the government.
- To understand the national security threats of different countries in cyberspace through their cases.
- To highlight their problems and issues and accordingly suggest measures for their betterment.

LITERATURE REVIEW

- [961]**Kathan Patel, Dhaval Chaudasama(2021)National security threats in cyberspace:** this paper examines how some threats may affect national security. The digital infrastructure of the nation must be treated as a national asset and should be protected.
- [962]**Jobin Sebastian, Sakthivel (2020) cyber-Terrorism – a Potential threat to National security in India:** This essay explores the potential threats to India's national security posed by domestic and foreign cyberterrorism. It is important to adequately enlighten the populace and other elements of society about the threat that terrorism poses and how it may damage India's national security.
- [963]**Imre Dobak (2021) Thoughts on the evolution of national security in cyberspace:** The future of national security, related thinking, and the formation of principles and processes are directly impacted by the development of the technological environment and the extraordinarily rapid changes in cyberspace. Future nations' access to cutting-edge technology and capabilities with unanticipated advantages will depend heavily on technical leadership.
- [5]**Sushma Devi Parmar Cyber security in India: An Evolving Concern for National Security:** This essay analyses the

[961] Dhaval Chudasama, Kathan Patel, National Security Threats in Cyberspace (June. 17, 2021), http://lawjournals.celnet.in/index.php/njcsl/article/view/829.
[962] Jobin Sebastian, P. Sakthivel, CYBER TERRORISM: A POTENTIAL THREAT TO NATIONAL SECURITY IN INDIA (July. 08,2020) http://www.jcreview.com/fulltext/1971600594378.pdf.
[963] Imre Dobak, Thoughts on the evolution of national security in cyberspace (February. 08, 2021), http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.doi-10_35467_sdq_133154. [5] Sushma Devi Parmar, Cybersecurity in India: An Evolving Concern for National Security, https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

importance of cybersecurity in the current security debate, concentrating on the topic from India's perspective. According to policies already in place in other digital nations, protecting key information infrastructure has risen to the top of the list of security-related concerns for the country.

EVALUATION OF THREATS TO NATIONAL SECURITY IN CYBERSPACE

[964] In this age of digital change and globalization, Cybercriminals are constantly on the lookout for new exploits and developing advanced techniques to defraud and destroy institutions and businesses . When cybercrime is perpetrated against the government, it is regarded as a threat to the country's sovereignty. Hacking, obtaining confidential information, cyber warfare, cyber terrorism, and pirated software are all forms of cybercrime against the government. Hacking government and military websites, as well as spreading propaganda, are examples of government cybercrime. Terrorists or various countries' enemies are frequently the perpetrators of these crimes. Cybercriminals are always looking for new exploits and devising advanced strategies to defraud and harm institutions and organizations in this age of digital change and globalization.

Every day in today's world, hackers break into systems and cause harm, make modifications to the targets' sensitive information, and web pages, or just prevent the user from accessing their device. From medical records to bank account information, hackers can attack in a variety of ways. There is a digital shift due to the COVID-19 outbreak, which has provided hackers with new targets. Malicious actors are benefiting from this digital shift, posing an increasing threat to national security on a global level. Various banks have witnessed a spike in cyberattacks during the pandemic. The health sector is the industry experiencing COVID-19-related cyberattacks at the second-highest rate, according to the Bank for International Settlements. As innovation, competition, and the pandemic propel the digital revolution, national security in cyberspace will only become more vulnerable. Hackers attempted to steal $1 billion from Bangladesh's central bank in February 2016 by taking advantage of holes in SWIFT, the main electronic payment messaging system used by the world's banks. The majority of transactions were stopped, but $101 million was lost. The incident acted as a sobering warning to the financial industry that systemic cyber risks to the banking system had been greatly underrated. Such events should be avoided. A country or organization must ensure that its systems are secure. Cyber threats arise from a variety of sources, including hostile Nation-states, Terrorist groups, Hacktivists, Hackers, and Disgruntled insiders.

[965]The most common cyber-attacks are as follows:

1. **Malware attacks:** Malware refers to malicious software, and viruses including Trojans, worms, ransomware, adware and spyware. This malicious software infiltrates, monitors, or creates a backdoor into a company's systems or data. [966]Microsoft was the victim of the WannaCry ransomware attack caused by the WannaCry crypto worm (May 2017). WannaCry perpetuated a weakness in Microsoft's operating system, Businesses across the globe had to pay a Bitcoin ransom to the WannaCry program's designers to recover access to their systems and any files that hadn't been saved up.

[964] Abi Tyas tunggal, What is a Cyber Threat, Upguard (Nov. 10, 2021), https://www.upguard.com/blog/cyber-threat.

[965] Diego Poza, The 7 Most Common Types of Cybersecurity Attacks in 2021, autho (Aug. 16, 2021), https://auth0.com/blog/the-7-most-common-types-of-cybersecurity-attacks-in-2021/.

[966] Massive ransomware infection hits computers in 99 countries, BBC (May. 13, 2017), https://indianexpress.com/article/explained/explained-the-darkside-cyberattack-on-a-usoilpipeline-and-how-it-impacts-prices-7310822/.

Colonial Pipeline Company, an American oil pipeline company, was hit by a significant ransomware attack (2021). The Colonial Pipeline Company's IT systems were destroyed by a cyberattack, which also cut off the petroleum supply to the US East Coast and resulted in a one-day shutdown. The corporation paid the hackers $4.4 million in bitcoin with the help of the FBI. Dark Side, according to the FBI, was behind the attack.

2. **Phishing attacks:** this is the most damaging type of cyberattack. In this, the hacker sends fake emails, which source appears to be legitimate. By doing so, the hacker can install malware or steal sensitive data like credentials, credit card information, and so on. [967]In 2013, To get access to the AP News Twitter account and falsely post that the White House was under attack, hackers employed a targeted phishing attack (spear-phishing).

3. **Distributed denial of service** attacks- DDoS attacks interrupt traffic by flooding a network with traffic from hijacked computer networks (botnets), preventing legitimate users from accessing it. In February 2018, GitHub[968] was subjected to the world's largest DDoS attack, receiving 1.35 terabits of traffic per second and being knocked offline for about 20 minutes as a result. In September 2017 2020 google attack, the IT giant stated that its infrastructure was subjected to a massive 2.5Tbps DDoS attack, the highest-bandwidth attack, which was the climax of a six-month campaign using several attack tactics. This attack was four times larger than the Mirai botnet's record-breaking 623 Gbps attack a year ago. Google said it is collaborating with others in the internet community to detect and decommission attack infrastructure.

4. **Man-in-the-Middle Attacks**- Bad actors spy on or intercept communication between business and your users or staff in man-in-the-middle (MitM) attacks. MitM attacks are most typically used to steal personal or company information, divert it to a different location, or in espionage situations. MitM attacks involve hackers exploiting unsecured Wi-Fi while disguising themselves as guests, sending data, and installing malware to process victims' data.

5. **Credential stuffing attacks**- a form of brute-force cyber-attack in which criminal actors access user accounts at another business using stolen usernames and passwords from one data breach. It's feasible to stuff credentials because people reuse the same password to access multiple accounts and it is the main cause of data breaches globally.

6. **Structured query language (SQL) Injection** attack-By utilising SQL to inject malicious code into a server, an attacker

[967] AP Twitter account hacked in fake 'White House blasts' post, BBC (April. 24, 2013), https://www.bbc.com/news/world-us-canada-21508660.
[968] GitHub Survived the Biggest DDoS Attack Ever Recorded, Wired (Jan. 3, 2018, 11:01 Am), https://www.wired.com/story/github-ddos-memcached/.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 1 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

can force it to divulge confidential data.

VULNERABILITIES IN INDIAN CYBERSPACE

India's digital infrastructure, user base, and accessibility are all improving at a rapid pace. However, adequate cyber security measures have not kept pace with India's digital surge, leaving many businesses vulnerable to cyber-attacks. Cyber threats are always changing to take advantage of internet trends and behavior. This outbreak of COVID-19 is no exception.

In the midst of a health crisis, cybercriminals are attacking networks and systems; 6.97 lakh events were reported in 2020, almost matching the total from the previous four years' CERT-In.

The Minister of State for Electronics and Information Technology, Rajeev Chandrasekhar, claims cyberattacks using masked actors and covert servers against Indian internet. In 2021, CERT-In recorded 6.07 lakh cyber security incidents, 12,000 of which included governmental bodies.

There were 6,07,220 cyber security events reported in the first half of 2021, according to data from CERT-In, which is in charge of collecting and monitoring cyber security occurrences in the nation. This number was 2,08,456 in 2018, 3,94,499 in 2019, and 11,58,208 in 2020. [969]The IP addresses of the computers from which the attacks seem to have come are from Algeria, Brazil, Canada, China, France, Germany, Hong Kong, Indonesia, the Netherlands, North Korea, Pakistan, Russia, Serbia, Singapore, South Korea, Sri Lanka, Taiwan, Thailand, Tunisia, Turkey, the United States, and Vietnam, according to the logs examined and made available to CERT-In. The overall number of cyber security incidents in 2021 includes the hacking of 15,651 Indian websites. (Through June). In 2018, this number was 17,560; in 2019, it was 24,768; and in

2020, it was 26,121. Similarly, over the years 2018, 2019, 2020, and 2021 (up to June), a total of 70,798,85,797,54,314 and 12,001 cyber security incidents were related to government organizations, respectively

THREATS TO INDIAN CYBER SECURITY

Chinese hacker organizations have been constantly attacking Indian public sector firms and technical establishments through cyberspace. China has been an enemy of countries like the United States and Europe for decades. Chinese hackers have recently been invading India's cyberspace in large numbers. security breaches since the border conflicts between India and China in May 2020. China is now ranked second in cyber power by Harvard University's National Cyber Power Index. However, India is one of the world's most cyber-targeted countries and India is China's most important target.

Shadow Pad & Red Echo on February 28 2021, a Massachusetts-based firm produced a report claiming that a Chinese group known as Red Echo had increased its usage of resources such as malware. Attacking "a large swath" of India's electricity industry was its main objective. According to the report, four Regional Load Dispatch Centre's (RLDCs), which are in responsible of balancing the supply and deman' of electricity in the nation's power system, were among the 10 distinct Indian power sector organizations targeted. Cyber offensive activities and events increased globally in the second half of 2020, with a focus on the pharmaceutical and vaccine industries. Stone Panda, a Chinese hacking organization, discovered flaws and vulnerabilities in Bharat Biotech and the Serum Institute of India's IT infrastructure and supply chain software. Stone Panda's attack on SII and Bharat Biotech's IT systems was motivated by a desire to steal their intellectual property and acquire a competitive advantage. Biggest cyber-attacks in Pune, 2018 The FBI has warned banks of a

[969] Over 26,100 Indian websites hacked in 2020 as per CERT- In data: Sanjay dhotre, economic times (Mar. 18, 2021, 4:34 PM), https://economictimes.indiatimes.com/news/defence/over-26100-indian-websites-hacked-in2020-as-per-cert-in-data-sanjaydhotre/articleshow/81569782.cms.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

major hacking threat to cash machines worldwide after the largest cyber-attacks in Pune, in which unidentified hackers transferred about Rs 95 crore from [970]Cosmos cooperative bank into foreign-based bank accounts.

MEASURES TO STRENGTHEN NATIONAL CYBERSECURITY

India's CERT-In provides cyber security alerts and advisories, addressing national cyberspace security concerns in the new National Cyber Security Strategy 2021 (NCSS2021).

Various strategies to counter cyber attack

- The 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre) is a government-run organisation that aids in the discovery of risky programmes and offers free ways to get rid of them.
- National Cyber Coordination Centre operational; Phase I of NCCC provides situational cyber security knowledge.
- The National Informatics Centre (NIC) has a Security Monitoring Centre (SMC) in place to detect and respond to security incidents involving NIC infrastructure and data centers.
- In addition, security audits and vulnerability assessments of resources are performed regularly to improve data security.
- At CERT-In, a Cyber Security Incident Response mechanism is in place 24 hours a day.
- Union Ministry of Home Affairs recognizes I4C as key combatant against cybercrime.
- The government establishes the National Cyber Crime reporting system, focusing on women and children's cybercrime.
- The NCIIPC analytics center enables near real-time threat intelligence and situation awareness, dependent on which daily alerts and advisories are provided to Critical Information Infrastructure (CII) or Protected System Entities (PSE) to prevent cyber threats.

[971]According to the United Nations specialized agency for information and communication technologies-the International Telecommunication Union, India has been ranked 10th at the global level and ranked in fourth place in the Asia-Pacific region in the Global Cybersecurity Index[972] (GCI) 2020. In the index's previous edition from 2018, it was rated in the 47th spot. India's ranking of 10th place is a significant improvement. Since the pandemic began, there has been an increase in cyber-attacks in India. The GCI is a reliable indicator of a country's commitment to cybersecurity on a global scale. The United States came out on top, with the United Kingdom and Saudi Arabia tied for second place in the GCI. China and Pakistan were placed 33 and 79, respectively.

CONTEMPORARY CHALLENGES

Digital revolution demands cybersecurity for businesses, corporations, organizations, and governments; India enacted Information Technology Act 2000, revised 2008, to protect against cyberattacks.. Every day, technology advances in some way. To be more watchful and attentive in the face of cybercrime, India implemented a National Cyber Security Policy in 2013. The policy, however, turned out to be extremely weak. To deter Data breaches, ransomware, and hacking, cybersecurity must

[970] DNA, Pune ATM hack: FBI had issued cash-hack alert to banks globally few days back (August. 14, 2018, 03:40 PM), https://www.dnaindia.com/technology/report-pune-atm-hack-fbi-had-issued-cash-hack-alert-tobanksglobally-few-days-back-2649699.

[971] PTI, India ranks among top 10 in ITU's Global Cybersecurity Index (June. 30, 2018, 12:32:33 PM), https://indianexpress.com/article/india/india-ranks-among-top-10-in-itusglobalcybersecurity-index-7382520/.

[972] GLOBAL CYBERSECURITY INDEX 2020, https://www.itu.int/en/ITUD/Cybersecurity/Pages/global-cybersecurity-index.aspx.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

also advance. [973]Automotive hacking is on the rise, Modern vehicles are equipped with automatic software and these automobiles connect using Bluetooth and WIFI, which exposes them to several vulnerabilities and hacker threats. Increased mobile banking, malware, and attacks make devices vulnerable to hackers, despite security measures by programmers. Hackers can exploit system bugs and vulnerabilities in 5G and IoT, exposing devices to vulnerabilities and posing a significant cybersecurity threat in 2021.

India is the second-fastest digital adaptor among 17 of the world's most digital economies, and growing digitalization necessitates proactive cybersecurity measures. Businesses and government departments must identify and address security gaps in their organization, as well as build a tiered security system in which security threat intelligence is shared between tiers. To establish operational coordination among numerous agencies and ministries, an apex entity is required[974]. The 2021 X-Force Threat Intelligence Index released by IBM Security showed how cyberattacks advanced in 2020. Threat actors targeted organizations that couldn't afford disruption owing to concerns of disrupting medical operations or key supply chains, with cyberattacks on healthcare, manufacturing, and energy doubling over the previous year. IBM predicts manufacturing and energy will be the most targeted industries in 2020, followed by banking and insurance. Attackers exploited 50% rise in ICS vulnerabilities. India's finance and insurance industries were heavily targeted, accounting for 60% of attacks. Asia Pacific faces data theft, ransomware, and business email compromise threats.

AUTHOR'S VIEWPOINT

In today's world, there is a greater reliance on technology; technological advancements have provided both ease and trouble for society in every way. Pandemic accelerates digitization of critical infrastructure, including financial services, banks, and power, with 5G implementation increasing interconnection and internet entry points. A local, state or federal government keeps a significant amount of sensitive information about its residents and the country (geographical, military-strategic assets, and so on). Hackers cause harm, modify sensitive information, and prevent user access to systems. From medical records to bank account information, hackers can attack in a variety of ways. There is a digital shift due to the COVID-19 outbreak, which has provided hackers with new targets. Malicious actors are benefiting from this digital shift, posing an increasing threat to national security on a global level. Businesses and government departments must identify and address security gaps in their organization, as well as build a tiered security system in which security threat intelligence is shared between tiers. To establish operational coordination among numerous agencies and ministries, an apex entity is required. As digitalization increases the more it is posing threat to national security. So proper strategies require to prevent these threats to national security.

REFORMS, SUGGESTIONS AND CONCLUSION.

The pandemic has brought greater reliance on technology, and the government's need to keep up with the digital revolution. This advancement in technology has created both conveniences as well as trouble for the national security threats in cyberspace. Developed nations, such as the United States, have been the target of several cyberattacks WannaCry ransomware attack (2017), SolarWinds attack (2020) and Colonial Pipeline ransomware attack, etc. and developing countries like India have also been a target like cosmos (2018) Chinese 'Red Choc-bar attack (2021) are some

[973] Nikita Duggal, Top 10 Cyber Security Trends for 2021(Nov 15, 2021), https://www.simplilearn.com/top-cybersecurity-trends-article.

[974] Central body accountable for nation's cyber security: NCSC Pant, The Economics Times, (Oct. 26. 2021, 08:48 PM IST) https://economictimes.indiatimes.com/news/defence/centralbodyaccountable-for-nations-cyber-security-missing-ncsc-pant/articleshow/87285059.cms.

of the examples necessitating modern cybersecurity operations that are appropriate with the scope and complexity of security threats. It is essential to ensure that all digitization projects in the country are designed with security in mind from the start and demand that security roles and duties in such programs and initiatives be strengthened. Implementing a high level of cybersecurity operations that correspond to the scope and complexity of security threats assuring timely reporting of vulnerabilities and problems in the projects' equipment and solutions. The digital economy's primary driver would be the digitization of payment and financial transaction processing. To ensure a fast-paced but innovative and experimental transformation of transaction processing, careful and concentrated efforts would be required.

Digital presence is growing, exposing them to more threats. Security issues may cause individuals, organizations, and governments to be unprepared or underprepared, thereby damaging national security. Advanced technology (5G, wireless, cloud, mobile, IoT, robotics, and so on) provides convenience while also posing risks. The challenges of technology transformation and widespread digitization are advancing threats to national security, which demand a fresh look at cybersecurity in India and around the globe. Governance and Institutions should work together to strengthen cybersecurity. Current challenges and future threats necessitate the evolution of national cybersecurity.

TABLE OF CASES

WannaCry Ransomware Attack (May 2017)

Colonial Pipeline Attack (May 2021

AP Twitter Account Hacked in Fake 'White House Blasts' Post (2013)

Distributed Denial of Service Attack (February 2018)

Google Attack (September 2017 and 2020)

Software Data Attack

Credential Stuffing Attack

Structured Query Language Injection Attack

Shadow Pad & Red Echo (February 28. 2021)

Stone Panda's Attack

Largest Cyber Attack, Pune (2018)

TABLE OF ABBREVIATION

Serial No.	Abbreviation	Full form
1	IP	Internet protocol
2	SWIFT	Society for worldwide interbank financial telecommunication
3	US	United state
4	IT	Information technology

5	**FBI**	Federal bureau of investigation
6	**DDoS**	Distribution denial of service
7	**SQL**	Structured query language
8	**CERT**	Indian computer emergency response
9	**SII**	Science information infrastructure
10	**NCCC**	National cyber coordination center
11	**SMC**	Security monitoring center
12	**NIC**	National informatics center
13	**MHA**	Ministry of home affairs
14	**NCIIPC**	National citizen information infrastructure protection center
15	**CII**	Critical information infrastructure
16	**PSE**	Protected system entities
17	**COVID**	Coronavirus disease
18	**GBPS**	Giga per second
19	**MITM**	Man in the middle
20	**RLC**	Regional load dispatch
21	**NCSS**	National cyber security strategy
22	**GCI**	Global cybersecurity index
23	**IOT**	Internet of things
24	**IBM**	Industrial business machines
25	**ICS**	Industrial control system
26	**RAT**	Remote access Trojans
27	**CVE**	Common vulnerabilities and exposure
28	**BEC**	Business email compromise