To study about the policy response to the cyber-Terrorism

Richa Tiwari[1]*, Dr. Ganesh Dubey[2]

[1] Research Scholar, Jiwaji University

[2] HOD, Institute of Law, Jiwaji University

Abstract - When cyber incidents occur, the government assists potentially impacted entities, analyses the possible impact across key infrastructure, investigates those responsible with law enforcement partners, and coordinates a national response to major cyber catastrophes. To achieve better unity of effort and a whole-of-nation response to cyber events, the Department collaborates closely with other agencies that have complementary cyber responsibilities, as well as private sector and other non-federal owners and operators of vital infrastructure. This article examines the government's response to cyber-attacks and cyber-terrorism.

Keywords - Cyber mission, Cyber attack, Security, NCS Policy

- x -

1. INTRODUCTION

Internet-connected computers and other devices make up the "cyberspace" of information technology networks, databases, resources, and gadgets. As a component of the global cyberspace, cyberspace has no borders. This feature distinguishes cyberspace from other places. The pace of communication and computation is being pushed to new heights by technological advancements. Since the size of cyberspace is inversely proportional to the activities that take place inside it, the Internet's penetration has led to a rapid expansion of the cyberspace. In ways that no one could have predicted, it has changed the global economy and linked people and markets like never before.

The complexity of cyber laws is growing, as is the scope of the concerns they must address. India's economy is becoming more and more international. Every aspect of the internet is technical. There are instances when new technology and new standards put a hurdle in the way of law's genuine dynamic nature, but this is not always the case. As a result, the whole planet now has fresh points of vulnerability and potential for disruption. The perpetrator's identity, motive, and whereabouts of a disruption might be difficult to determine, as the act can take place at any time and from any location. Thus, cyber security concerns represent one of the most severe economic and national security dangers.

Organized criminal gangs, criminal societies, and national and international criminal organizations are major participants in cyber terrorism. There is no one way to stop cyber terrorism, which combines a desire to inflict harm with advances in technology. As a consequence, only a multifaceted response can provide positive outcomes. The word "policy" is derived from the Greek, Sanskrit, and Latin languages, respectively. The Latin politic (State) and the Middle English policies (Government administration) derived from the Greek and Sanskrit roots polis (city-state) and pur (city). All three terms, police and politics, have a same etymological basis for policy. Modern languages like German and Russian utilise only one term to refer to both policy and politics because of this. A policy is a road map for the government to follow in order to accomplish its objectives. An recognised and specific issue is taken into consideration, together with steps taken by the state to prepare for a specific response to it. For example, it envisions how one may go about achieving a certain outcome, whether it's bad or good, and how one can avoid taking action on a particular topic or subject. In most cases, public policy is the result of in-depth research and in-depth examination of the available facts and information. Therefore, it seems to be seen as a superior role that is reserved to the upper echelons of management. The development of a strategy would be impossible without policies. For planning, executing and achieving goals and maintaining actions inside a specified framework of action, they provide important guidelines. The policies so offer meaning and define the objective8... An action taken and followed as beneficial or expedient by a government, party, or other group is referred to as a policy.

Legislation, presidential orders, and other official actions are all examples of policy. It is possible for a policy to be comprehensive or specialized, wide or limited, public or private, simple, complicated or detailed, qualitative or quantitative, discretionary or explicit. Governing activities may be divided into two groups, depending on public policy: those based on the rule of law and those based on the rule of the people.

i. policies that are clear and explicit; and

ii. In the second case, those founded on broadly defined rules that are contradictory in their application.

In the case of legislation, rule, or plan and the like, important public policies are typically made more apparent. The policies are typically imprecise or generic, and are not necessarily compatible with one other. Moreover when the situation is tense, government agencies are frequently forced to act without regard to any set policy. The computer, computer system, and the Internet are all being used to launch coordinated assaults on a state's unity, integrity, and sovereignty. Because acts of cyber terrorism and cyber warfare pose a significant threat to people, property, and the government, it is the responsibility of the state to develop technological and legal strategies to combat the looming threat of terrorism. As a result, a Nation State must have a legislative framework in place to combat cyber terrorism and enhance cyber security. Terrorism in a cyber context includes acts or threats, emotional responses, and the societal consequences of the acts or threats and the actions that follow, all while operating in a quickly changing technical environment that impacts terrorist resources and possibilities. These advancements have had a direct impact on terrorist tactics, targets, and weaponry, prompting increased debate of a new terrorist approach known as "cyber terrorism."

India has always been harsh on terrorism, hence in the case of cyber terrorism, our country has enacted rigorous legislation under Section 66F of the Information Technology Act of 2000. The notion of cyber terrorism, on the other hand, was not in the parental law when T. Vishwanathan authored the first IT Act. However, after evaluating cases of worldwide and national cyber terrorism in 2008, it was determined that a strict provision as well as penalty for cyber terrorism was required. As a result of the Information Technology (Amendment) Act, 2008, Section 66F has been added to the Act.

Punishment for cyber terrorism

(1) Whoever

With the goal to jeopardize India's unity, integrity, security, or sovereignty, or to instil fear in the people or any segment of the people –

(i) Refusing or causing the denial of access to any individual who has been given permission to utilize a computer resource; or

(ii) Trying to breach or gain unauthorized access to a computer resource, or exceeding authorized access; or

(iii) introducing or causing the introduction of any Computer contaminant; and by doing so, causes or is likely to cause death or injury to persons, damage to or destruction of property, or disrupts or is likely to disrupt supplies or services essential to the community's life, or adversely affects the critical information infrastructure specified under section 70, or

(iv) It is punishable by life in jail for anybody who engages in or conspires in acts of cyber terrorism.

2. Vision of the Policy

When it comes to protecting and responding to cyber-attacks, there is no limit. It presents a serious threat to national security, crisis management, and economical growth in the cyberspace, as well. A "world leading," "resilient," and "vigorous" internet is a priority for Japan for all of the above reasons. This will be a part of the social structure.

3. Basic Principles

The following are the foundational tenets for establishing Japan as a cyber security nation:

- **Ensuring free flow of information**

Japan has attempted to offer open and interoperable information in the cyber realm without the need for excessive regulation. As a consequence, new ideas are generated, the economy expands, and social problems are addressed. This year's cyber security plan also assures that information may flow freely. Cyber security threats are also being addressed by the organization.

- **Responding to increasingly serious risks**

In order to make Japan a cyber security nation, it is imperative that the hazards in the country's environment be addressed with urgency. People's trust in cyberspace depends on it being protected from outside threats.

- **Enhancing of risk-based approach**

In previous regulations, Japan has emphasized that everyone involved in the information industry in cyber space should work together to raise awareness of and reduce hazards from cyberspace. So why is it that we now have a new economy that relies on the protection of essential data and information?

- **Acting in partnership based on shared responsibilities**

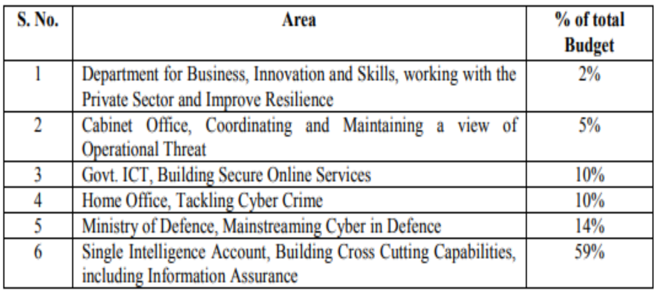
In the computer age of the twenty-first century, almost every organization reaped the advantages of the internet's growth. Japan is no different. Everything that happens in the real world is now dependent on cyberspace. As the dangers of the internet grow, so do our duties in the real world. This means that each player and organization must come up with its own set of information security procedures.

It is everyone's obligation to help maintain "cyberspace sanitary" so that it can react effectively to cyber-attacks, malware infestations, and other threats.

4. Strategy For The Implementation Of 2011 Policy

An impressive £650 million was allocated to the UK government's four-year National Cyber Security Program (NCSP) in the wake of the 2010 Strategic Defence and Security Review.

Table 1: National Cyber Security Programme Investment



S. No.	Area	% of total Budget
1	Department for Business, Innovation and Skills, working with the Private Sector and Improve Resilience	2%
2	Cabinet Office, Coordinating and Maintaining a view of Operational Threat	5%
3	Govt. ICT, Building Secure Online Services	10%
4	Home Office, Tackling Cyber Crime	10%
5	Ministry of Defence, Mainstreaming Cyber in Defence	14%
6	Single Intelligence Account, Building Cross Cutting Capabilities, including Information Assurance	59%

The Cabinet Office's Office of Cyber Security and Information Assurance oversees and coordinates the NCSP on behalf of the federal government. The 10 items listed below have been prioritized throughout the NCSP development process:

i. Focus Approach

Detection and analysis of cyber-threats to key national infrastructure and other systems of national importance is the top priority of the NCSP.

ii. Knowledge Sharing

As part of the strategy, the UK will combine its cyber security expertise in order to develop a truly national response.

iii. Prevent Criminals from Techniques

The United Kingdom will improve its defenses and deterrents against high-end, state-sponsored threats. Make sure that the crooks can't get their hands on any of the new procedures that are being developed.

iv. International Cooperation

The creation of international norms or "rules of the road" in the cyberspace necessitates international collaboration. As a result, the UK will cooperate with other nations to develop trust and prevent misunderstandings.

v. Work on Budapest Convention for Compatible Laws

The Budapest Convention on Cybercrimes has been approved by the United Kingdom. Therefore, the UK will lobby other nations for the adoption and development of regulations that are compatible in order to effectively respond to the cyber threat. Anywhere in the globe, the perpetrators of cybercrime may be brought to justice. There must be no safe haven in this world for them to return.

vi. Maintain Effective Legal Framework

The United Kingdom will maintain a strong legal framework and the tools necessary to root out and apprehend cyber offenders. To do this, it is necessary to make reporting cyber crimes easy from the outset. A system of feedback and public guidance that works well.

vii. Educate Suppliers on Best Practices and Solid Measures

The government plans to develop its own model of best practise in the field of cyber defense. The government's vendors should likewise be held to high standards.

viii. Establish a Cyber Security Corps of Experts

For the best delivery of solutions, the UK will encourage and build an army of qualified cyber security specialists, which will be maintained via research and development.

ix. Prevention and Education of the General Public

Because the best defense is a good offence, the United Kingdom will seek to increase public and corporate understanding of cyber security issues. A recent study found that internet users' carelessness was at blame for more than 80% of all successful cyber-attacks. Antimalware software can be updated often to prevent this problem.

x. Increasing the Chances of Succeeding

As a result of the greatest cyber security goods and services, the UK firm will be able to expand internationally. Also, it will help the UK to be seen as a good site to collaborate in online.

2. UNITED STATES' CYBER SECURITY POLICY

Any precise information on cyber terrorism is doubtful by law enforcement, the CIA, NATO, and the governments of the US and other nations. As of now, they tend to agree that it represents a serious danger. Law enforcement may seem to be concerned about the scale and vicinity of such an assault, despite the fact that the agency is not. NATO, on the other hand, may argue that this danger has not yet materialized to a significant degree. They both agree that terrorists will be able to conduct a well-planned cyber-attack within a year or less, if not months. Politicians and the military are debating whether or not a planned and operational cyberspace is necessary. To combat cyber terrorism, policymakers must develop a framework of rules and prohibitions as soon as possible.

A global race for cyber supremacy has begun. The United States is rapidly expanding its cyber capabilities and weaponry, as well as training and equipping cyber specialists. In order to prevent threats and assaults, a significant degree of auspice and a well-rounded legal framework must be put in place It also provides defense against non-state actors and simplifies the process of dealing with potential dangers, should any arise. The most pressing concern is whether or not the United States can withstand an unbeatable cyber onslaught.

Critical Infrastructure Security Strategy

Since cyber terrorism attacks the vital infrastructure, the policies or plans to defend the critical infrastructure of the states must be taken into consideration. As a result, it is imperative that vital infrastructure be protected to the fullest extent possible from outside influence. In this respect, the US government has taken some action:

i. Cyber-attacks, like any other kind of warfare or assault, must be prepared for in advance. It has been decided to put in place an early detection and warning system.

ii. A new idea for enhancing cyber defense capabilities has evolved for a complete active cyber defense.

iii. ts capacity to find, detect, analyze, and monitor threats to critical infrastructure has been improved via the use of sensors software and intelligence equipment.

iv. An entirely different and completely secure system has been set up to monitor critical infrastructure systems that need a lot of data to be collected.

3. NATIONAL CYBER SECURITY POLICY (NCSP), 2013

As cyber terrorists are able to attack vital infrastructure from anywhere in the globe, it may be difficult to track many of these attacks. Accordingly, it is no exaggeration to argue that cyber terrorism has become an actual threat, and a worldwide discussion is necessary in order to counter the threat of cyber terrorism. In spite of the fact that cyberspace has no physical borders, countries must safeguard their online assets. Legislation, regulations, security programmes and technology, as well as IT staff with the necessary expertise, knowledge and training, may all help accomplish this goal. In this context India has published its National Cyber Security Policy (NCSP), 2013, on July 2, 2013. It is a positive move in the right direction. New and continuing activities and initiatives will be brought together under an umbrella structure that has a unified goal and a comprehensive strategy for implementing it.

Cyber assaults have been classified into many categories, including unauthorised access, virus and spam distribution and identity theft and voyeurism as well as physical privacy breach and cyber terrorism. This amendment helps to punish cyber offenders. Nevertheless, a comprehensive and efficient national cyber security policy was necessary to empower various agencies and provide the greatest degree of cooperation in cyber space to safeguard India. The NCSP, 2013 delivers responses and provides a wide policy framework. The examination of National Cyber Security Policy (NCSP), 2013 is crucial to understand the posture of India in cyber space.

3.1. Vision of National Cyber Security Policy, 2013

Building a safe and resilient cyberspace is the goal of the National Cyber Security Policy, 2013. India's Communications and IT Minister Kapil Sibal claimed that cyber-attacks from both state and non-state actors, as well as corporations and terrorists, were inevitable. A well-protected vital infrastructure, which includes the air defence system and electricity infrastructure, nuclear reactors, and telecommunications, is essential

otherwise, the economy will be at risk. This policy's distinctive attribute is to establish a system to gather information about risks to ICT infrastructure and react to it in a timely manner. Actions that are effective, deterring and practicable are the primary goal.

Over 13,000 cyber assaults occurred in India during the first half of 2011 alone. For the next five years, the government plans to train 5,00,000 qualified cyber security specialists to secure India's vital infrastructure, aid in the investigation and prosecution of cyber crime, and enhance the protection of India's critical infrastructure81.

Policymakers want to establish a nodal agency in the nation to coordinate all aspects of cyber security, including duties and responsibilities, with the goal of creating a more efficient and effective system. Create methods for early warning, vulnerability management, and response to security threats. This strategy is aimed at developing a safe cyber eco-system. In addition, it aims to boost cyber security research and development and eliminate supply chain risks.

4. SECURING E-GOVERNANCE SERVICES

It is imperative that all e-Government projects in the nation follow best practices, business continuity management, and a cyber crisis management strategy, as well as strengthen their security posture, to control and reduce the risk of vulnerability. With PKI88, secure communication and transactions inside the federal government are promoted. Professionals in the field of information security will be needed to make certain that all systems are secure according to industry standards.

i. Critical Information Infrastructure (CII) Security and Resilience

A watertight strategy for safeguarding Critical Information Infrastructure (CII) and integrating it into the business plan at the entity level will be designed and executed in NCSP, 2013 There will be strategies to safeguard information flow at every level of the organisation. Operationalization of the National Critical Information Infrastructure Protection Centre (NCIIPC), the country's central institution for safeguarding the nation's critical information infrastructure.

The danger of a disruption will be minimized by requiring all critical sector organizations to apply best practices in cyber space, business management, and cyber crisis management. All critical infrastructures must be audited on a regular basis to ensure the security of IT products that have been tested and approved.

ii. Cybersecurity Research and Development (R&D)

For a safe cyberspace, it is required to conduct R&D projects for short-term, medium-term, and long-term objectives in order to address all elements of development in the internet age. These programs will cover all areas of system creation, testing, deployment, and maintenance, as well as cutting-edge security technology research and development. All of these projects are aimed at promoting cost-effective goods and cyber security concerns, as well as exporting them to other countries. Both the public and the commercial sectors will benefit from the R&D results. There will also be collaborative and solution-oriented research initiatives done with both industry and academia in the form of Centers of Excellence.

iii. Reduced supply chain risks91 and the development of human resources

As part of the 2013 IT security product evaluation policy, new testing infrastructure and facilities will be developed, global standards will be adhered to, and an effort will be made to build trust with vendors and service providers in order to improve supply chain security visibility from end to end.

In order to serve the nation's cyber security demands and create capacity, cyber security training infrastructure will be built throughout the country via public-private partnership agreements, as well as education and training initiatives. Concept labs for cyber security awareness and skill development will be developed, as well as institutional structures for law enforcement agencies to increase their capabilities.

iv. Increasing public and private sector understanding of cyber security and fostering successful public-private partnerships

The government plans to conduct a comprehensive national awareness campaign on cyberspace security in order to raise awareness among individuals and other organizations. It ensures that awareness-raising efforts continue in various forms, such as via the use of electronic media and other events like workshops and seminars on cyber security.

To maintain and sustain cyber security in the cyber space it is necessary to build collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices. A think tank for cyber security policy inputs, debate, and discussions will be established by all key parties.

v. Cooperation, Prioritized Approach

Boost national and international collaboration between security agencies, CERTs, military forces, law enforcement agencies, and judicial systems in the domain of cyber security via bilateral and multilateral connections. In order to ease recovery and resilience activities for systems, particularly key information infrastructure, methods for technical and operational communication with industry must be established.

The policy will be implemented in a prioritized manner, focusing on the most crucial regions first.

4.1 Operationalization of the Policy

National, sectoral, state, ministry/department/enterprise-level guidelines and plans of action will be used to implement this policy at different levels (national, sectoral, state, and so on).

5. CONCLUSION

In order to properly oppose cyber terrorism, we need to study its networks in detail and engage with specialists in computer security and law enforcement to understand how they might be effectively stopped. High-tech professionals now have the capacity to recognize cyber-attacks. Government agencies, companies, and other organizations have implemented a number of security measures in reaction to cyber terrorism and the worry that networks of terror may be limitless due of the universality and flexibility of the Internet. Cyber terrorism has no boundaries, both in terms of its perpetration and its consequences. Due to their geographical nature, law enforcement organizations have a difficult time dealing with such crimes since terrorists in one nation typically target victims in another. Law enforcement agencies that are both based in and have their jurisdiction derived from a certain nation. As we all know, the globe is made up of several independent nations, each of which has its own authority over the inquiry. When a law enforcement officer is able to identify the perpetrator of cyber terrorism, he has a number of challenges as he moves on with his investigation. Due to jurisdictional issues, he may not have the authority to act in a certain place. This is why.

Strict regulation of computer network-based cybercrime and terrorism will necessitate the creation of numerous new networks, including those between law enforcement and other government agencies, between law enforcement and the private sector, as well as networks of law enforcement across national borders. Over the last decade, there has been a significant increase in the ability of police departments across the world to react to cybercrime, as well as an increase in the knowledge of computer users about the need of basic protection online. Cyber-criminals' agility and the rapidity with which technology changes will continue to be a problem for law enforcement. To combat cybercrime effectively, the adage "think globally, act locally" is particularly relevant. Cyber terrorism has emerged as an even more severe kind of crime linked to online, and we haven't been able to react to it as quickly as we would have otherwise.

REFERENCE

1. PurohitMona:Legal Education & Research Methodology, Central Law Publications, secondedition 2012.
2. MakkarAshok:Legislative Framework to Combat Cybercrimes in India: An OverviewCyber Law Cybercrime Internet an E-commerce, Bharat LawPublications (2011).
3. Holt J Thomas, StrumskyDeborah, SmirnovaOlga: Examining the Social Networks of MalwareWriters and Hackers, International Journal of Cyber Criminology Vol. 6 Issue 1January - June 2010.
4. Pandey J.N. The Constitutional Law of India, 47th Edition Central Law Agency, Allahabad 2010.
5. McquadeSamuelC. III: Encyclopedia of Cybercrime, Greenwood Press, Westport,London©2009.
6. Kumar Ranjit : Research Methodology - a step -by - step guide for beginners, 3rd editionSage South Asia.
7. NagpalRohas:Cybercrime and Corporate Liability CCH India,(New Delhi), (2008).
8. Jain BandarmuthaRavikumar,Cyber Forensics: Concept & Approaches, Ed,(2006),The ICFAI University Press
9. Henderson Scott, The Dark Visitor: Inside the World of Chinese Hackers, Scott HendersonPublisher,2007
10. Lim Yee Fen,(2008), Cyber Space Law: Commentaries and Materials, Oxford University Press(Ne West Delhi).
11. Manikyam K Sita: Cybercrime: Law& Policy Perspective, Hind Law House (Pune).
12. PandeyAshish: Cyber Criminal Detention and Prevention, JBA Publisher (New Delhi), (2006),

Corresponding Author

Richa Tiwari*

Research Scholar, Jiwaji University