CYBER SECURITY STRATEGY: POLICY BRIEF RECOMMENDATIONS

Over the last decade, the cyber intrusions and attacks have increased tremendously causing high implications and repercussions in terms of breach of sensitive personal and business information, disruptions of critical operations, and imposing high costs on the economy of our country.[i]

Owing to the large demography our nation withholds, it is imperative to safeguard the national and public interest in today's technocratic society. Subsequently, the cyber world has posed significant new challenges that differ from the conventional challenges. The emerging challenges are borderless in nature. In the given scenario, safeguarding our cyber security architecture is indeed the need of the hour. India is among the top five targeted countries to have received the highest number of cyber-attacks. T

This highlights the importance of cyber security measures in the current times. Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Therefore, steps to protect the sensitive business and personnel information becomes imperative for the country.

However, the most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security.

Current Threat landscape

The present cyber threat landscape poses significant challenges due to rapid technological developments such as Botnets, Dark Web, DDoS attack, Cloud Computing, Artificial Intelligence, Internet of Things, 5G etc. Owing to the inherent vulnerabilities that come along in the realm of cyberspace, it becomes imperative for a diverse country like India to strengthen the cyber ecosystem and infrastructure vis-à-vis its regulatory bodies and Law Enforcement Agencies (LEAs).[ii]

New challenges include data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime & cyber terrorism, and so on. Threats from organised cybercriminal groups, technological cold wars, and increasing state sponsored cyber-attacks have also emerged.

The current legal framework dealing with cyber-security is not centralized. Different agencies are responsible for various aspects of cyber-security.

We have different cyber security framework for their regulated entities. However, none of the frameworks talk about inter-regulator coordination or integrated approach to handle cybercrime. Thus, we need a unified cyber security framework across various regulators.

IIPA in its Third-Party Evaluation of I4C of MHA found out that India lacks a robust cyber-security policy. In the light of the growing cyber-attacks, India must come to the terms to have its own cyber-security policy keeping in line with the developed countries of the world. Cyber security is important because it encompasses everything that relates to protecting our data from cyber attackers who want to steal this information and use it to cause harm. This can be sensitive data, governmental and industry information, personal information, personally identifiable information (PII), intellectual property, and protected health information (PHI). IIPA suggested some recommendations to widen up the scope of cybersecurity in India due to the very fact that the country has witnessed thousands of cyber-attacks on various institutions and organisations. IIPA underlined in its study the need of developing a cohesive national cybersecurity strategy with a portfolio of initiatives, among them protecting the critical infrastructure of the country, mobilizing the response to cyber incidents, defining cybersecurity standards, improving the cyber awareness of citizens, and a taskforce to combat cyber-attacks.

Suggestions

1. Centre-State Coordination on Cybercrime:

To effectively implement the Joint platform mechanism that has been constituted to combat cybercrime threats and attacks, an integrated approach on both Centre and State level may be implemented. The center-state coordination could be strengthened by establishing a one nodal agency at the Centre with its subcomponents replicated at the state level. Currently, the cyber security system in the country is being operated across many different agencies and LEAs which cause conflict of interests and hinder the investigation process. Establishment of an analogous centralized system at both Centre and state level with uniform rules and framework will facilitate the joint identification, prioritization, preparation, and initiation of multi-jurisdictional action against cybercrimes.

2. Centralized Framework for Effective Inter-stakeholder Coordination:

This is in support of the above recommendation. Since the current cyber security practice involves dealing with different agencies at different locations, the absence of a well-defined framework that talks about inter-coordination and an integrated approach for handling cybercrime, creates procedural delays and prevents timely resolving of the reported cases.

This highlights a need to strengthen the inter-ministerial and inter-agency coordination for cyberspace security. Therefore, it is suggested that Centre may have a single authority or agency responsible for the entire spectrum of defensive cyber operations in the country, the idea is to ensure better coordination and functioning amongst inter -ministerial and departments.

3. Pre-preparedness against new set of cyber threats:

With the technology advancement and the data connectivity across the globe, cyber landscape is facing increasing challenges of cyber threats related to Malware, Dark Web, Network Security, Cloud Computing, Artificial Intelligence, Internet of Things, and Financial Frauds etc. It is recommended that defensive capabilities be improved upon by carrying out proactive risk assessment and vulnerability management. Indigenous capabilities need to be developed in terms of critical infrastructure protection. There is also a need to foster more startups, innovations, incubation centers and carry out extensive R&D activities on cyber defensive capabilities in the country.

4. Categorization of Cyber-attacks on the NCRP portal:

The NCRP portal is a milestone step in the digital arena which allows cyber victims to report incidents immediately therefore helping LEAs in taking timely action. The option of "Learn about cybercrimes" on the portal is also a good medium of spreading cybercrime awareness across the country. However, the listing of cybercrimes on the portal lacks a comprehensive overview of the categories of cybercrimes prevalent across the country. Since the world of IT is ever evolving; the forms and sources of crimes also change accordingly. Therefore, it is imperative that the list of cybercrimes be re-structured on the basis of different types of crimes and how they are carried out. New additions, as and when required, should also be added so that users of the portal find it easier to report the crime.

This may be achieved, e.g., by categorizing online payments/financial transactions linked like ATM pin; UPI frauds; and Cryptocurrency related crimes under one category, namely, "Online Financial Frauds". Similarly, social media crimes like burglary via social networking; Social engineering and phishing; Cyber-stalking; Cyber-casing, and Cyber bullying etc. be clubbed under the heading, "Social Media Frauds".

This step will also enable the government to easily acknowledge the new range of cyber threats linked to Artificial Intelligence (Deep fakes; tailored phishing; large-scale blackmail; AI-authored fake news; data poisoning; autonomous attack drones; denial of access to online activities; tricking face recognition; manipulating

financial or stock markets; Burglar bots; AI-authored fake reviews; AI-assisted stalking; and forgery of content such as art or music.) More categories of cybercrimes could be added related to Cloud services; IoT; Cyber terrorism; Malicious threats; and Website defacement, etc.

5. Harnessing Predictive Analytics Technique in Cyber Security:

Today, in a cyberspace that operates like a warzone, cyber security requires an ever more proactive approach, and the historical and real time data need to be analysed to identify patterns and detect anomalies in real time basis. There is a need to employ innovative and sophisticated techniques like predictive analytics which uses self-learning analysis and detection techniques to monitor network activity and report real-time data breaches. Predictive analytics is the use of data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on past data.

The predictive analytics works like a radar by discovering a data breach before it even happens. Like a radar that shows the enemy approaching, it determines when and where future cyber-attacks may occur. This allows organizations to detect what is likely to happen before anything affects the security of the organization's physical infrastructure, human capital, or intellectual property.

It is, therefore, suggested that predictive analytics may be integrated with PRATIMAAN platform and TAU to figure out and learn about the threat pattern, behavioral pattern, and the country of origin based on historical and real time data. This will further assist in risk and vulnerability assessment and allow authorities to be proactive in their approach.

6. Supply Chain Cyber Security - carry out Vendor Risk Management:

Supply chains present a weak link for cybersecurity because organizations cannot always control the security measures taken by supply chain partners. This can create opportunities for cybercriminals to attack an organization by first infiltrating a weak supply chain partner. Cybercriminals will look for every vulnerability to attack an organization, so it is essential to address every gap, down to the last link in the supply chain.

Cybercriminals may use a vendor's website to host malware. Therefore, it is suggested to carry out vendor risk management by reviewing internal and external security procedures of the vendors before fully integrating them into the internal infrastructures. The essential elements of a vendor risk management program include risk ranking vendors, developing clear policies which vendors are expected to adhere to, making conditions explicit within contracts, and establishing a program to verify the performance of vendors.

Where possible, government should mandate suppliers to adhere to processes and protocols that minimize the likelihood of cyber-attacks. A written agreement should require vendors to provide timely notification of any internal security incidents as well as periodic security reports to regularly ascertain their security status.

7. Reduce Third-party dependency:

The Covid-19 pandemic brought the whole world to face a new set of challenges. One of the most critical challenge was the transformation of almost all economic, business or work activities from physical realm to digital realm. In this process, many countries had to depend upon third party applications and software's. India being one of the major hub of IT sector also underwent the same process. However, the third-party apps posed security threats, as reports of privacy breaches and data theft started emerging. Therefore, it becomes imperative to work on indigenous technology platforms and encourage Indian industries to come up with India-specific technology solutions.

8. Integration of e-Court Services for Cybercrime Cases:

In the NCRP portal there is already provision of repository of court cases related to cybercrime cases and judgments. Integration of e-Court Services with the platform will aid in faster resolving of the registered cybercrime cases and the judgments of the same, then, may be used as references in future judicial proceedings.

Furthermore, integration of e-court services will clear the pre-existing log of cases and bolster the process of proactive identification of cyber threats and organized criminal groups for future readiness.

9. Involvement of NGOs and Women Empowerment in Cyber Safety Programmes:

To strengthen the cyber ecosystem at large it is suggested to increase the involvement of NGOs wherein programmes on cyber safety and security, participation of women will also escalate. It is therefore recommended to increase the strength of NGOs for women and holistic empowerment at large.

10. Capacity Building at Block Level (emphasis being on Rural India):

To spread awareness among the mass citizens, broadcasting can be done with the help of All India Radio (AIR), Doordarshan (DD) that will enable in attaining mass outreach on areas related to awareness of cyber security and safety. For the masses living in the rural India, awareness program can be carried with the help of Block Development Officers and Panchayats. In addition to this, capacity building can be bolstered by incorporation of a course on cyber safety in educational curriculum at initial levels of education (primary and secondary level) of education.

11. Institutional Repository and Center of Excellence (CoE):

It is suggested to lay emphasis on establishing a sound institutional knowledge repository of cyber security and measures and other remedial initiatives. This may be achieved by bringing together cyber experts from across the industry, academia, and other institutions under one ceiling and use their knowledge and skill set for a better cyber secured environment of the country. In support of this, it is further suggested to develop a Centre of Excellence (CoE) for the study of best practices in cyber security and institutionalize the development, sharing, collation and implementation of best practices across country. This will also progressively develop the skilled and trained personnel on matters related to cyber security.

12. Standardization of Cyber Safety Programmes:

To standardize the cyber safety programmes, we may opt for global certification in the significant areas of information security domain by benchmarking against the best global practices. This will enhance the capacity building standard and knowledge base of global recognition. The concept of "Cyber Belt" should be given consideration similar to six sigma global certification courses to validate the knowledge base and skills are acquired for obtaining a certification. The cyber belt can be classified into different levels based on degree and weightage of particular skill sets attached with the certificate.

13. Contribution in Global Dialogues on Cyber Norms and Laws:

Regular consultation with the identified groups such as Government agencies, academia, NGOs, private players, and technical companies at both, national and international level should be given importance in a regular manner. The Intersection of law, policy and strategy in the international cyber security dialogue is important to laid emphasis on more systematic and structured way of formulating national strategy pertaining to cyber norms.

14. Competency Framework:

A Competency framework can be designed and implemented for building adequate cyber security workforce. The competency framework will assess the technical skills set requirement, identifying current existing gaps, define major competency areas across the components with defined roles and devise strategies and programme for building and train the required capacity.

15. Lawful Interception Capabilities:

Emphasis may be given to build lawful interception capabilities to provide balance between national security and economic growth by establishing a competency center for performing research in the same area. More

research work and capabilities are required to strengthen encrypted communication on a real time basis and also build trust among the different stakeholders in matters related to cyber security.

16. Role of IT Infrastructure Management:

IT infrastructure management involves a variety of aspects, including the management of policies, devices, processes, sensitive information, and workforces. Managing all of these aspects is no easy feat, resulting in stress when handling IT matters or scaling back an IT infrastructure. Taking control of an organization's IT environment is an essential component of operations. Additionally, proactively monitoring IT infrastructure allows other changes, such as inadequate storage capacities or outdated technology, to be detected in advance. Awareness of these types of situations enables officials to take the necessary steps to resolve them.

17. Development of a Comprehensive National-level Policy:

There is a need to review the 2013 national cyber security policy and other existing cyber security frameworks in the country. A new comprehensive national level policy needs to be developed with corrective steps towards strengthening the resilience of cyber security infrastructure and defense capabilities. The new policy should consider the latest technological innovations and its related forms of sophisticated cyber threats that are emerging in the cyber space.

18. Developing effective Public Private Partnership (PPP) Model:

It is imperative that Government and industry cannot overcome the cyber security challenge in isolation, therefore there is a need to work together in a trusted and collaborative environment, leveraging each other's strength to strengthen the cyber security systems of the country. Incorporation of Public Private Partnerships in the cyber field has proven to create effective solutions for both industry and government. Therefore, it is important for the Indian government to work out best suited PPP for improving cyber defence system in the country.

According to a study conducted by European Union Agency for Network and Information Security (ENISA), there are various successful cooperative models for effective PPPs in the field of cyber security. Based on the study, following types of PPP models have been identified:

- Institutional PPPs- In this type of PPP, the whole institution works under a PPP framework. Common means of cooperation are working groups, rapid-response groups, and long-term communities.

The goal is to secure critical infrastructure in general, and cyber threats are considered important elements in the threat landscape.

- Goal-oriented PPPs- this type of PPP is usually built, when cybersecurity is understood as a distinguished and specific task/objective of the economy, which needs extra support and interest from the government. This type of PPP is focused on providing strategic solutions, supporting the IT market, and creating a framework for cybersecurity development in the country. There is usually a platform, or a council established which brings private and public sector together to exchange knowledge and good practices. The objective for the members is to focus around one subject or a specific goal.

- Service outsourcing PPPs- This model of PPP is intricately linked to the critical infrastructure protection. It delivers services which are supporting critical infrastructure operators and raises the overall cybersecurity level in critical sectors. These PPPs can actually be considered as third parties for outsourcing services which address the need of industry and support the government in policy making process (e.g., policy implementation, drafting of national cybersecurity strategies etc.).

- Hybrid PPPs - Hybrid PPP is actually a combination of outsourcing cybersecurity services and institutional PPP. It occurs when the government does not have enough resources to deliver necessary cybersecurity solutions on a national level and starts cooperation with the private entity which has the appropriate expertise and can deliver these solutions.

Some of the possible areas of effective implementation of PPPs are:

- Capacity Building in the Area of Cyber Crime and Cyber Forensics
- Developing Security Expertise for Protection of CII
- Developing Approaches, Best Practices and Standards
- Bringing Innovation through R&D
- Technology Support

19. Enhance the Technical Manpower:

It is suggested to increase the employment of technical manpower in all the sub-components. It is also suggested that component-wise delegation of trained and professional workforce take place and the ratio of manpower in LEAs to combat cyber-attacks should be increased for all the components.

In support to the suggestion, a well-established accreditation and certification system for various training institutes, organizations and individuals working in the field of cybercrime should also be laid emphasis on. It will ensure a rise in trained workforce and cyber experts in the future.

Best Practices

Cyber-attacks are increasingly becoming frequent, sophisticated, and impactful. Globally, we have seen a surge in the number of cyber incidents, such as ransomware, cyber theft, banking fraud, cyber espionage, and disruptions to Internet services. Attacks on systems that run utility plants, transportation networks, hospitals and other essential services are also becoming more frequent. Successful attacks result in disruptions which could cripple economies, and lead to loss of life. Experts argue that the advent of the Internet of Things (IoT) will further increase the attack surface. Left unchecked, malicious entities can find more ways to launch attacks steal data and make cyberspace dangerous for all. The result is a cyberspace that is hostile, and where basic interactions and transactions cannot be trusted. It is important, therefore, to stay ahead of the curve and adopt

The Privacy Protection Authority (PPA) is the primary regulator for matters relating to privacy and data security, it conducts criminal investigations, administrative investigations and audits, publishes guidelines, conducts research and initiates new regulations; regulates and enforces data privacy and protection laws and regulations across all sectors.

state of the art facilities. Some of the best cyber warfare practices which are used by various countries across the world are mentioned below:

A. United States of America

The United States of America is one of the nations that is encountering a huge amount of cyber-attacks every year. In response to that US has been very much successful in enacting legislation on cybersecurity.[iii]

Though USA has not adopted any international cyber security standards into law, the National Institute of Standards and Technology (NIST)[iv] has created a voluntary 'Cyber security Framework', which provides a risk-based approach to cyber security and references various national and international standards. It catalogues best practices for identifying, protecting, detecting, responding to, and recovering from cyber security incidents by creating adaptable benchmarks and recommendations. Moreover, the country has the Federal Risk and Authorization Management Program (FedRAMP), a government-wide programme that aims at continuous monitoring for companies providing cloud services to federal civilian agencies.[v]

B. United Kingdom

In UK, the regulatory authorities primarily responsible for enforcing cybersecurity rules are the National Cyber Crime Unit (NCCU), a dedicated unit within the NCA and the Information Commissioner's Office (ICO), and where national security is at risk, the UK's security and intelligence agencies are involved. In addition to the NCCU and the ICO, professional regulators such as the FCA and the Solicitors Regulation Authority oversee cybersecurity in particular sectors.[vi]

In 2016, the UK government also initiated the creation of effective firewalls and the use of the latest supported application versions and patches. Further, the country encourages talent from the private sector to work with government in enhancing cybersecurity operations.[vii]

C. Israel

Israel's cyber defence framework is considered one of the best globally. Israel was one of the first countries to recognize the need to protect the national vital digital systems, and in February 2002 the Israeli government passed a resolution assigning the Israel's National Information Security Agency with the responsibility for protecting those systems.[viii]

The Privacy Protection Authority (PPA) is the primary regulator for matters relating to privacy and data security, it conducts criminal investigations, administrative investigations and audits, publishes guidelines, conducts research and initiates new regulations; regulates and enforces data privacy and protection laws and regulations across all sectors, private and public, and may initiate enforcement actions based on information it receives from sources that can include other regulators and public bodies and the media, as well as complaints of aggrieved citizens.

Further, the National Cyber Security Authority (NCSA), set up in 2015, has overall national responsibility for cyber defence, oversees cyber defence actions so as to provide a comprehensive response against cyberattacks including dealing with threats and events in real time, operates an assistance centre - a Cyber Event Readiness Team (CERT), for dealing with cyber threats in order to strengthen resilience of organizations and sectors in the economy. NCSA combines security and operational characteristics with civil ones, to synergistically lead, together with all other State security organizations, the defence efforts against cyber-attacks.

D. Estonia

Estonia is the country that has learned lessons from its past and came out strong. Estonia has been at the centre of global cybersecurity discussions and action since at least 2008. That year saw the establishment of the NATO Cooperative Cyber Defence Centre of Excellence. The Centre is best known for its *Tallinn Manual* process, a non-binding, academic study on how international law applies to cyber conflicts and cyber warfare.

Estonia has also enacted its third generation National Cybersecurity Strategy (2019-2022). The focus is on the global nature of threats in cyberspace and the need for international, multilateral action. It supports effective cooperation between state, academia, and the private sector's key partners. To this end, Estonia will launch a cluster that facilitates both domestic and international cooperation.[ix]

E. South Korea

South Korea is synonymous for establishing its trademark as the world's most connected nation with the fastest Internet and a diverse digital economy, however, it is faced with cyber-attacks that are growing day by day.[x] Though the country in past had held talks with the EU to forge a partnership on cybersecurity, it is the reluctance of South Korea to join the Budapest Convention that has made the road of alliance bumpier. India can learn a great deal from South Korea in terms of implementation of a strong cybersecurity policy. South Korea has a National Cybersecurity Center that empowers Ministry of National Defence, Central Administrative Agencies, and Ministry of Science, ICT & Future Planning to engage public sector, private sector and military in mitigating cyber-attacks.[xi]

However, the fate of world lies in close collaboration amongst countries to work on a similar track of cybersecurity by engaging in dialogue with each other on a global platform like the UN which in turn can give much needed impetus to the Budapest Convention. ■

REFERENCES:

1. Steve Ranger, (2015), inside the secret digital arms race: Facing the threat of a global cyberwar. [online] Available from: http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/.
2. The cyber raiders hitting Estonia, [online] Available from: http://news.bbc.co.uk/2/hi/europe/6665195.stm.
3. https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/
4. https://eucyberdirect.eu/content_research/cyber-resilience-and-diplomacy-in-the-republic-of-korea/
5. https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/dr-so-jeong-kim-national-security-research-institute-s-korea-cyber-security-in-the-republic-of-south-korea
6. https://www.gov.il/en/departments/israel_national_cyber_directorate
7. https://www.ncsc.gov.uk/
8. https://www.cisa.gov/cybersecurity

9. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
10. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
11. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-07.pdf?ver=2017-06-16-115052-740
12. https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp
13. https://cybervolunteer.mha.gov.in/webform/Volunteer_AuthoLogin.aspx
14. https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division
15. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-07.pdf?ver=2017-06-16-115052-740
16. https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

i. https://www.cisa.gov/cybersecurity
ii. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
iii. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
iv. https://www.ncsc.gov.uk/
v. https://www.ncsc.gov.uk/
vi. https://www.gov.il/en/departments/israel_national_cyber_directorate
vii. https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/
viii. https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/dr-so-jeong-kim-national-security-research-institute-s-korea-cyber-security-in-the-republic-of-south-korea
ix. https://eucyberdirect.eu/content_research/cyber-resilience-and-diplomacy-in-the-republic-of-korea/

AUTHORS

Dr. Surabhi Pandey

(The author is the Assistant Professor, ICT & e- Governance, Indian Institute of Public Administration)

Yumna Jamal

(The author is Research officer in Indian Institute of Public Administration)