Implementations of Operative Cyber Security

Deepa RM[1], Deepika S[2], Snigdha Srivastva[3], Pujayant Kumar[4]
[1]LG soft India Pvt Ltd, Bengaluru, Karnataka
[2]TCS, Bengaluru, Karnataka
[3]DXC Technology, Delhi
[4]Aligarh college of Engineering, Aligarh, Uttar Pradesh

Abstract- *The transition to cyber operations signifies a transformation for cyber security education and research as well as for defence organizations around the world. Through financing, shared interest in the study's results, and the possibility of a job market for graduates, cyber security research and education are linked to the homeland security agencies and the defence. Through financing, shared interest in the study's results, and the possibility of a job market for graduates, cyber security research and education are linked to the homeland security agencies and the defence. In addition, it discusses the various facets of cybercrime and its security in a worldwide context. As internet usage has increased, cyber security is now utilised to protect not only a person's workstation but also their own mobile devices which have become essential means of information to transfer data in recent technological breakthroughs. In order to execute the national cyber defence plan cohesively and successfully, defensive information assurance measures and active defence-driven information operations must be collaboratively and cooperatively launched. The goal of this paper is to describe various cyber risks and how to protect ourselves from them and to the move toward cyber operations and the associated challenges.*

Keywords- cyber operations; cyber defence; information assurance, defence; Cyber Crime , information operations.NIC (National Informatics Centre), Cyber Crime, Cyber Security, NISAP (National Information of security Assurance Program), ISTF (Inter Departmental Information Security Task Force).

I. INTRODUCTION

The newest and maybe most challenging issue in the cyber realm is cybercrime. One may classify cybercrime as a species whose genus is conventional crime and in which either the computer is an object or the subject of the criminal activity. Cybercrime is any illegal behaviour that makes use of a computer, either as a tool, a target, or a way to commit more crimes.

"Acts that are penalised by the Information Technology Act" would not be appropriate because numerous cybercrimes, like email spoofing, cyberdefamation, sending threatening emails, etc., are also covered by the Indian Penal Code. Cybercrime might be defined as "illegal conduct in which a computer is either a tool, a target, or both" in a clear and concise manner.

A centre for cyber security research must be able to successfully discover the unknown. Cyber operations turn become a concrete approach to help with national security. For academia, there is also a new context in which universities may contribute to improving business and military readiness to respond swiftly to threats as opposed to prior studies that took years to enhance through the creation of products and the acquisition of defensive equipment.

As a result of the catastrophic occurrences and society's growing reliance on the Internet and computerised systems, traditional IT security has received considerable financing for the past ten years. This stance is based on fortifying systems and developing robust fail-safe procedures that can fend off invaders. resources are being poured into research facilities for cyber security.

Fig 1 : Cyber security threats and reports

II. CYBER DEFENCE CAPABILITIES IN INDIA

India is ranked 21 in the Belfer Nation Cyber Power Index, which evaluated the cyber capacities of 30 nations. India's cyber power is categorised as having lesser capability and lower intent by analysing its cyber policies. India therefore has a long way to go, particularly in light of the increased sense of danger from both state and non-state actors.The Ministry of Electronics and Information Technology's lead agency for handling cybersecurity-related issues in India is the Indian Computer Emergency Response Team (CERT-In). In order to network its activities, each of India's three military branches—the Indian Army, Navy, and Air Force—has its own cyber infrastructure. In addition, the tri-service Defence Cyber Agency was founded in 2018 to address cybersecurity threats. The National Critical Information Infrastructure Protection Centre, together with the banking, financial services, insurance, electricity, energy, telecom, transportation, government, and strategic public businesses, must all be protected (NCIIPC).

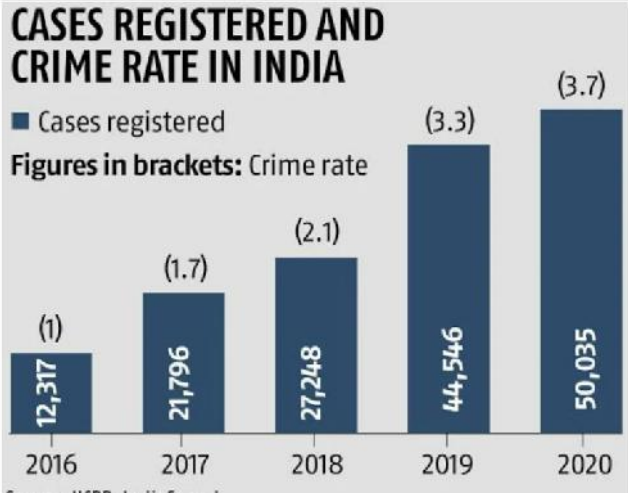

Fig 2: Cases registered and Crime rates in India

URGE NEEDED

India is one of the key participants in the international IT sourcing business, and it is still expanding. In 2020, the GDP of the nation's IT sector amounted to roughly 8%. Work from home lifestyle and the Covid-19 epidemic are both contributing to a rapid digitalization and an increase in digital payments. The key infrastructure, particularly the telecommunications network that serves as the foundation for all other services, must thus be secured immediately. In India, a substantial portion of the communication infrastructure is imported from abroad, and if that infrastructure is compromised, all other services that rely on it would also cease to exist.Some of the biggest equipment suppliers to Indian telecom firms including Vodafone, Bharti Airtel, BSNL, and MNTL include the Chinese firms ZTE and Huawei. [4] This technology poses a serious hazard since it could include backchannels for sending crucial information to China. In India, the market share of telecommunications equipment is shared by Huawei and ZTE to the tune of roughly 55%. Huawei and ZTE are not listed as participating network equipment vendors by the Indian government.The National Cyber Security Strategy 2020 seeks to create a robust, safe, and safe online environment.

Data is the new gold, hence it is crucial to secure the important information infrastructure in order to stop data espionage. The majority of India's vital infrastructure is interconnected and connected to information networks. Given that they have a significant influence on the population's economic and social well-being, protecting these is essential for India's national security. As a result, the danger to cyberspace also poses a risk to national security. Cyberspace protection is as critical than ever.

III. RECOMMENDATIONS:

1. To achieve India's goal of "Atmanirbhar," it is essential to build and manufacture the essential infrastructures domestically. Investments must be made in research and development to do this. Public-private collaborations should be promoted as the private sector also has a significant stake.
2. A plan for thwarting China's expanding cyber capabilities is required. Along with the collaboration of the three services and their effective use on the battlefield, the combined employment of conventional weapons and cyber weapons should be investigated.
3. With the number of users growing quickly, it is important to educate the public about cybercrimes and the need of fostering digital literacy.

NATIONAL CYBER SECURITY STRATEGY

- The Data Security Council of India (DSCI), under the direction of Lt. General Rajesh Pant, conceptualised the National Cyber Security Strategy in 2020. The paper concentrated on 21 areas to guarantee an India-specific cyberspace that is safe, secure, trustworthy, robust, and dynamic.
- However, the Centre has not yet put the National Cyber Security Strategy into practise despite an increase in assaults on India's networks.
- Cyber Warfare Offensives: The US is only one of several nations that has made considerable financial investments in creating not only attack defences but also the capacity to launch destructive cyber warfare offensives.

- The US, China, Russia, Israel, and the United Kingdom are thought to have the most advanced cyberwarfare capabilities. Critical infrastructure, such as financial services, banks, power, manufacturing, nuclear power plants, etc., is rapidly becoming digitalized.

Fig 3: National Cyber security strategy goals

- The proliferation of access points into the internet and the growing interconnection of sectors, which might continue to rise with the deployment of 5G, make it particularly important for protecting critical industries.
- According to data submitted to and maintained by the Indian Computer Emergency Response Team, there were 6.97 lakh cyber security incidents reported in the first eight months of 2020, almost equal to the preceding four years combined (CERT-In).

IV. OBJECTIVES

1. Large-scale digitalization of public services: Put security first in the planning phases of all digitalization projects. Enhancing institutional capacity for core device certification, rating, assessment, and evaluation and timely disclosure of occurrences and vulnerabilities.
2. Integrated Circuits (ICT) and electronics goods' supply chains are tracked and mapped as part of supply chain security. Utilising the nation's technological, strategic, and tactical expertise in semiconductor design internationally.
3. Protection of Critical Information Infrastructure: Including Security in Supervisory Control and Data Acquisition (SCADA)maintaining a vulnerability database. Establishing and monitoring a sector-wide baseline for security at the overall level and establishing threat readiness audit requirements and creating cyber-insurance products.
4. Digital payments: mapping and modelling of the platforms and devices used, the supply chain, the parties involved in the transactions, the payment flows, the interfaces, and the data interchange.

State-level cybersecurity policies must be created, funding must be set aside specifically for this purpose, digitalization plans must pass critical inspection, and security architecture, operations, and governance guidelines must be followed.

V. RECOMMENDATIONS AND STEPS TAKEN BY GOVERNMENT

1. Budgetary Provisions: It has been suggested that a minimum of 0.25 percent of the yearly budget, which can be increased to 1 percent, be set aside for cyber security.

- 15-20% of the IT/technology budget for individual ministries and agencies should be set aside for cyber security.
- Additionally, it recommends creating a Fund of Funds for cybersecurity and giving central funds to states so they may develop their expertise in the area.

2.Research, innovation, skill-building, and technology development are all recommended in the study, along with investments in ICT modernization and digitization, the creation of an outcome-based cyber security agenda, and funding for deep-tech cyber security innovation.

- Additionally, DSCI advises establishing "cyber security services" using personnel drawn from the Indian Engineering Services.

3.Crisis Management: DSCI advises conducting cyber security drills that contain realistic situations and all of its implications in order to be adequately prepared to handle a crisis.

- Cyber Insurance: Because it is a new area of study, cyber insurance needs actuarial science to handle cyber security risks in technological and business contexts and to estimate threat exposures.
- Cyber Diplomacy: India's international relations are greatly influenced by cyber diplomacy. Therefore, initiatives, exchanges, and industrial assistance are required to maintain the cyber security preparation of important regional blocks like the Shanghai

Cooperation Organization (SCO) and the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC).

- The government should promote India's reputation as a trustworthy participant in cyber security and appoint "Cyber envoys" to important nations and areas in order to advance better diplomacy.

4.Cybercrime Investigation: The research suggests reducing the strain on the legal system by passing rules to deal with spamming and false news in light of the rise in cybercrime throughout the world.

- It also advises developing a five-year strategy that accounts for potential technological change, establishing special courts to handle cybercrimes, and clearing the backlog of cybercrime.
- In addition, DSCI advises agencies to undergo sophisticated forensic training to stay current in the era of AI/ML, Blockchain, IoT, Cloud, and Automation.

VI. INTIATIVES TAKEN

The Indian Cyber Crime Coordination Centre (I4C) was recently inaugurated by the government. National Cyber Crime Reporting Portal has also been launched pan India.

A) Indian Cyber Crime Coordination Centre

The scheme to set up I4C was approved in October 2018, to deal with all types of cybercrimes in a comprehensive and coordinated manner.

B)National Critical Information Infrastructure Protection Centre (NCIIPC).

Critical Information Infrastructure (CII) is defined as "those computer resources, the loss of which shall have crippling impact on national security, economy, public health or safety" by the Information Technology Act, 2000.

C) Information Technology Act, 2000

All actions involving the use of computer resources in India are governed by the Information Technology (IT) Act, 2000, as revised from time to time.

- It applies to all "intermediaries" involved in the usage of computer systems and electronic data.

D) Indian Cyber Crime Coordination Centre (I4C).

- To serve as a hub for the battle against cybercrime
- Determine the research issues and requirements of LEAs, and then engage in R&D activities to create new technologies and forensic tools in cooperation with academic institutions and research centres both domestically and internationally.
- Make changes to cyber regulations as necessary to keep up with rapidly evolving technology and international collaboration.
- In cooperation with the relevant nodal authority in MHA, coordinate all actions relating to the execution of MLATs (Mutual Legal Assistance Treaties) with other nations regarding cybercrimes.

VII. EXPLICIT SUGGESTIONS

1) The Government of India must create the National Mission of Cyber Forensics in order to hasten the prosecution of cyber terrorists and cybercriminals. It is important to emphasise implementation and development, and both the public and commercial sectors should get the appropriate training. Periodic cyber audits are required for all networking enterprises.
2) It must be guaranteed that the protection of privacy and human rights is an essential component of the global cyber security requirements.
3) Cyber operations require an ability to do collection, exploitation, and response. Academic institutions train the workforce that will staff the execution, management, and monitoring of cyber operations.

VIII. CONCLUSION

If a cybercrime involves a bot attack, it may cause havoc online. It is crucial to track down the perpetrator as soon as possible and preserve original evidence in cybercrime investigations because of how quickly crimes are committed and how much of an impact they have as well as how readily electronic evidence may be manipulated or is volatile. Due to the availability of several methods for hiding one's identity, such as steganography, onion routing, or other conceal IP techniques, tracking the perpetrator in cybercrime situations may also be more challenging.

Cyberspace is being exploited more and more quickly as a result of the significant increase in demand for it. Nowadays, a larger number of terrorist attacks on major information centres make cyber security a very significant and crucial issue. Current laws are ineffective at combating cyber dangers, thus there is a strong need to amend them. These laws should be reviewed promptly and modified in accordance with improvements to Indian society.

IX. **FUTURE SCOPE**

Finally, a cultural and institutional challenge to academics is necessary for the future of cyber operations research and education. Many of the resources required for success, in our opinion, are already available. The assignment is to determine, organise, and structure the existing intellectual capacity for each university.Create cyber-relevant courses that are cohesively developed between, for instance, public policy courses, business school information and risk management courses, and other relevant course offerings. Then, advertise these courses to students to increase their chances of receiving a quality education.

REFERENCES

[1] A Survey of Cybercrime by Zhicheng Yang; retrieved from http://www.cse.wustl.edu/~jain/cse571-11/ftp/crime

[2] IntroductiontoIndianCyberLawbyRohasNagpal,AsianSchoolofCyberLaw;retrievedfromhttp://www.cccindia.co/corecentre/Database/Docs/DocFiles/india_cyber.pdf

[3] United States Department of Justice, editor. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 2002.

[4] Paul Ohm, Douglas Sicker, and Dirk Grunwald. Legal Issues Surrounding Monitoring (Invited Paper). In Internet Measurement Conference, October 2007.

[5] Yang and J. Lui. Security adoption in heterogenous networks: The influence of cyber-insurance market. In IFIP Networking , 2012

[6] M. Lelarge and J. Bolot. Economic incentives to increase security in the internet: The case for insurance. In IEEE INFOCOM , 2009

[7] A. Khouzani, S. Sen, and N. Shroff. An economic analysis of regulatingsecurity investments in the internet. In IEEE INFOCOM , 2013

[8] Cui Jing, Liu Guangzhong, the basics of computer network [J]. Tsinghua University Press,2010.07.01.

[9] Geer, Dan. A New Cybersecurity Research Agenda (In Three Minutes or Less). https://threatpost.com/en_us/blogs/new-cybersecurity-researchagenda-three-minutes-or-less-110711