Major Events and Trends in Cybersecurity in 2019

January 2020

An Overview of the Cybersecurity Landscape in 2019

Cybersecurity threats and challenges continued to be a top priority for policymakers around the world in 2019. Cyber-attacks are no longer seen as standalone attacks, but as national security threats, not just because state actors are seen to be behind many of these attacks, but also because cybercriminals now have reached levels of sophistication at par with those of state actors.

Industrial control systems and other critical infrastructure continued to be targeted by malicious actors though none reached the scale of Wannacry and Notpetya attacks of 2017. Many high-profile data breaches also grabbed headlines in 2019, including those at Wipro, Toyota and Capital One. Advanced persistent threats (APTs) remained true to their classification, persisting even in the face of responses like naming and shaming, sanctions and the like. Some mutated while others went dormant even as their wares continued to persist in networks, used in campaigns ranging from cybercrime to political and industrial espionage. Whilst threats to the electoral process were the focus of many investigations in the United States (US), attempts to manipulate the electoral process were also seen in countries across the world.

Even though the threats were global, policy responses, by virtue of the fact that there was no overarching authority to regulate the internet, necessarily had to be local. The trends were largely in the direction of asserting national sovereignty through a variety of measures, ranging from cutting off from the global internet, as in the case of Iran, to data localisation to executive orders mandating several regulatory measures designed to reduce dependence on foreign vendors and products, increasingly seen as severe vulnerabilities and threats to national security.

As the impending militarisation of cyberspace seemed to have become a self-fulfilling prophecy, it is not so much a case of militarisation as it is of the realisation that the military also had a role to play in the cyberspace. Though militaries have so far largely played a passive role in cyberspace, the formalisation of cyber conflict has made a more prominent role for the military in cyberspace an inevitability.

The private sector evokes imagery of multinational corporations with large cybersecurity budgets and the wherewithal to take care of themselves but the medium and small-scale companies are susceptible to cyber-attacks since they lack the resources to ensure 360-degree security. Micro, small and medium enterprises (MSMEs) largely ended looking up to third-party security vendors and cloud providers to mitigate risks of breaches but that resulted in third-party vendors being targeted and ending up as sources of compromise. The vulnerabilities associated with third-party vendors added to already existing problems as to where the responsibility lay in the event of a breach. In the absence of any certification of third parties, the company had to *ipso facto* do their due diligence with regard to vendors and cloud providers. Issues facing chief information security officers (CISOs) who form the frontline against malicious actors include the scarcity of qualified personnel, the skills

gap, addressing emerging technologies such as artificial intelligence (AI) and blockchain and securing existing technologies such as the cloud.

With many countries in various stages of enacting data protection bills, data privacy issues came to the fore in 2019. There was a concomitant uptick in the cyber insurance business, which was seen as an additional factor, with the potential to improve cybersecurity practices of companies. However, the nascence of the business was underlined by the fact that even in 2018, cyber premiums in India were only in the range of US$ 14 million with about 350 policies being sold, as compared to about US$ 2.5 billion in the US.

By way of remedial measures in India, the most notable was the establishment of the Defence Cyber Agency announced by the Prime Minister in May 2019. It will be part of the three new tri-service agencies, for cyber warfare, space, and special operations. Being a tri-service agency, it will consist of personnel from all three arms of the Indian defence forces: army, navy and air force. The National Cyber Security Co-ordinator's (NCSC) office also announced that it is in the process of finalising a National Cyber Security Strategy, to be brought out in 2020.

In 2019, it was not just India, but the wider South Asian region that was subject to attacks on critical infrastructure. The most notable attack came towards the end of the year when a malware infection in the IT network of the Kudankulam Nuclear Power Plant (KKNPP) located in Tamil Nadu was first reported in social media on October 28, 2019. The coincidental shutdown of one of the plants in the preceding week led to speculations that the two were connected. An initial official response from the plant authorities refuted these reports. Subsequently, officials from other agencies including the NCSC confirmed these reports, and the Nuclear Power Corporation of India Limited (NPCIL) – the parent body responsible for running the nuclear power plants in the country – came out with an official press release giving some details of the incident. In its October 30 press release, the NPCIL clarified that the infected personal computer was in use for administrative purposes only, and the control systems of the plant and critical functions were unaffected by the breach. These details were later confirmed by the Union Minister of State for the Department of Atomic Energy in the Parliament on November 20.

These headlines notwithstanding, it was the finance and banking sectors that were most susceptible to hacking incidents as well as cyber frauds. In early November, it was reported that details of 1.3 million credit cards issued by Indian banks were up for sale on the dark web. These details were believed to have been obtained through card skimmers, installed either on automated teller machines (ATMs) or point of sale (PoS) systems. This was first reported by the tech website *ZDNet* which described it as one of the biggest card dumps in years. The Reserve Bank of India (RBI) issued an advisory to banks on November 29 advising them to "verify the correctness and genuineness of the data" and to take a series of measures if the leaked data was found to be authentic, including re-issuing of cards and closely monitoring transactions to check for anomalies. The National Payments Corporation of India (NPCI) also held a meeting with banks.

Even if there were no reports subsequently, a similar incident in Pakistan in 2018 showed that these incidents were all too common and the compromised cards could make their way into the hands of criminals before long. In October 2018, Pakistani banks were hit by hackers, compromising the data of 19,864 customer cards of 22 Pakistani banks. This data was put on sale on the dark web, according to the Pakistan Computer Emergency Response Team (PakCERT). Considered as the most audacious cyber-attack on banks in the history of Pakistan, the identity of the hackers is yet to be confirmed. Just a month later, in November 2018, Pakistan's banks were brought to a halt due to rising reports of more than 8,000 leaked card details online of the customers. One of the banks affected, the Bank Islami, shut down international transactions after noticing about Rs. 2.6 million (US$ 20,000) in "abnormal" transactions. Although Pakistan denied that their banks have been hacked, they acknowledged the online leaking of card details for sale. The payment details were offered in two formats. One included the cardholder's name, address, phone number, card number, expiry date, and CVV. The other format is skimmed card details, which may have been collected from an ATM or a merchant. This was quite similar to the details of 1.3 million Indian credit cardholders allegedly available on the dark web.

Despite a number of measures taken by the financial authorities, such incidents continue to pose a grave risk to users and come in the way of achieving the goal of increasing digital transactions within the financial system. Whilst incidents of payment card and ATM fraud were on the increase as seen in daily news reports, it was not adequately captured by the official statistics which show only 911 such incidents in 2017-18 with a cumulative loss to customers of Rs. 21.46 crores (down from Rs. 65.4 crores the preceding year). Part of the reason for this was that the data does not account for losses below Rs.1 lakh.

Whilst ATM frauds come in all sizes and shapes and range from cloned ATM cards to armed thefts inside ATM kiosks, many of the notable bank thefts perpetrated through cyber hacks had the money flowing out of ATMs and were linked largely to the North Korean hackers. The theft of US$ 13 million (Rs. 100 crores) from the Cosmos Bank in Pune in August 2018 was executed through simultaneous ATM withdrawals across 23 countries in three hours as well as the transfer of Rs. 13.92 crores to a Hong Kong-based company's account in three unauthorised SWIFT (Society for Worldwide Interbank Financial Telecommunication) transactions. The overall impact on the bank was estimated to be in the range of Rs. 1000 crores, counting premature withdrawal of deposits of Rs. 500 crores and saving deposits amounting to Rs. 300 crores. While the technical details are available in various reports, the bottom line is that the entire operation was made possible by the fact that the bank's infrastructure was connected to the global financial infrastructure and the attackers made use of vulnerabilities and insufficient security safeguards both at the level of the bank as well as the global level. The bank recovered about Rs. 10 crores. A year on, even though about 15 "money mules" involved in withdrawing money from the ATMs have been arrested, and a special investigation team (SIT) has been investigating the attack, with queries sent to several countries

including Turkey, Bulgaria, Japan, United Kingdom (UK), France, Hong Kong and Latvia, the masterminds of the heist are yet to be traced.

According to the reply to a right to information (RTI) application filed with the RBI, over 50,000 "cyberfrauds" were reported in the period 2018-19 including those perpetrated through ATMs, debit and credit cards, and internet banking. These did not include fraud perpetrated through new modes such as the unified payment interface (UPI) and prepaid instrument (PPI).

The Central Bureau of Investigation (CBI) organised its first-ever National Conference on Cyber Crime Investigation and Cyber Forensics in September 2019. The conference had several panel discussions, lectures and presentations on various topics of law enforcement, including social media, mobile/digital forensics, online harming including child sexual abuse, establishing standard formats for data exchange between service providers and law enforcement agencies (LEAs), and intermediary liability. Whilst this is a noteworthy initiative, the fact that this was only the first time that such an event has been organised shows that investigative agencies have been slow to respond to issues of cybercrime.

The other notable event that took place during the year was related to WhatsApp. In early May 2019, a zero-day exploit called Pegasus spyware was detected on WhatsApp. This spyware could inject itself on any targeted mobile phone through a call and access all its data including call logs, email and messages. This spyware was created by an Israeli firm NSO that has a stated objective of creating "technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe." Following the discovery of the malware, a number of cases where at least 100 human rights defenders, journalists and other members of the civil society were targeted via app came to the fore.

According to a report generated by Citizen Lab at the University of Toronto, NSO's software has been detected in almost 45 countries with civil society members seen to be targeted in six. Recent reports have suggested that India with more than 200 million active WhatsApp users has also become the target of the malware. Following this, the authorities asked for an explanation from WhatsApp, to which the company responded that CERT-In had been informed in May and other government agencies in September. Governments around the world are seeing WhatsApp and other social media companies as being non-co-operative in providing the antecedents of false and fake social media communications that have time and time again led to social unrest. Cyber intelligence firms also have to be regulated, for they are taking advantage of the fact that cyber-surveillance products are largely unregulated and sold to the customers without doing due diligence.

Mobile phones belonging to at least two dozen Pakistani officials were also compromised in the Whatsapp breach. Pakistan's leading English daily *Dawn* reported that the federal ministry of information technology had issued a confidential letter to the authorities affected by the breach, advising them not to use WhatsApp for official correspondence due to "hostile" intelligence agencies seeking to gain access to sensitive information stored in

or communicated via mobile phones. The ministry also advised government officials to discard all mobile phones purchased before May 10, 2019.

One important caveat that must be noted is that the focus of the policymakers is increasingly on social media apps and the potential for its misuse, which might lead to less attention being paid to core cybersecurity issues, even as they continue to be as potent as before. Even at the international level, the deliberations of the newly resurrected UN Group of Governmental Experts (UN GGE) and the newly introduced mechanism of Open-Ended Working Group (OEWG) have not received the kind of attention and interest of earlier iterations. Given the virtual split between country groupings at the UN, the proposed open-ended ad hoc intergovernmental committee of experts to be set up in August 2020 to look into a UN cybercrime convention, will in all likelihood make slow, if at all, any progress on its primary mandate "to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes."

Sectoral Analysis of Key Cybersecurity Incidents in 2019

Cybersecurity incidents continue to target a wide variety of businesses, government systems and industries. The motive behind the attacks vary from political gains to industrial espionage. An assessment of the key cybersecurity incidents over the last one year suggests that a vast majority of them were either espionage attempts (political and industrial) or targeted at the critical infrastructure (including industrial control systems and utilities). A few of them were reported to be targeting the elections, political parties or the electoral processes. Most of these incidents occurred against the backdrop of an ongoing geopolitical standoff. Cybersecurity incidents reported or originating from the US, UK, Australia, China, Iran, North Korea and India have been included in this assessment.

Critical Information Infrastructure

Amongst the critical infrastructure, electricity grids and oil facilities were the prime targets. Iranian, Chinese and Russian hackers were reported to be behind most of these attempts. At the very beginning of the year, Iran was revealed to have engaged in a global DNS hijacking campaign targeting telecommunications and internet infrastructure providers in Europe and North America. Throughout the year 2019, various reports surfaced where Iranian hackers were found to be targeting government, industry digital infrastructure, banks, and operators of industrial control systems. The beginning of the year also marked the arrest of Huawei's Chief Financial Officer Meng Wanzhou in Canada on an American request over the alleged role of Huawei in crimes ranging from wire and bank fraud to obstruction of justice and conspiracy to steal trade secrets. In February, following an attack

on the Indian security forces in Kashmir, Pakistani hackers targeted almost 100 Indian Government websites and critical systems. In March, an Iranian cyber espionage group reportedly targeted government and industry digital infrastructure in Saudi Arabia and the US, and in a separate hacking campaign targeted banks, local government networks, and other public agencies in the UK. In June, the US electricity grid regulator NERC issued a warning that a major hacking group with suspected Russian ties was conducting reconnaissance into networks of electrical utilities. In the aftermath of Iran's attacks on Saudi Arabia's oil facilities in October, the US also carried out cyber operations against Iran.

Political Espionage

Geopolitical confrontations continued to reflect in the attempts of espionage through cyber means. Most of them were targeted against adversarial nation states, their diplomatic missions, think tanks, non-governmental organisations (NGOs), and other political organisations. Accusations were made against the Chinese hackers for espionage on students at the Australian National University, and malware attacks targeting the Uyghur community and senior Tibetan lawmakers, to name a few. They were found to be using backdoors through propaganda apps, using compromised websites, exploits for Apple, Google, and Windows phones, and NSA hacking tools which were leaked in 2015. Hackers with ties to the Russian Government were reportedly conducting phishing campaign against embassies and foreign affairs ministries of countries across Eastern Europe and Central Asia and also using an Iranian hacking group's tools and infrastructure to spy on West Asian targets.

Amidst tensions between the US and North Korea, a phishing campaign targeted US entities researching the North Korean nuclear programme and economic sanctions against North Korea. Around the middle of the year, Russia accused Western intelligence services of hacking into Yandex to spy on user accounts and Iran exposed an alleged Central Intelligence Agency (CIA)-backed cyber espionage network working across multiple countries. In July 2019, Microsoft revealed that it had detected almost 800 cyberattacks over the past year targeting think tanks, NGOs, and other political organisations around the world, with the majority of attacks originating in Iran, North Korean and Russia. Towards the end of 2019, Chinese hackers were reported to be targeting entities in Mongolia, Myanmar, Pakistan and Vietnam; individuals involved in UN Security Council resolutions regarding the Islamic State of Iraq and Syria (ISIS); and, members of religious groups and cultural exchange non-profits in Asia.

Industrial Espionage

Several instances of industrial espionage surfaced during the year from across the globe. A majority of the instances pointed to China and a few named Russia, Iran and North Korea. The US accused the Chinese hackers of stealing research on naval technologies from 27 of its universities, cancer research institutes, and also unearthed the intellectual property theft campaign which supported the development of Chinese C919 airliner. Some of the major German firms including BASF, Siemens and Henkel announced that they had been the victim of a state-sponsored hacking campaign and it was linked to the Chinese Government. Huawei had also accused the US Government of hacking into its intranet and internal information systems. Iranian hacking campaigns throughout 2019 were found to be stealing corporate secrets from oil and gas companies, as well as from 60 universities in the US, Australia, UK, Canada, Hong Kong and Switzerland. North Korean hackers allegedly targeted an Israeli security firm as part of an industrial espionage campaign.

Electoral Processes

Since the last US presidential elections, electoral processes have remained vulnerable to cyber-attacks. The Democratic National Committee of the US, in the early part of 2019, revealed that it was targeted by Russian hackers in the weeks following 2018 midterm elections. Russian hackers were also accused of targeting individuals in Europe at civil society groups working on election security and democracy promotion in the wake of the European Union (EU) elections. A couple of cases of DDoS (distributed denial of service) attacks against political parties and also probing surfaced from the UK, Indonesia and Israel as well.

Major Cyber Incidents in the South Asian Region

Pakistan

In the wake of *Ashura*, during the observance of related religious activities, arbitrary network shutdowns were reported from a number of areas in Karachi and Islamabad. Network shutdowns are a regular practice every year during sensitive religious and national events, including *Ashura*, the Independence Day, and especially in the sensitive areas surrounding the hubs of religious activity. In February 2019, several Pakistani websites fell prey to cyber-attacks. According to reports, the Indian hacker group called Team I Crew was behind the hack. The cyber-attack occurred as a response to the attack

on India's Central Reserve Police Force (CRPF) personnel martyred in Pulwama, for which Jaish-e-Mohammed took responsibility. Among the websites hacked, were Pakistan Ministry of Foreign Affairs and the Pakistan Army. At the same time, Pakistani hackers targeted almost 100 Indian Government websites and critical systems. Indian officials reported that they engaged in offensive cyber measures to counter the attacks.

Bangladesh

In September 2019, Bangladesh's Permanent Representative to the UN Ambassador Masud Bin Momen placed some specific proposals for defining international rules of the road and capacity building in cyberspace. Bangladesh targets to have at least 1,000 cyber security experts by 2021. Earlier, in February 2019, hackers turned the Bangladeshi Embassy website in Cairo into a crypto mining scheme. They gained entry by force-downloading malicious files onto users' desktop changing the URL (uniform resource locator) access of the embassy website. Out of the 69 anti-virus engines, only three identified the infected site as malicious.

Sri Lanka

In June 2019, the Sri Lankan Government drafted the Cyber Security Bill that would tackle the growing problem surrounding cybersecurity in the country. Being part of the Cyber Security Strategy introduced in 2018, this would also help in providing vital information about cyber-attacks in the country. The Bill provides the government with the capability to establish a Cyber Security Agency, the Sri Lanka Computer Emergency Readiness Team, and the National Cyber Security Operations Centre. All these institutions would help in protecting critical information infrastructure. After the cabinet approval of the draft bill, it will require the consent of the Sri Lankan Parliament before becoming a law.

In May 2019, the Sri Lankan Government issued a social media ban following a report which stated an intensification in religious strains, weeks after the suicide bombings that rocked the country. Facebook, WhatsApp and Viber were few of the social media services banned. Similar restrictions were placed on YouTube as well. The decision to ban the social media services met with heavy criticism across the board and services were restored within a few days. In the same month, the Sri Lanka Computer Emergency Readiness Team (SLCERT) discovered the hack on websites of more than 11 institutions. The list included the Kuwait Embassy website in Sri Lanka as well. SLCERT is working along with TechCERT and Cyber Security Operation Unit of Sri Lanka Air Force to investigate the cyber-attack. SLCERT is continuously monitoring other websites that may have been attacked but not noticed yet. These websites are attacked to publish the messages of the hacker group involved.

Bhutan

In December 2018, the Bhutanese Government announced plans to draft a new cybersecurity strategy for the country. The Bhutan Ministry of Information and Communications (MoIC) in collaboration with the International Telecommunication Unit (ITU) steered a workshop to improve the cybersecurity sphere of Bhutan, thereby its first cybersecurity strategy. Along with it, the Bhutan Computer Incident Response Team (BtCIRT), formed in 2016, has tackled more than 250 cybersecurity indents, but without a comprehensive policy in place. This initiative would bring the required framework for a safer and secure cyber-space in Bhutan.

Nepal

In December 2019, 122 Chinese nationals were detained for their involvement in cross-border cybercrimes from various locations in Kathmandu. In early January this year, they were released on bail of Rs. 1000 each. The District Administration Office (DAO), Kathmandu decided to release the Chinese nationals on bail after the police failed to gather evidence to substantiate the cross-border online fraud allegations against them. The Chinese nationals were fined Rs. 1000 each on the charge of misbehaving during the police interrogation in custody. It was said that the DAO Kathmandu is preparing to hand over the Chinese nationals to the immigration department.

***

Published by:
IDSA Cybersecurity Centre of Excellence,
Institute for Defence Studies and Analyses,
1, Development Enclave, (near USI), New Delhi, Delhi 110010
Email: iccoe.idsa@gov.in