India the prime target of Cyber Warfare campaigns is taking many measures to enhance its cyber security

World has seen recently a series of high-profile global cyber attacks such as the WannaCry ransomware attack in May and NotPetya in June. In May 2017, a massive cyberattack caused major disruptions to companies and hospitals in over 150 countries, prompting a call for greater cooperation around the world. In 2016, nearly one percent of all emails sent were essentially malicious attacks, the highest rate in recent years.

A cyber security firm Quick Heal Technologies said it has detected over 48,000 MS-17- 010 Shadow Broker exploit hits responsible for 'WannaCry ransomware' outbreak in India with West Bengal witnessing the most incidents. Ransomware attacks increasingly affected businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. Attackers are demanding more and more from victims, with the average ransom demand rising to over 1,000 USD in 2016, up from approximately 300 USD a year earlier.

On May 17, the cyber-security firm Symantec stated in a blog post that it had traced breaches of several Indian organisations to a cyber-espionage group called Suckfly. The targeted systems belonged to the central government, a large financial institution, a vendor to the largest stock exchange and an e-commerce company. The espionage activity began in April 2014 and continued through 2015, Symantec said. Another cyber-security firm, Kaspersky Lab, announced that it too had tracked at least one cyberespionage group, called Danti, that had penetrated Indian government systems through India's

diplomatic entities.

India has been a target of many cyber attacks, cyber espionage and cyber warfare with fingers often pointing towards China and Pakistan. In one instance, according to the Toronto based Munk Centre of International Studies, GhostNet – a Chinese network, had infiltrated networks of the Indian Government as well as of the Dalai Lama. The elite National Security Guard's website was reportedly defaced with profanity-laden messages for Prime Minister Narendra Modi last month.

On the other hand the commitment of india towards cybersecurity measures remain inadequate. As per the findings of the Global Cybersecurity Index 2017 (GCI) released by the UN telecommunications agency International Telecommunication Union (ITU), India ranks 23 out of the 193 member countries when it comes to commitment to cybersecurity. Singapore has topped a global cyber security index released by the United Nations, followed by other UN member states such as the United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France and Canada, the other top 10 countries.

The Union home ministry has created new division to check radicalisation and cyber fraud as part of a major rejig of some of its crucial wings. The new wing, CIS, has been created to monitor online crimes and threats, including cyber fraud and hacking, and suggest ways to minimise and fight them. This division will track and counter online fraud, hacking, identity theft, dark net, trafficking and cyber attacks on critical information infrastructure, the officials said.

Rising Cybersecurity threat

Rapid digitisation in all sectors in India is making the country critically prone to targeted cyber attacks and 'WannaCry' ransomware attack is "just the tip of the iceberg", according to cyber intelligence security company. The

vulnerability of Indian critical infrastructure is further increasing with increasingly networking of the country under Digital India including critical infrastructure like transportation networks, power grids and financial institutions through on-line integration, with more and more official data stored on-line.

“Owing to the government initiatives and efforts, coupled with booming penetration of smartphones, PCs and high-speed internet access, the challenges associated with such attacks amplify significantly – making India one of the hot favourite destinations for a targeted cyber attack,” Israel-based Vital Intelligence Group said in a statement.

According to many cyber experts, several Indian companies and some government institutions have seen recently an increase in cyber attacks originating in China.Like in the case of the infrastructure company, these attacks are often carried out through difficult to-trace proxy servers in North Korea, Africa, Eastern Europe and Russia. Unlike a normal attack, the Chinese breaches tend to exploit vulnerabilities of Indian IT systems and “just observe.”

Large hardware imports from China is also leads to growing threat of hardware attacks through malicious insertion of malware or kill switch. Malware is a software which is designed to disrupt, damage, or gain access to a computer system There are reports that the Chinese have introduced malware or hidden software in Android phones and other hardware for surveillance, making it almost impossible for the user to detect any anomaly.

“The recent attacks strengthens the point that the biggest existential threat that is out there is cyber. It is evident that the world is already engaged in a 24×7 conflict with anonymous soldiers who are extremely difficult to trace,” said Marc Kahlberg, CEO and MD of Vital Intelligence Group.

The group noted that “one size fits all approach” can never be the solution to curb the increasing cyber attacks and a constant vigil is the only solution to stay ahead in the race with the intruders.

“Just like the traditional battlefield, there is no one correct strategy, no short term solution and no silver-bullet to win a war. But awareness, understanding and vigilance combined with accurate targeted offensive frontline cyber intelligence will go a long way to keep the enemy busy and protect all of our cyber interests,” added Kahlberg.

India’s cyber security Initiatives

Indian government unveiled a National Cyber Security Policy 2013 on 2 July 2013, with vision to build a secure and resilient cyberspace for citizens, business and government and also to protect anyone from intervening into your privacy. The mission is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

Recognising the strategic dimensions of cyberspace, the Prime Minister’s Office (PMO) created the position of the National Cyber Security Coordinator in 2014 to implement the policy.

In India, cyberspace is being looked after primarily by the National Technical Research Organization (NTRO) operating under R&AW. Other top layer of agencies performing cyber operations are the National Intelligence Grid, and the National Information Board.

To ensure Internet security, Computer Emergency Response Team (CERT-IN) was established by Government of India in 2004 that

reports Forecast & alerts on Cyber incidents, issuing of guidelines on Cyber incidents etc. occurring in India.

In addition, the National Critical Information Infrastructure Centre (NCIIC) carved out CERT in 2013 is to protect assets in critical sectors like energy, banking, defence, telecom, transportation etc. The NSA is to oversee a public-private partnership to set up a cyber-security architecture.

Cyber warfare

Cyber warfare has developed into a more sophisticated type of combat between countries, where you can destroy critical infrastructure such as power, telecommunications or banking by damaging the computer systems that control those infrastructures. It’s widely acknowledged that offensive cyberattacks will be a necessary component of any future military campaign, and the extreme cyberweapons are being developed now.

In early September 2016, Some 22,000 pages of data related to India’s top secret Scorpene submarine program were published online. This presumed data breach brought the issue of cyber security into the headlines.

Indian Army may face serious cyber attacks from non-state actors in Pakistan, on its critical Information Infrastructure say, the Oil and Natural Gas Corporation of Electric grids.

Pakistan has unleashed a cyber war against India on social media, Over 1000 videos supporting Jehad in Kashmir have been created and several thousand anti India posts in social media have been shared in the last six months. They are both soft toned as well as radical videos, some arousing sympathy for victims, others arousing hatred against armed forces.

Cyber Agency and Cyber command

Many countries starting with US and which now includes U.K., China, Russia, Israel and others are setting up Unified cyber commands for more effective and coordinated efforts for conducting cyberspace operations , both offensive and defensive. The offensive operations are seen as deterrent to adversaries. US, Russia and China are also implementing various defence measures to protect their classified networks from Cyber Warfare.

In a bid to enhance its combat capabilities in the virtual domain, the defence ministry is working towards establishing a new cyber agency to tackle attempts by Chinese and Pakistani hackers to break into its systems and networks. “The tri-services integrated defence staff (IDS) is coming up with a unit to tackle the cyber warfare domain and it will be staffed with personnel from all the three services,” senior government sources told Mail Today.

“The forces have already started pooling in their resources in the cyber domain under the new agency, which would be headed by a major general-rank officer. The organisation will have both offensive and defensive capabilities in cyber warfare,” said the sources. Cyber arsenal shall serve as the key function of strategic deterrence.

Till now, the army, navy and air force have their own separate cells dealing with cyber issues and they have also developed individual networks for safe communication and data exchange.

The information networks created by the forces are state of the art and are capable of detecting any violation at centralised locations within a few microseconds. “If anybody puts in a pen drive in a computer of the military network, our men sitting in Delhi and other centralised locations can detect it within no time and prevent any leakage or attack immediately,” said the sources.

“This step of creating a new cyber agency, which would be a precursor to a cyber command, is in the right direction. Now the focus should be on creating infrastructure for manufacturing totally indigenous information and communication technology equipment,” said information warfare expert Pavithran Rajan.

To test its capabilities, the new agency has also carried out its first cyber warfare exercise under which Indian forces carried out attacks on their own networks to check for loopholes and steps required to strengthen the system, the sources informed.

“The forces deduced that cyber should be the first agency to be raised for dealing with the increasing instances of attacks on military networks and systems,” they said.

The command of the new agency would be on rotational basis for the three services, which means that if it is first headed by an army officer, he would be succeeded by navy and air force officers. The head of the unit would report to the chief of integrated defence staff Lt Gen Satish Dua who heads the organisation at present.

Indian Military testing its own indigenous operating system

In his maiden address to the senior commanders of the three services, the prime minister had asked them to guard against the threats in the cyber domain and after that, Army’s Jammu and Kashmir-based Northern Command started the evaluation of the indigenous operating system for military requirements.

‘The Northern Command has been evaluating the BOSS at its headquarters as an option for replacing the foreign solutions to provide more security to the critical security-related

information of the forces deployed there,’ government sources told Mail Today.

BOSS is a software developed to benefit the usage of free software in the country and considered to be an important initiative by military analysts when cyber is fast emerging as warfare domain.

Army sources said protection of vital information in cyber domain is critical for the forces deployed in the command which faces both China and Pakistan as even if the itinerary of a small convoy gets leaked, it can be proven dangerous.
At present, the Indian military is using foreign-origin software, which have been frequently coming under the scanner for working for their countries’ intelligence agencies and cannot be considered safe in the prevailing atmosphere of leaks and cyber espionage.

Currently, a number of equipment in the cyber infrastructure used by the public sector agencies supporting military communication is sourced from foreign manufacturers. Fearing espionage through foreign equipment, an advisory was issued couple of years ago by the Air Force to its personnel against using the phones of a particular phone firm. Army officials from the Corps of Signals – which is responsible for maintenance and looking after entire gamut of military communication – said creating our own information and communication technology infrastructure would also help in providing opportunity for ‘Make in India’ products in the sector.

Cyber Range Centre at IIDT to train cyber

warriors

The International Institute of Digital Technologies (IIDT) in Tirupati is planning to establish a Cyber Range Centre to impart training to students in thwarting cyber attacks. “eSF Labs, which is the technology partner for GFSU, is setting up the Cyber Range Centre,” according to J.A. Chowdary, IT Adviser to the Chief Minister.

“At present, phishing, cyber frauds, ransomware, malicious domains, data thefts, and mobile frauds are posing a threat to the country. We have to prepare lakhs of cyber security warriors to protect from malwares,” he said.

“The IIDT students will be trained in tackling all kinds of cyber security threats. The proposed high-end Cyber Range Centre will provide a real-time environment on how to detect and thwart cyber attacks. Discussions will be held with cyber experts, researchers, and students on the subject,” said Mr. Chowdary.

International Cooperation

A cyber partnership can be critical for India to meet its immediate goals in securing its cyber infrastructure and expanding opportunities for the country’s tech sector.

Indian and US officials also met in Washington in August 2015 at the whole-of-government cyber dialogue to discuss enhanced cyber security information sharing, cyber incident management and cyber security cooperation in the context of ‘Make in India’. In Jan 2017, India and the US have signed a Memorandum of Understanding (MoU) for close cooperation and exchange of information pertaining to cyber security. The MoU between Indian Computer Emergency Response Team (CERT-In) and US CERT was signed by Electronics and IT Secretary Aruna Sundararajan

and Richard Verma, the US Ambassador to India.

With Narendra Modi's three-day state visit to Israel –India and Israel in their joint statement have committed to promote security and stability in cyberspace – with the possibility of exploring bilateral ties between their respective governments and businesses.

India's Cyber Security strategy

Ministry of Communications and Information Technology (India) define objectives as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.
- To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.
- To create workforce for 500,000 professionals skilled in next 5 years through capacity building skill development and training.

- To provide fiscal benefit to businesses for adoption of standard security practices and processes.
- To enable Protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen’s data and reducing economic losses due to cyber crime or data theft.
- To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

Strategies

- Creating a secured Ecosystem.
- Creating an assurance framework.
- Encouraging Open Standards.
- Strengthening The regulatory Framework.
- Creating mechanism for Security Threats Early Warning, Vulnerability management and response to security threat.
- Securing E-Governance services.
- Protection and resilience of Critical Information Infrastructure.
- Promotion of Research and Development in cyber security.
- Reducing supply chain risks
- Human Resource Development (fostering education and training programs both in formal and informal sectors to support Nation’s cyber security needs and build capacity.
- Creating cyber security awareness.
- Developing effective Public Private Partnership.
- To develop bilateral and multilateral relationship in the area of cyber security with other country. (Information sharing and cooperation)
- Prioritized approach for implementation.
- Operationalisation of Policy

“Cybersecurity is an ecosystem where laws, organisations, skills, cooperation and technical implementation need to be in harmony to be most effective,” stated the ITU report. India’s highly skilled IT workforce should be trained and harnessed by the government for strategic use. There is requirement to develop comprehensive cyber defence strategy to not only defend India, create a social media counter strategy but also attack adversary networks.

References and resources also include:

http://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article8327987.ece

https://thewire.in/67398/india-is-unprepared-for-future-cyber-attacks/

http://blogs.economictimes.indiatimes.com/Whathappensif/india-needs-to-fight-not-ban-pakistans-cyber-war/

http://indiatoday.intoday.in/story/cyber-attacks-pakistan-china-india-defence-ministry/1/896511.html

http://indianexpress.com/article/technology/tech-news-technology/india-a-favourite-for-cyberattacks-says-israeli-cyber-security-company-4674309/

http://timesofindia.indiatimes.com/business/india-business/india-ill-prepared-to-handle-chinese-cyber-attacks-says-expert/articleshow/59987974.cms

http://www.thehindu.com/news/national/andhra-pradesh/soft-launch-of-cyber-range-centre-at-iidt-tomorrow/article19984208.ece

http://www.dailymail.co.uk/indiahome/indianews/article-4371794/Indian-army-boss-guard-against-cyber-attacks.html