DE JURE NEXUS LAW JOURNAL

Author:

Huzaifa Hasan

Symbiosis Law School, Noida

1st Year, BBA LL.B.

NATIONAL SECURITY AND CYBER POLICIES

Abstract:

This entry on the topic "National Security and Cyber Policies" aims to bring into highlight the importance of cyber security policies for the enhanced posture of the nation's security in the cyber space. Due to the technological advancements, internet is a pool for every individual, and it is extensively being used by the government in different tasks such as operations of military, data storage, critical information infrastructure, video and audio conferences of delegates and what not, but due to the dearth of appropriate cyber security policies, it is clearly difficult to draw boundaries among these groups. Cyber space appears to be more perplexing in the foreseeable future, and a need of an enhanced cyber policy is axiomatic, hence ***DeitY*** *launched its National Cyber Security Policy in 2013.*

Therefore, this article is an attempt to throw spotlight on the efforts that government make to diminish cyber unhygienic activities, hacktivism and what objectives and strategies government has envisaged to deal with the cyber security of the Information and Communication Technology (ICT).

Keywords: *Cyber space, critical information infrastructure, data storage, hacktivism, National Cyber Security Policy, DeitY (Department of Electronics and Information Technology), ICT.*

Introduction

As a country we keep on taking on conflicts to safeguard our power, jurisdiction and privacy from nosy and unknown dangers ruling in the field of the internet. The dominating threats in the arena of the cyber space can only be dealt when there is a comprehensive and expressed cyber security policy passed by the government. Therefore, in 2013 government of India passed the National

Cyber Security Policy providing a framework for dealing with the rapidly increasing dilemma in cyber sphere. The protection of sensitive data and the identity if people is a matter of outmost concern for a nation, and it is nation's responsibility to provide a hygienic environment for the functioning of cyber activities without the fear of breach. This article enables the reader to understand the quandary in cyberspace and governments' measures curtail them.

Threats to National Security in Cyber sphere

The only means to interact with the other country for a country is cyberspace and every nation is directly connected with every other nation by the means of internet. This fight against the hollowness and the nuisance sprinkled by the cyber terrorists is becoming typical as more and more crimes are increasingly growing.

"A countries system, which supports the country's critical defense and intelligence, should be secure regardless their place. Today internet is weapon for political, economic and military espionage. In the past, many cyber-attacks have been seen like:"

- As per the Pentagon, that is the United States' Defense department, over three million illegal scans for invaders attempting to get official figures are detected every year.
- Chinese hackers are reported to have attacked ***Indian vaccine*** manufacturers "***Serum Institute and Bharat Biotech***" in order to get knowledge on the Corona Virus vaccine.
- According to several cyber-security specialists, China and North Korea, among other nations, are teaching hackers how to utilize cyber warfare methods.
- According to reports, Chinese military cyber-attacks infiltrated the Pentagon, the German Chancellery, and England's Whitehall in 2007.
- In the late spring of 2007, a solitary assault debilitated 1500 PCs of the Pentagon[1]

The aforementioned examples are apparent that how can a nation's security go on a toss in chunk of seconds and it can make the whole network connection of the victim country paralyzed. The softwares that were used in attacking these countries were more resourced and powerful than the ones seen in usual or ordinary attacks. Countries which have fewer monitoring techniques and less sophisticated arena can be a breeding ground for the attackers, as traditional methods are not enough to safeguard a country against giant attacks of these sort.

The Need for a Comprehensive Cyber Security Policy

Given the country's growing IT sector, lofty ambitions for rapid social transformation and shared prosperity, and India's notable role in the global IT market, putting the right kind of emphasis on creating a secure computing environment with adequate faith and credibility in online transactions, software, assistance, gadgets, and connections has become one of the country's most pressing

[1] Patel, K., 2021. *National Security Threats in Cyberspace*. [online] ResearchGate. Available at: <https://www.researchgate.net/publication/352507748_National_Security_Threats_in_Cyberspace> [Accessed 21 February 2022].

priorities. Such a focus allows the nation to develop a proper cyber security eco-system that is compatible with the global smart environment.[2]

Since cyberattacks and information breaks might be costly, online protection rules are fundamental. Employees, then again, are regularly the failure points in a company's security. Employees share username and password, click on malware and mong other things, they send unsolicited attachments, utilize unapproved cloud programs, and neglect to encrypt important information. "***According to Grand Theft Data, a McAfee report on data exfiltration, people inside organizations are responsible for 43 percent of data loss, half of which is unintentional.***" Enhanced digital protection strategies can help representatives and consultants in seeing step by step instructions to keep information and applications secure.[3]

Cybersecurity policies and strategies are additionally basic to the public picture and validity of an association and country's security. Clients, accomplices, investors, and forthcoming representatives need proof that the association can safeguard its touchy information. Without a cybersecurity policy, an association will be unable to give such proof.[4]

Objectives of India's National Cyber Security Policy 2013

There are 14 objectives that are enshrined by the DeitY (Department of electronics and Information Technology) in the National Cyber Security and some of them are jotted down below:

i) To build a safe cyber environment in the nation, increase trust and confidence in IT systems and transactions in cyberspace, and increase IT adoption throughout the economy.

ii) By means of conformity assessment, build an affirmation system for the formulation of policies on security, as well as enablement and promotion measures to ensure compliance with international security standards and best practices (product, process, technology & people).[5]

iii) To provide a secure cyberspace environment, the regulatory framework must be strengthened.

iv) By developing foundation for testing and approval of safety of ICT goods and services, the visibility of their integrity would be improved.

v) To provide information security throughout the processing, management, storage, and transit of data in order to preserve citizen privacy and reduce losses incurred as a result of cybercrime or data theft.

[2] MeitY. 2022. *National Cyber Security Policy (draft v1)*. [online] Available at: <https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf> [Accessed 21 February 2022].

[3] Mcafee.com. 2022. *How Cybersecurity Policies and Procedures Protect Against Cyberattacks | McAfee*. [online] Available at: <https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html> [Accessed 21 February 2022].

[4] Mcafee.com. 2022. *How Cybersecurity Policies and Procedures Protect Against Cyberattacks | McAfee*. [online] Available at: <https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html> [Accessed 21 February 2022].

[5] En.wikipedia.org. n.d. *National Cyber Security Policy 2013 - Wikipedia*. [online] Available at: <https://en.wikipedia.org/wiki?curid=40617071> [Accessed 22 February 2022].

vi) To improve global collaboration by establishing common understanding and leveraging ties in order to promote the cause of cyberspace and information security. Businesses will get tax breaks if they implement industry-standard security procedures and practices.[6]

Strategies To Bring Down Cybercrimes and Unhygienic Activities:

i) **Creating a secure cyber ecosystem:** It provides that a Nodal agency will be allocated that will exclusively deal with the cyber matters and the private and public organisations will be expected to assign an individual from senior administration as Chief Information Security Officer (CISO) who'll be liable for security drives and endeavours. It'll also require all the organisations to frame cybersecurity policy and an annual budget that will solely be lodged to the cybersecurity.

ii) **Creating an assurance framework:** To encourage adoption of worldwide best practices in information security and compliance and consequently increase cyber security posture. Also, to implement security practices in the risk management and the vulnerable areas to increase the security posture and reduce the chance of interruption.

iii) **Encouraging Open Standards:** To promote usage of open measures to allow coordination and data exchange across various goods or services. To establish a coalition of government and business sector organizations to encourage the open availability of proven and true IT products based on open standards.

There are other numerous strategies enlisted in the government's cyber security policy such as Strengthening the Regulatory framework, making instruments for security danger early admonition, weakness the executives and reaction to security dangers and securing e-governance services.[7]

Summary of Incidents in Cyber Horizon in the Last One Year

January 22:

A Chinese hacker squad hacked major German healthcare and IT businesses. According with German authorities, the hacking into the systems of service suppliers and enterprises was largely an effort to steal intellectual property.

January 22:

A Belarusian cyber espionage gang infiltrated the infrastructure of nation's Belarusian Railway. The gang seized the most of hosts of Railway and deleted data housed on a backup server, potentially to hamper Russian army moves around the nation.[8]

December 2021:

[6] MeitY. 2022. *National Cyber Security Policy (draft v1)*. [online] Available at: <https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf> [Accessed 21 February 2022].

[7] MeitY. 2022. *National Cyber Security Policy (draft v1)*. [online] Available at: <https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf> [Accessed 21 February 2022].

[8] Center for Strategic and International Studies. n.d. *Significant Cyber Incidents | Center for Strategic and International Studies*. [online] Available at: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> [Accessed 21 February 2022].

Hackers were able to tweet from Prime Minister Modi's Twitter account that India has officially recognized bitcoin as legal cash. A fraudulent link advertising a bitcoin giveaway was also included in the Tweet.

November 2021:

After infiltrating a US military contractor, hackers acquired access to workers' social security and driver's license data.

October 2021:

The site of Indonesia's State Cyber and Password Agency, the National Malware Centre, was hijacked by Brazilian attackers. The hackers changed the content of the site and asserted it was in revenge for an Indonesian hack on the Brazilian government's website.[9]

A long perpetual list of incidents will pop up if we start to jot down each and every thing. These above-mentioned incidences are heinous and can enable a reader to notice that how far the malicious acts of the hackers can go. Additionally, when the internet access to one and each has become convenient, it has brought the challenges owing to cybersecurity on a bigger landscape.

Conclusion and Suggestions

As this research have made clear the intricacies in the cybersecurity and how vulnerable networks can possibly be a breeding ground for the cyber terrorists and criminals. Not only this, when the cybersecurity of a country's overarching network is weak, the data of public at large also is at stake and can be breached by attacks like **Denial of Service, SQL Injection, and mere phishing attacks**. These attacks sometimes are of lethal nature that they can cause everything go on a toss and their mitigation is very slow and gradual. Countries like India with a developing infrastructure have a huge amount of people using the internet and its access is so cheap that nearly everyone in India is accruing benefits from internet. According to the data shown by ***Telephone Regulatory Authority of India (TRAI),*** a total of **825.30 million** people were the users of internet in India till March 2021.

While dangers emerging from the internet are notable, ironically at public level, we actually don't have a methodology which spreads out the rules on the best way to handle them. There is no basic fundamental system to safeguard basic data framework and other public resources. ***The National Cyber Security Policy (NCSP)*** released by the Indian Government in 2013, had laid forth a few approaches to battle security hazards from the internet. While eight years have passed, restricted execution has occurred, and our nation stays among the most victimised countries. The absence of an extensive network safety procedure/strategy is prominent and expanding weakness. But there is a ray of hope, before we set out into 2023, India would have been given by the ***Department of Electronics and Information Technology (DeitY)*** a National Policy on Cybersecurity. Be that as

[9] Center for Strategic and International Studies. n.d. *Significant Cyber Incidents | Center for Strategic and International Studies*. [online] Available at: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents> [Accessed 21 February 2022].

it may, in issues of network safety, India must plan and set up a cooperative way to deal with accomplish soundness and security.