Vol. 13 No. 2 ISSN: 0976-3570

Cyberspace Based Cross-Border Terrorism: An Overview of Global and Indian Legal Regime

Veerendra Mohan[1]

Abstract

Conventional noisy cross-national and continental physical terror attacks have evolved dynamically in a contemporary form of terror power through borderless 5G cyberspace[2]*, leveraging remotely the world web repository, satellites, drones, robots and instant data sharing etc. digital technology, capable of freezing critical native infrastructures including health, financial institutions, energy facilities, and disruption of social harmony and state governance etc. Cyberspace terrorists trained in pervasive vitriolic activities like arousing indignation, separatism, mass sympathy and mobilisation; and hiring, training terror agents, terror fund raising etc., under State agencies like ISI or non-state actors with unfailing synergy have been mercilessly overriding and frustrating the States' anti-terror laws, endangering the ICT (Information and Technology) domain involving Computer Network exploitations (CNEs) and Computer Network Attacks (CNAs). The author, having experience of four decades, examined efficacy of extant laws to deal with this contemporary form of terror.*

Keywords: *ICT environment, cyberspace driven cross-border terrorism, multinational cyberspace jurisdictions, dual criminality requirements, responsible state behaviour in cyberspace, pervasive terrorism, cyber sovereignty, self-defence doctrine.*

I. INTRODUCTION

The cross border terrorism using cyberspace, is a complex domain indelibly transforming conceptions of organised terrorists acts, requiring an indigenous, collective and collaborative unfailing global, technical and binding international constitutional/preambular safeguards and legislative responses criminalising even the conspiracy, solicitations, group forming, promoting, inducing, justifying,

[1] Research Scholar, Department of Law, University of North Bengal and Former Deputy Judge Advocate General, Ministry of Defence, India.

[2] GIBSON, WILLIAM (1984), NEUROMANCER, P. 69, (New York: Ace Books).

discrediting or humiliating victim, imparting training/instructions in firearms, nuclear material, detonative explosives, menacing, chemical or biological terror tools, possessions of terror software or hardware, deciphering encrypted information, collecting and dissemination of critical tangible terror literature, incitements and provocations advocating perverse ideological/religious/political opinions or eminent unlawful actions, glorifying or supporting of terrorists successes intended to disrupt public order or good governance, uploading maps, coordinating operational plans, uploading terror related weaponry/ ballistics /equipment literature, terror targets, tactics, purchasing/designing/launching and maintaining websites/file sharing sites/social networking sites, strategies, fundraising, virtual currency exchanges, tracking important public or private personalities/targets or carrying out their surveillance, offensive/ Jihadi/ radicalising/ ethnic/ strife or intolerance contents, integrating terrorists organisation, financial frauds, interfering/intercepting lawful actions against terrorism, commanding/controlling terrorists actions, racism or xenophobia, firearms/ammunitions/equipment trafficking, like inchoate terrorist offences, phishing and fraud etc. using multinational cyberspace jurisdictions through capacity building, striding aside the public as well as and private entities for a seamless sanctity of an open, secure, free, accessible and stable cyberspace much required as checks against the individual/institutional vulnerability, innovations, economic growth, sustainable development integrity, confidentiality, free flow of useful information, respect for cultural and linguistic diversity with an overarching objective to harness the cyberspace for growth and empowerment of people not just for India, but, for the entire humanity, by sustained and progressively advancing development against current trends in phishing, business spoofing, ransomware, honey trapping, hacking so and so forth, if need be to disrupt and deter the terrorists or prospective terrorists.

II. CURRENT CYBERSPACE INTERNATIONAL LAW LANDSCAPE

Internet is global, borderless and unfragmented (One World, One Internet), while at the application level 193 very different national jurisdictions coexist, cooperate or conflict (One World, 193 Jurisdictions). ICANN's CEO Göran Marby attempted in 2020 to disentangle the DNS from the "Political Internet Governance" (PIG) controversies by introducing the term "Technical Internet

Governance" (TIG). However, the discussion of this matter is not only not settled, but it has just begun, in particular with a view to the Chinese proposals to replace (or complement) the TCP/IP protocol with a new Internet protocol (New IP) and Russian initiatives to create options for a "national Internet segment", independent of the global DNS. However, the attempt to harmonise the legal systems of the 193 national jurisdictions is reaching limits. Technical realities determine political possibilities to some degree, as Larry Lessig noted in the late 1990s with his "Code is Law" thesis. The distance between "code makers" and "law makers" has not diminished in the last 20 years. "Code makers" have difficulties recognizing the political implications of their developments, "law makers" often have an inadequate understanding of how the technical infrastructure works. In his speech to the 14th Internet Governance Forum (IGF) in Berlin in November 2019, UN Secretary-General António Guterres pointed out the problem: *"There's an absence of technical expertise among policymakers even in the most developed countries, invention is outpacing policy setting, and measured difference in culture and mindset are creating further challenges. ... while industry has been forging ahead and at times breaking things, policymakers have been watching from the side lines"*[3].

According to **Black's Law dictionary**, cyber terrorism is defined as the act of "*Making new viruses to hack websites, computers, and networks".* The **U.S Federal Bureau of Investigation** defines cyber terrorism as a "premeditated attack against a computer system, computer data, programs, and other information with the sole aim of violence against clandestine agents and subnational groups".

A. UNCITRAL Model Law on E-Commerce[4]

Whereas NATO had put the cyber defence policy way back in 2008 followed by UNGGE in 2009. Successive "Group of Governmental Experts (GGEs)" are still struggling to control the cyber horns and we are still nowhere. In June 2021, the 25-member "*GGEs on Advancing Responsible State Behaviour In Cyberspace In The Context of International Security*", adopted a consensus report on the application of international law on cyberspace after protracted 18 months

[3]https://internet-governance-radar.de/en/whats-new/translate-to-englisch-blogpost/qiv-2021zusammenfassung.
[4] United Nations Resolution A/RES/51/162, Jan 30, 1997.

extensive deliberations, overcoming the earlier failed consensus on self-defence "international humanitarian laws", inclusions, as well as the contentiousness over the right to take countermeasures in 2016-17, honouring `*opinio juris sive,* necessitates', *lex lata, lex feranda* and the customary rules which have to be inseparably applied for the sake cyberspace sovereignty. A key portion of the Group's work was conducted during the coronavirus (COVID-19) pandemic, which has highlighted the tremendous potential of digital technologies while accelerating the world's dependency on them, thereby further underscoring the importance of responsible behaviour in the use of ICTs in the context of international security.[5] Seized of the continued differences on information systems security owing to diverse national laws, regulations and practices related to the use of ICTs, and unequal awareness of and access to existing regional and global cooperative measures available to mitigate, investigate or recover from terror attacks, and related risks/vulnerabilities globally, the GGEs re-resolved that the use of ICTs for terrorist purposes, against ICTs or ICT-dependent infrastructure, may threaten international peace and security, and also that the diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident etc. are risky. A host of necessities to bring in substantial clarity in issues of specificities requiring responsible states' conduct in cyberspace, still remain in discussions only. Cross border terrorist narratives, incitements, recruitments, and radicalizations having found ways through offline disseminations requiring continuous scanning/monitoring of the sources in real-time, though been put in place as a policy of predictive policing, yet, remain amenable to frequent breaches. Proactively the States are being urged to adhere to `Responsible State Behaviour' policy in the cyberspace domain in the same manner as they behave in the conventional domain and be always on the lookout for malicious actions and operations as these, do not always bring immediate results.

States are forbidden to consciously allow their territories to be used for wrongful acts using ICTs, it has clear connections to a nation's capacity to address malicious or criminal use of ICT infrastructure. Another norm that States are

[5] UN GA 14 July 2021; Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.

obliged to follow is not to conduct or support ICT activities that may potentially damage critical infrastructures.

B. Universal Anti-Terrorism Instruments (UATI)

The international legal framework for the fight against terrorism chiefly includes the UATIs (United Nations, their Conventions, Amendments and Protocols) as well as relevant United Nations Security Council resolutions (UNSCR).

C. UN Conventions, Protocol and Resolutions on Terrorism and International Criminal Law

Cyber-attacks seem to be covered under the banner of Article 2.4 of the UN Charter wherein the State are to refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'. Consequently, a cyber-attack that cripples a country's banking system, energy network or causes significant damage etc. could be comparable to a situation in which this infrastructure is attacked through conventional military methods[6]. Security Council has bound itself by its statement that every act of terrorism constitutes a threat to international peace and security, besides being against the purpose and principles of United Nations. As per Article 7(1) read with Article 7(2) of the Rome statute, widespread and systematic terrorist attacks against the civilian population also constitute crimes against humanity. Terror attacks using cyberspace, though not specifically covered under the Article would be *infra legem*. Article 8 features a host of acts as war crimes that do not specifically refer to the crimes committed using cyberspace as a tool or weapons having kinetic connections, though cyberspace is comparable to a virtual projectile capable of delivering the operational plans, codes for remote detonation of fuses, misleading messages in armed conflicts etc. Another glaring lacunae lies in the Article 4 of the Statute whereby the Courts have no jurisdiction over any person under the age of 18 years at the time of the alleged commission of a crime

[6] Erica Moret & Patryk Pawlak, The EU Cyber Diplomacy Toolbox: towards a cyber sanctions' regime?, European Union Institute for security studies, July 12, 2017, http://www.iss.europa.evlcontentleucyber-diplomacy-toolbox-towards-cuber-sanctions-regime.

thereby absolving the criminals below 18 years of age from individual or collective criminal liability.

Various preventive and suppressive terror related conventions identifying various terrorist conducts as offences, integrating the nations into a global legal regime that criminalises identified conducts of the perpetrators, penalise them with due concern for *aut dedere judicare or extradite or prosecute,* have been legislated over a period of time by the UN. Additional protocols and numerous Resolutions have also been passed to deal with different facets and ever evolving cross-border terrorism. Participating in an association or group for the purpose of terrorism viz to participate in the activities of an association or group for the purpose of committing or contributing to the commission of one or more terrorist offences by the association or the group, has been mandated to be criminalised in the domestic laws by the member states. Likewise, 'receiving training for terrorism' viz to receive instruction, including obtaining knowledge or practical skills, from another person in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence have been criminalised.

D. UNODC (United Nations Office on Drugs & Crime)

UNODC intensely does member state's domestic criminal justice systems capacity strengthening, harmonising international legal instruments against terrorism, particularly imparting specialised knowledge of law including internet related terrorist acts, though not so adequate to deal with the pervasive terrorism, investigations, and prosecutions besides the essence of customary laws. UN has revolutionized inter-state collaborative cooperation at international and regional layers to defeat terrorism in any manifestation including cyberspace[7].

E. Tallinn International Framework

Among the multinational organizations is the North Atlantic Treaty Organization (NATO) whose Cooperative Cyber Defence Centre of Excellence (CCDCOE)[8] in Tallinn, Estonia, helped facilitate the original Tallinn Manual on the International

[7] UN Resolution 60/288
[8] https://ccdcoe. org/

Law Applicable to Cyber Warfare (Tallinn Manual 1.0)[9] and Tallinn Manual 2.0[10]. Forging the views of internationally acclaimed expert scholars and practitioners, these manuals remain the most explored literature on the cyberspace laws ecosystem, and address the applicability of existing international laws to cyber warfare and cyberspace based cross order terror, focussing on attacks close to armed conflicts' threshold.

Cyber Sovereignty

Lacking in consensus until now, the issue remains debatable. UNGEE stated that international law applies to cyberspace, especially the UN Charter. For some nations, sovereignty has remained the keystone in the UN Charter and for some nations, the collective self-defence and non-interference in the internal affairs of a nation.

Utilitarian principle

Issue of Capacity building and helping those nations who cannot help themselves are not so easy to understand or implement in the extant ecosystem that has treaties on trust-building and confidence-building measures, regional confidence-building measures, and an elementary normative framework. But, how to go about implementing these. UNODC provides capacity-building legal assistance and training to member states to tackle investigation, prosecution and adjudication of terrorism-related offences besides digitization and relevant technologies, to prevent radicalization, recruitment and training of terrorists using cyberspace which saw a surge during COVID-19 rendering member States' to increased vulnerability to cybercrime and cyber-attacks.

Several CBMs are designed for seamless communication channel amongst states so that if any norm is broken, they can fall back. The states which are not in a position to develop indigenous security-building measures, are obliged to become active contributors to the international efforts.

[9] NATO Cooperative Cyber Defence centre of excellence, TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2012) [hereinafter TALLINN MANUAL 1.0].

[10] NATO Cooperative Cyber Defence centre of excellence, TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

Cyber Diplomacy Toolbox

UN and NATO have their own policy response framework, using cyber diplomacy toolbox for punishing cyberspace breaches by perpetrators/accomplices beyond the reach of law enforcement agencies. Also, there are statesmen, declarations, joint attribution statements, and very importantly the 28 nations' sanctions regime applicable in the cyber domain. NATO, within itself, has guidelines below the threshold of armed attack. NATO nations have been undertaking for a more coherent understanding of and also setting up mechanics of taking all those actions. European Union (EU) has adopted high profile sanctions regimes in recent years, including nuclear talks with Iran and North Korea. Besides resorting to this tool for conflict management and in support of rule of law, it employed the sanctions for countering international terrorism including against al-Qaeda), though, not so fool proof as to deter the perpetrators and accomplices as to most of the countries' war remains the last resort.

Incubator and Implementor Duo

The regional organisations serve as an incubator for generating ideas, practical effects and synergy with international laws. These organizations are immensely helpful as all concerns cannot be escalated to an international platform. That apart, these organizations also serve as implementors of the global mandate of international organizations like UNGEE. UN instruments are translated into reality through these organisations. Innovative ideas at the regional levels are invariably of global significance, thus, requiring better collaboration. Regional follow-up projects and collaborations with targeted norms campaigns are optimizing regional amalgamation. Alongside, capacity building measures also need to be undertaken. Also, creating an international legal structure without territorial bias.

Confidence Building Measures

Defensive measures automatically result in offensive capabilities *i.e.,* the retaliatory potential. So, is it true in Cyberspace security arena? A quintessential riposte to this daunting problem is the use of Inter-State confidence-building measures (CBMs). CBMs are pointers to ingraining robust cybersecurity themes, particularly at nascent stages of a country's entry into cyberspace for repelling cybercrime threats, and, sync in the international consistent cybersecurity domain

to combat cybercrime and cyber terrorism. CBMs acts as pressure valves to release mutual distrusts and tensions amongst states averting retaliatory measures i.e. cyber war. CBMs are incorporated into cyberspace covenants. CBMs are placed at the fulcrum of the UNGGE 2015 (Voluntary) norms of responsible state behaviour in cyberspace capitalizing on the framework of the Organization for Security and Co-operation in Europe (OSCE) *i.e.,* the 2013 CBMs. Miscalculations and misperceptions may potentially move the virtual world to the real one e.g., after the 2008 Mumbai attacks, 2010's `Pakistan-India Cyber war saw "cyber armies" from each country vandalizing official websites, intensifying diplomatic and military tensions. Ongoing tensions between the West and Russia, North Korea, and China also feature potent elements of cyber-distrust and readiness to proliferate into a cyberwar. These are typically the hybrid module of the cross-border terrorism.

F. 2001 Budapest Convention on Cybercrime[11]

It is a common criminal policy signed by members and non-members for combating cybercrime, adopting appropriate legislations and fostering international co-operation in the world digitisation, convergence and continuing globalisation of computer networks which are vulnerable platforms for committing criminal offences including terrorism, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation in seizing and provision of evidence relating to such offences honouring the interests of law enforcement and respect for fundamental human rights.

G. 2005 Warsaw Council of Europe Convention on the Prevention of Terrorism[12]

It criminalises certain acts amounting to terrorism, in particular, public provocation, recruitment, and training; and, seeks to bolster national and international co-operation to eradicate terrorism through individual state prevention laws and simplified extradition of the perpetrators and mutual

[11] *http://www.coe.int/en/web/conventions/full-list/- /conventions/treaty/185*
[12] *http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.*

assistance arrangements. 2015 Additional Protocol[13] to the Council of Europe Convention on the Prevention of Terrorism supplementing the convention further criminalizes certain additional acts stipulated in Articles 2 to 6 of the Protocol viz taking part in an association or group for the purpose of terrorism, receiving terrorist training, traveling abroad for the purposes of terrorism and financing or organizing travel for this purpose and exchanging information etc. regarding acts of terror.

H. Cross-border Information Sharing Laws

The 09/11 attack acted as a stimulus for advancing international harmony, cyber security international laws ecosystem and approaches to meaningfully and assertively deal with the prospective terror threats in all domains including the cyberspace, the mainstay being quick cross border information sharing. Adoption of the Resolution 1373 of 2001 by the Security Council is a proactive expanse in the adoption of policies and legal frameworks globally. Articles 19(3) and 20(2) are consistent with upholding national security and public order, and national or religious or racial hatred or discrimination and hostility or violence. Cyberspace often is used by terrorists for these purposes.

III. INDIAN SCENARIO

India has been targeted of intense terrorism for decades. Struggling through, however, it has maintained a fast-developing posture including its nuclear power status. Globally, India is amongst the fastest countries with exquisite dominance over the global IT market. Thus, potentially vulnerable to top tier national risk to the complex malicious subversive cyber-attacks or cyber aided physical territorial attacks using viruses, worms, phishing, malware, Trojans, etc. in ICT.

As defined in Section 2(y) of the Assam Rifles Act, 2006 (Act 47 of 2006), terrorist means any person who, with intent to overawe the Government as by law established or to strike terror in the people or any section of the people or to alienate any section of the people or to adversely affect the harmony amongst different sections of the people, does any act or thing by using bombs, dynamite or other explosive substances or inflammable substances or fire arms or other lethal weapons or poisonous or noxious gases or other chemicals or any other

[13] *http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217.*

substances (whether biological or otherwise) of a hazardous nature in such a manner, as to cause or is likely to cause death of, or injury to, any person or persons, or damage to, or destruction of, property or disruption of any supplies or services essential to the life of the community". Notably the definition is silent on hybrid module of cross border terrorism using cyberspace.

A policy framework named '*National Cyber Security Policy 2013*' was framed by the Department of Electronics and Information Technology (DeitY) under the Ministry of Communication and Information Technology (India) to build a secured, assured, regulatory, early warning, 24x7 emergency response teams (CERT), vulnerability management and response to security threats, protection of all e-governance initiatives, global best security practices, resilient etc. cyberspace framework for citizens, businesses and govt., laying down protection of entire ICT user and provider world and security breaches integrating all key players be it public or private. A national cyber co-ordination centre (NCCC) has also been brought in place specifically to tackle cyber terrorism with integration platform for CERT & ISACs. Home Ministry has set up `*Indian Cyber Crime Coordination Centre*' to tackle cyber-crimes and cyber terrorism. Cyber Swach Bharat Kendra (Botnet Cleaning & Malware analysis centre) has been set up to tackle threat bearing products and provide costless means and measures to get rid of the same, and, curtailing internet traffic expanse to Indian territories only

Indian legislators have taken years to recognise the Cyberspace vices and acknowledge its devastating impact on the national sovereignty, peace and security. Even after the UNCITRAL model law on e-commerce[14] adopted by UN Commission on International Trade Law, and, having been the signatory to said model law, India took another 04 years to give effect to the said resolution and to promote efficient delivery of Govt services by means of electronic records. Thus, came the Indian legislation `*Information and Technology Act, 2000'* which came into force on 17th Oct 2000[15]. *This was, however, not legislated as the complete solutions to deal with all kinds of contingencies. Instead, in order to make the provisions compatible, the existing penal code, evidence act including the Banker's Books Evidence Act and RBI Act,* were amended. The IT law, 2000 has also not been an original thought. It was legislated with threefold objectives to

[14] UN Resolution A/RES/51/162, Jan 30,1997.
[15] Notification No GSR 788(E), Govt of India Extraordinary Part II, sec.3(ii).

give effect to model E-commerce law adopted by UNCITRAL in 1996, thus, providing recognising and legalising electronic documents, digital signatures, e contracts and establishment of regulatory regime to supervise the certifying authorities issuing digital signature certificates, as also creating civil and criminal liabilities for contravention of the provisions of the IT Act,2000. With the passage of time, as the technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000.This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act,2008 has brought marked changes in the IT Act,2000 on several counts.

A. The Information Technology Act and Cyber Crime

The IT law vide Section 43, criminalises unauthorised accesses to a computer, computer system or network viz switching over a computer; using a software program installed on a computer; viewing the contents of a floppy disk; switching off a computer; taking a computer print-out; logging on the Internet; pinging a computer; and, gaining entry into, instructing or communicating with the logical, arithmetic or monetary function resources of a computer, computer system or computer network etc. Section 44 criminalises failure to furnish any document, return or report to the certifying authority. Section 65 criminalises, tampering including hiding or keeping secret; demolishing or reducing to nothing; or, changing in characteristic or position any the computer source document. Section 66 criminalises intentional causing of wrongful loss or damage to any person by unlawful means such as hacking; or, having knowledge that information residing in a computer resource document if concealed, destroyed or altered etc would cause damage to any person. Further the Act is committed with an intent to threaten the unity, security, sovereignty of India or to strike terror in the people or any section of people by denying or causing denial of access to any authorised person to access computer resource; or attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or introducing or causing to introduce any computer contaminant, and, by such conduct causes or likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or

adversely affects the critical information infrastructure specified under section 70; or knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the state or foreign relations; or any restricted information, data, computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of state, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, are construed as `Cyber Terrorism', commission whereof is criminalised under section 66 F. Further, Section 67 criminalises making of generally known, promulgate or issue copies for sale to public or disseminating of pornographic material on the website and Section 68 r/w 69 criminalises non-compliance of directions of certifying authority to interception or monitor or decrypt any information transmitted through any computer resource authorises the Controller or Certifying Authority whenever it is expedient to do so. Section 70 criminalises securing/attempt to secure access to a protected system, to wit, any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure declared as such by appropriate Govt incapacitation or destruction whereof, has debilitating impact on national security, economy, public health or safety. Further, Section 73 criminalises publishing of electronic signature certificate or it's making available to others, knowing it as having not been issued by certifying authority or that the listed subscriber has not accepted it; or that the certificate has been revoked or suspended, except where it is for the purposes of verifying a digital signature created prior to such suspension or revocation. Further, Section 74 criminalises creation, publication or making an electronic signature certificate for any fraudulent or unlawful purpose. Section 69-A empowers the Central Government or any of its officers to issue directions for blocking for public access of any information through any computer resource. The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 was promulgated under section 69B of the Information Technology Act, empowers monitoring and collection of traffic data/ information for forewarning imminent cyber incidents; monitoring network application with traffic data or information on computer resource; identification and determination of viruses or computer contaminant; tracking cyber security breaches or cyber security incidents; tracking computer resource breaching cyber security or spreading virus or computer contaminants; identifying or tracking any person who has breached, or is suspected of having breached or likely to breach cyber security; undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resources; accessing stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force; and, any other matter relating to cyber security. Rule 419(A) read with Sec 5 of IT Act, permits surveillance and interception of messages by Secretary and in exceptional circumstances by a Joint Secretary, a provision akin to Sec 91 of Cr PC which also permits surveillance by Court orders and of District Magistrates. Incriminating information collected during afore stated surveillance and interceptions, is admissible as evidence under The Unlawful Activities Prevention Act, 1967.

Shri Ajit Doval, KC, National Security Advisor, in his keynote address, while highlighting the Digital Revolution taking place in the country with the induction of a large number of digital services by the Governments at national and state levels, stressed over ensuring safeguards of the Indian Cyberspace[16]. Adding further he urged that Cyber Security remaining the foundation of any successful Digital Transformation, needs to be guarded against at all times. Any threats in the Cyberspace directly impacts the Indian National Security besides social and economic security.

B. Indian Penal Code on Cyber Terrorism

Treason, sedition and rebellion etc under sections 121, 121A, 122, 123, 124A, 153A and 153B of Indian Penal Code (IPC) read with section 118 of Indian Penal

[16] National Cyber Security Incident Response Exercise (NCX India) for Government officials and Critical Sector Organisations to strengthen India's Cyber posture, held on 18th Apr. 2022.

Code being 'Offences against the State', have been criminalised. Additionally, traversing beyond Sec 379 of IPC, Sec 411 of IPC criminalises acquisition of stolen cell phone, computer or digital or electronic data (Physical possession not being a sine qua non). Obtaining passwords, launching sham websites and phishing like fraudulent activities in cyberspace stand criminalised under Ss. 419 and 420 of IPC.

Spoofing or online forgery for committing other serious offences viz cheating, can be dealt under Sec 468 of IPC. Online forgery in a document in electronic forms or acts of disrepute can be dealt in Secs 469 and Sec 500 of IPC respectively. Acts of online threats, insults, provocation intended to breach the peace through email or any other electronic form, amount to an offence under Sec 504 of IPC. Online criminal intimidation with respect to the life of a person, property destruction through fire or chastity of a woman amounts to an offence under Sec 506 of IPC.

C. The Personal Data Protection Bill, 2019.

In India, the protection of data, its usage, and issues related to it are currently regulated by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules") notified under the Information Technology Act, 2000 ("IT Act")[17]. After the landmark judgment[18], the Supreme Court of India "**Right to Privacy Case**", the need was felt to have a stronger legislation in place to protect the personal data[19] and privacy of individuals. Bill was introduced by the Ministry of Electronics and Information technology in Lok Sabha. It was also inspired by the principles of the General Data Protection Regulations, 2016. The aim and premise of this Bill are to protect personal information and create a Data Protection Authority to do so for controlling data use by both public and private entities and means to regulates the collection of data by both Indian governments and businesses. It also applies to international companies that deal with the personal data of Indian citizens. This bill provides certain rights to data principles

[17] Information Technology Act 2008, Section 43.
[18] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., 2017 10 SCC 1.
[19] Aditi Phadris & Neha Alawadhi, JPC members record dissent towards parts of personal Data Protection Law, BUSINESS STANDARD, (Nov. 23, 2021) https://www.business-standard.com/article/current-affairs/jpc-members-record-dissent-towards-parts-of-personal-data-protection-law-121112200607_1.

with respect to their personal data, such as confirmation on whether their personal data has been processed, seeking correction, completion, or erase of their data, and restricting continuing disclosure of their personal data. The Joint Parliamentary Committee (JPC) constituted in December 2019 with 20 members from Lok Sabha and 10 from Rajya Sabha, on 21st September 2021 have finally tabled the PDP Bill.

IV. STEPS TAKEN TO CURB CYBER-TERRORISM

Various measures have been taken to combat cyber terrorism. Some of the steps taken are as under:

National Cyber Crime Reporting Portal[20]***,*** has been launched for enabling victims and complainants to register online their cyber-crime related grievances. This website only handles complaints about cybercrime, with an emphasis on cybercrime against women and children.

Indian Computer Emergency Response Team**,** a national nodal agency has been created for responding to computer security incidents as and when they occur.

National Cyber Security Policy**,** *a policy* framework has been set up by the Department of Electronics and Information and Technology to protect the public and private infrastructure from *cyber*-attacks.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), malicious programs detection and free tools to remove such programs center has been set up.

Cybercrime Coordination Cells**,** at national level [National Cyber Co-ordination Centre (NCCC)]; state level [State Cyber Crime Co-ordination Cells (SCCCC)]; and District Cyber Crime Cells (DCCC) have been set up with powers to scan and collect meta data of intelligence value in cohort with other intelligence agencies,

[20] www.cybercrime.gov.in: The Government has launched online cybercrime reporting to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries, or sexually explicit content. The Central Government has rolled out a scheme for the establishment of the Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cybercrime in the country in a comprehensive and coordinated manner.

and, share it with intelligence agencies for timely preventive actions wherever needed.

National Technical Research Organisation (NTRO), Erstwhile National Technical Facilities Organisation (NTFO), is a super technical intelligence feeder on internal and external security to various intelligence agencies including those of the Indian Armed Forces, has been establishment under National Security Advisor. Alongwith Indian Airforce, it operates a number of `Very Long-Range Tracking Radar (VLRTR)' systems for Missile Monitoring and detection of spaceborne threats in aid of Ballistic Missile Defence, using Technology Experiment Satellite (TES), CArtosat-2A, EMISAT and Cartosat-2B besides Radar Imaging Satellites; RSAT-1 and RSAT-2. It also operates Ocean surveillance ship-INS Dhruv.

National Critical Information Infrastructure Protection Centre (NCIIPC), is an organisation of the created under Sec 70A of the Information and Technology Act, 2002(amended 2008) under NTRO.

National Counter Terrorism Centre (NCTC), was set up post 26/11 Mumbai attacks related intelligence and operational, this agency with abilities of real time intelligence inputs of actionable value specifically to counter terrorist acts against India, was raised on the US pattern.

Signals Intelligence Directorate, a joint service organisation with elements of Indian Army, Navy and Air Force with widespread `Wireless Experimental Units (WEUs)' for monitoring military links of other countries.

Aviation Research Centre, has been set up as part of the Research and Analysis Wing (R&AW) of the Cabinet Secretariat (Special Requirements) for carrying out extensive aerial surveillance, signal intelligence (SIGINT) operations, photo reconnaissance flights (PHOTINT), monitoring of borders, imagery intelligence (IMINT).

National Intelligence Grid (NATGRID), has been set up to store citizens data with accessibility to RAW, CBI, IB etc.

New Media Wing (NMW) and the Electronic Media Monitoring Centre (EMMC), has been set up to carry out media surveillance and shares data with other intelligence units.

National Cyber Coordination Centre (NCCC), an operational cybersecurity and e-surveillance agency has been set up to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies. It has expanded the charter of the Computer Emergency Response Team, India, (CERT-IN), which has jurisdiction over not only government, but also public-private and private sectors.

The National Crime Records Bureau (NCRB), Intelligence Bureau (IB), the National Investigation Agency (NIA), the Central Bureau of Investigation (CBI) and the Narcotics Control Bureau (NCB), have been set up under the Ministry of Home Affairs, Govt of India for collection of intelligence data which is accessible by the NCCC. Likewise at the State levels crime investigation cells associated with the State Criminal Investigation Departments (CID) have cyber-crime branches.

National Investigation Agency (NIA), has been established post the Mumbai terrorist attacks of 2008, to take *suo moto* cognizance of terrorist crimes staring at the Indian national sovereignty, security, integrity, and friendly relations with foreign States, as also to deal with crimes under laws enacted to implement international treaties, agreements, conventions, and resolutions of the United Nations, its agencies, and other international organizations and matters connected therewith or incidental thereto, and, to raid, and seize properties with links to terrorist crimes without permission of the a state police head, provided NIA DG sanction has been accorded, invoking `The Unlawful Activities (Prevention) Amendment (UAPA)'. The NIA Amendment Act in 2019 expanded the type of offences to include cyber terrorism within the ambit and scope of investigations and prosecution by the NIA.

The National Critical Information Infrastructure Protection Centre has been set up to gather intelligence using sensors and platforms which include satellites, underwater buoys, drones, VSAT-terminal locators and fiber-optic cable nodal tap points, to monitor, intercept and assess threats to crucial infrastructure and other vital installations.

Presently, specialised wings of the Govt viz National Intelligence Grid, Crime and Criminal Tracking Network System (CCTNS); and, Central Monitoring System; Unique Identification Authority of India (UID scheme); Indian Computer Emergency Response Team (CERT-In); and National Counter Terrorism Centre

(NCTC) are in place establishing cross communication links amongst computers of various ministries/departments; finger printing, collecting, storing, analyzing, transferring and sharing of data between various police establishments as respects all available information on any criminal or any suspect stored on the servers of other police stations or departments; monitoring communications viz text messages, phone calls, online activities, social media conversations and contents; quick responses to cyber security incidents pan India etc. Also, efforts are on by the Govt of India to completely integrate the cyber policing, creating a predictive data base highlighting hotspots and affording real time cluster mapping visuals using satellite imagery besides the global view of family/kins and crime/criminal antecedents/connections.

V. INVESTIGATIONS AND PROSECUTION

Ordinary criminal investigative domain and investigators are not equipped to deal with the sophisticated means and technical know-how with which cyber terror is carried out as also the very nature of the contents which are in virtual domain. At present, our country does not have an efficacious legislative framework to meaningfully investigate the cyber terror offences, and, collect the actionable evidence which pre-dominantly lies in digital form.

The certification under Section 65 B of Indian Evidence Act 1861, and last years' Supreme Court's observation on admissibility of whatsapp message as evidence, "What is the evidential value of WhatsApp messages these days? Anything can be created and deleted on social media these days. We don't attach any value to the WhatsApp messages". "Prima facie we are not satisfied with the HC direction for depositing the money in an escrow account. We are not considering the purported admission in WhatsApp messages*"* [21], has become a real impediment in true dispensation of justice, despite the tangible chain of its existence is available with the investigating agencies.

Indian laws do not give any credence to the VOIP (Voice Over Internet Protocol) records of calls, file sharing, screen sharing which has become the main source of communication between people, distance being no bars, because of its efficacy over the traditional landline and mobile communications which inherently give

[21] A2Z Infraservices Ltd. v. Quippo Infrastructure Ltd. (Now Known as Viom Infra Ventures Ltd.) SLP(C) No. 8636/2021

out the geo locational identity besides being cost less. India lacks in high class forensic investigations capabilities in providing quick results in identifying the perpetrators and their modules.

VI. CONCLUSION

Modern Information technologies can leverage economic as well as social benefits. The states have worked diligently to realize a common vision of an ICT environment that is safe, free, peaceful and accessible. In all attempts, the issue does not seem to be resolved. From a psychological perspective, cyber and terrorism are two growing yet convincing fears that remain unresolved and need rigorous analysis to resolve the fear of the unknown. The source of the problem is not just the technologies that are prone to vulnerabilities, errors, and flaws but human behaviour is too at fault due to its inclination towards the negative and destructive forces, mainly to overcome insecurities, feelings of revenge, cheating, and rebel to destroy. Cyberspace and associated ICT methods have been used by several State and non-State actors for a variety of malicious purposes including cross border terror activities.

The Information Technology Act, 2000 has outlined bound offences and penalties to overpower omissions, that are known to return inside the characterization of cybercrimes. Change is necessary and needed, as the dilemmas posed by new technical advances every day cannot be prevented. Criminals have changed their tactics and embraced advanced technologies, and non-public corporations and organizations in India will have to change their mechanisms to tackle the issues in a coordinated manner to protect society, the legal system, and compliance authorities.

Owing to the fast-expanding terrorists' reliance on internet and a hierarchical global reach, all nations need to respond in closely coordinated ways to disrupt cross border terrorism with a robust and equally sophisticated legal system at international, regional, sub regional and national levels, as the growing technological advancements in digital world with advanced features like screen sharing etc. UN Security Council unitedly resolved[22] to combat terrorism, imposing obligations on member states to transpose various UN conventions,

[22] UN Security Council Resolutions 1373(2001) and 1566 (2004)-UN Charter Ch VII.

protocols, evolving a domestic prohibitor & preventive legislative structure and incidental rules and policies etc. to criminalise, investigate, detect, collect intelligence, arrest, extradition and prosecute terrorism. Resolution 1624(2005), in its preamble itself repudiates incitements of terrorists acts or attempts at justification or glorification of such acts intended to further incite. Resolution 1963(2010) seeks united approach to prevent ICT and connected resources from terrorist exploitations. Still an end to the cross-border terrorism using the cyberspace is nowhere in sight. A lot needs to be done to criminalise the novel methods with which the Terrorists using the cyberspace keep on causing destructions and infringing and disturbing people's rights.

The need of the hour is Globally integrated special international laws and integrated worldwide cyberspace courts and specialised cyber police and procedural codes penetrating beyond state boundaries including extraterritorial prescriptive jurisdictions for detecting, investigating, extraditing, trying and punishing the cyberspace mounted acts of terror. Preferably, it should be integrated with the military laws as it remains the last resort against the terrorism.