JIRCMS Vol.: 01 II Issue 02 II Pages 01-50 II July 2017

Cyber Terrorism: Need for a Cogent Policy In India

Dr. Harsh Malhotra
Gauri Devi Government College, Alwar

Abstract: Cyber terrorism is regarded as one of the biggest threat to the word today. It is generally understood as serious unlawful attacks on critical infrastructure made of computers, networks and information stored in them. The terror attacks on September 11, 2001 brought cyber terrorism to the mainstream and the governments around the world realized the grave threat cyber terrorism possesses to their infrastructure. Today, it has become the most complex and national as well as an international problem as a serious cyber attack may cripple critical infrastructure of any country which is the backbone of any nation's economy, security and health. While there has been greater international cooperation on this issue, it still has not received adequate attention by the Indian government. The National Cyber Security Policy, 2013 is a positive step but not enough to enable a creation of the right ecosystem to prevent such attacks. With the government's increased focus on making government services available electronically by improving the online infrastructure and internet connectivity in the country, there is an urgent need to devise policies to counter the threat of cyber attacks/terrorism. The author will assess the potential impact of such attacks on the critical infrastructure of a government and defenses that may be employed to fight them. Finally, the author will scrutinize the need for a strong counter cyber terrorism policy and mechanism in the country.

Introduction:

Cyber-fighting invokes pictures of data warriors releasing assaults against a clueless adversary's computer systems, wreaking destruction on the critical infrastructure. Cyber assaults pose complex problems that venture into new regions for national security and open strategy. Cyber-terrorism is often described as "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population." It involves exploiting network vulnerabilities in the computer systems of the critical infrastructure of a country. A threatening country or group could misuse these vulnerabilities to enter an inadequately secured computer network and disturb the workings of these critical infrastructure. While it has been suggested that critical infrastructures, particularly in advanced economies, are more circulated, assorted, repetitive and self-recuperating than a quick evaluation may propose, rendering them less defenseless against assault, the importance of securing a country's critical assets, especially in a country like India cannot be underestimated or ignored. Cyber assailants persistently abuse new vulnerabilities and new strategies to disturb the infrastructure which may also affect a country's national security to its detriment. The extent of these new issues relies upon how we characterize national security and how we prevent adequate harm.

Given the advancing meanings of the more extensive classes, it is not unexpected that meanings of cyber terrorism have been similarly divergent. The term infers two components: cyber and terrorism. Both of these are viewed as the two awesome feelings of dread of the late twentieth century. While the Indian authorities are not perceived to be taking this matter seriously yet, there is still an urgent need for defining the precise contours of the policy governing cyberspace with an emphasis on critical infrastructure. This is because the frameworks and systems that make up the infrastructure of society are regularly underestimated, yet a disturbance to only one of those frameworks can have desperate outcomes crosswise over other sectors.

Importance of Critical Infrastructures: Indian Perspective:

A useful definition of critical infrastructure is given by the United States of America statute Critical Infrastructures Protection Act of 2001

"systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

The Information Technology Act 2000 defines Critical Infrastructure as "*the computer resource, the*

incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety".

In the author's view, this definition encapsulates the exact meaning of critical infrastructure and it by and large incorporates the essential archives of monetary information, control framework, airport regulation, media transmission lines and towers.

There has recently been a sudden headway in the technology space and the data innovation framework. The reliance of critical infrastructures on the data innovation and web is expanding. As every one of the divisions of government and privately-owned businesses turn out to be more effective in the activities of critical infrastructure, these parts turn out to be progressively reliant on computer systems and networks for their efficient operations. The threats to Critical Infrastructures could either take form of actions by a nation-state or a terrorist organization or through embedded systems.

Considering the above, the question that arises is whether the Indian government is doing enough. India is highly vulnerable due to its unique position in the sub-continent and the world. Further, the geo-politics of the region makes India's position a sensitive and vulnerable one. The damage done by Stuxnet, often described as a cyber weapon of mass destruction, brought these vulnerabilities to the fore. India was one of the most severely affected countries due to this virus.

In 2008, the Parliament amended the Information Technology Act 2000 and introduced Section 70A and 70B to the Act. These sections established a special agency that would designate "Critical Information Infrastructure" (CII) and formulate measures for their protection. The agency was finally established on 16.01.2014 vide a notification- The National Critical Information Infrastructure Protection Centre (NCIIPC). As per the notification, critical sectors are those *"sectors that are critical to the nation and whose incapacitation or destruction will have debilitating impact on national security, economy, public health or safety"*.

NCIIPC has also formulated Guidelines for Protection of Critical Information Infrastructure. According to these guidelines, NCIIPC's agenda is to *"facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders with a vision to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country."* The sectors identified by the government and the nodal agency include an array of sectors such as energy, power, law enforcement, aviation, banking, critical manufacturing, defense and space.

The Government has further established the Indian Computer Emergency Response Team (CERT-In). The Team is tasked with the responding to the cyber security incidents and take steps to prevent their occurrence again. The 2008 Amendment to the Information Technology Act 2000 has designated CERT-In to serve as the national agency for the following areas of cyber security:

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, preventation, response and reporting of cyber incidents;

(f) such other functions relating to cyber security as may be prescribed.

CERT-In is also tasked with National Information Security Assurance Programme (NISAP) which is responsible for security policy for government and other critical infrastructure. One of the steps taken by CERT-In is making it mandatory for organizations and institutions to have a proper cyber security control mechanism in place and report any deviations or suspicious activities to CERT-In. Further, CERT-In is also empowered to create a panel of auditors who may audit such organisations and institutions once a year.

The Reserve Bank of India has also recently set up a computer emergency response unit. This has been done in the backdrop of growing cyberattacks in the financial system. Although the above-referred steps are laudable and much needed, more efforts need to be put to offer adequate protection to the critical

infrastructures in the country. The nodal agency NCIIPC should also undertake efforts to assist in the "*...development of appropriate plans, adoption of standards, sharing best practices, and refinement of procurement processes in respect of protection of Critical Information Infrastructure*".

THE ROAD AHEAD:

The critical infrastructure and governance is progressively becoming more and more technology savvy and reliant. Terrorists would have the capacity to close the entire working of a nation by focusing on the institutions which are running that country. Cyber terrorism, being a worldwide hazard, can be said to be a global crime. Thus, it requires a universal reaction. Treaty administrations and standard worldwide law can help assemble a solid arrangement of universal jurisdiction. Multilateral co-operation between countries is imperative to battle this malice. Presently, Council of Europe Convention on Cybercrime is the main settlement against cybercrime at the worldwide level. This may appear like an enormous task, however start can be made by receiving measures like liberal sharing of information on psychological militants and assaults, sharing new advances, reacting rapidly to two-sided demands and references made by Interpol and other worldwide insight organizations, leading cross country preparing trade programs.

With respect to the domestic affairs, it is suggested that a more stringent cyber security doctrine be created and should be endorsed by the National Security Advisory Board of the Prime Minister Office. Further, CERT-In should be granted enforcement powers so that it can carry out its functions well. In the alternative, it may be made a division of Home Affairs Ministry rather than the current power division under which it is part of Ministry of Communication and Information Technology. This would translate into better accountability of vulnerability assessment.

Furthermore, the framework overseers and the administration need to remain exceedingly caution for any notice they get for cyber assaults anytime of time. Methodical and routine hazard appraisal of critical data infrastructures ought to be frequently directed and given need for legitimate hazard management. A legitimate cyber fighting and encryption arrangement should also be produced. Keeping up the frameworks ought to be given most extreme significance by continuing working framework, programming the networks to prevent against hostile infection programs on a routine basis. Dynamic security measures ought to likewise be embraced, for example, finding the wellspring of assaults and forcing genuine hazard and punishment, and counter attacks. With each assault, its delayed consequences ought to be examined and legitimate measures ought to be taken to guarantee such assaults don't represent any danger in future.

It would not be justified to not credit the government for making progress in recognizing the threat. However, there is still considerable work required to deter the cyber terrorists. There is a need for an exhaustive arrangement of principles concentrating on the conveyance of security on a national scale in cyberspace. CERT-In should function as a conduit for planning a National Cyber Security Strategy and coordinate the exercises of cyber-crime policing in various states. It can likewise go into cyber-crime avoidance arrangements with different nations to guarantee international participation against cyber terrorism. The Centre may, for this purpose, enter into a knowledge sharing arrangement with the US Department of Homeland Security. Such an arrangement may include data sharing and capacity building measures. It has also been suggested that CERT-In ought to build up an out-of-band private and secure correspondence arrange, 'The Cyber Warning and Information Network (CWIN)' to enhance national abilities for notice.

It is also suggested that the National Technical Research Organization (NTRO), a technical intelligence agency under the National Security Advisor in the Prime Minister Office, which was set up in 2003, after India was first presented to the cyber arms stockpile kept by the United States. On the planning phase, the NTRO was conceptualized as an office that would center around technical knowledge and observation and guarantee the security of key government systems. The NTRO's exercises incorporate aeronautics and remote detecting, information assembling and preparing, cyber security, crypto frameworks, key equipment and programming improvement and vital checking. The NTRO has, under its umbrella, the National Institute of Cryptology Research, National Information Infrastructure Protection Center, Disaster Recovery Center and Aerospace and Remote Sensing Center. As a great part of the work completed by the NTRO isn't

accessible in people in general space, it is hard to remark on its commitment, particularly in issues identified with cyber security. Likewise, it would not be right to assume that with such a significant number of indispensable capacities to deal with, each essential in its own particular right, the thoughtfulness regarding cyber security matters may not be as sufficient, remembering the earnestness and reality of the danger._The NTRO, as the very name proposes, should lead spearheading R&D and empower the exchange of results to clients all around. It might loan its ability, worked throughout the years, in regions, for example, encryption innovation and infiltration testing. The rise of optical processing and smart specialists, and also improvements in territories, for example, nanotechnology and quantum registering will, very likely, reshape cyberspace and its security. NTRO's central goal ought to be to guarantee that the country is at the cutting edge of understanding these advancements and their suggestions for security. Coordination with other concerned offices and in association with industry to grow best practices and new innovation will also go far in improving the security of cyberspace.

Conclusion:

Dynamism is a sine qua non for any technology. As the experience curve grows, the technology also improves, also leading to graver risks and security issues. Cyber terrorism and the risk it possesses for the critical infrastructures in India needs immediate and constant attention of the Government. A culture of continuous surveillance of vulnerabilities in the computer networks of the critical infrastructures amongst the enforcement and regulatory authorities needs to be developed in the country. Further, adoption of best practices, standards and quality assurance should be hastened to create high levels of awareness amongst the masses should be there about information security and cyber terrorism. Our country's reliance must grow hand in gloves with continuous efforts to secure cyber infrastructure to protect our economy and national security. The government should adopt an integrated approach to network security, economic ideals as well as privacy rights and civil liberties of the netizens of the country.