Cybersecurity and Threats
Cyberterrorism and the Order Today

Rebant Juyal*

The ever-growing dependence of man on cybernetworks has unbridled a modish genre of cyberthreat called cyberterrorism. The pervasive cyberspace has provided an advantageous operational frontier to the terrorists for executing cyberattacks on critical infrastructures, spreading hate propaganda over the Internet and using it for recruitment, planning and effecting terror attacks. Furthermore, it has proliferated terror configurations and metamorphosed terror operations. There is the most urgent need to secure our cyberspace from such formidable cyberthreats. Formulating a cybersecurity strategy through international cooperation is a desideratum to confront mushrooming cyberterrorism which poses a severe threat to global security and current economic scenario. This article examines cyberterrorism as a component of cyberthreats and further analyses the constitutional obligation of the state to protect cyberspace.

Keywords: *Cybersecurity, threats, Cyberterrorism, cybersecurity cooperation, Right to Trade and Business, cyber militancy, state sovereignty*

The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.[1]

– Ban Ki-moon

* The author is a final year law student at Guru Gobind Singh Indraprastha University, Delhi.

ISSN 0976-1004 print

Introduction

The development of cyberspace has been one of the greatest technological achievements of mankind. These technological advances entrust mankind with incredible benefits in diverse fields, yet they always influence the nature of security threats in society. Amongst contemporary security vulnerabilities, cyberthreats have emerged as a critical threat to our society.[2] Cyberthreat is an amorphic change in the nature of threats that is capable of convulsing the economic[3] and social order of the world.[4] These threats are hard to detect and difficult to investigate because of their anonymity.[5] Since the Internet has developed as an unregulated, open architect, the globally integrated transnational character[6] of cyberspace has favoured the growth of cyberthreats. It has been ideal for offenders wanting to anonymously carry out criminal activities in the cyberworld beyond territorial borders, thereby amplifying the scope of crime and stimulating it to move beyond mental torture, anguish and physical assault. Today, the criminals target the Web to derange the global order and virtual life of people.

Based on the perpetrators and their motives, cyberthreats can be disaggregated into four types.

Cybercrime

Cybercrimes are criminal activities carried out through a computer network, wherein a computer might be the target or used in the commission of an offence. Thus, it is the use of information technology for criminal activities.[7] Cybercrime has evolved in unexpected ways,[8] with cyber criminals embracing innovative and highly inventive techniques for executing diverse cyber offences.[9] The voluminous, expansive use of the Internet has led to a large online population, not only exposing many people and businesses to cybercrimes but also causing several vulnerabilities, including towering economic losses.[10]

Cyber-Espionage

The act of using a computer network to gain unlawful access to confidential information from another computer is called cyber-espionage. It is executed to extract classified information from the government and other crucial organisations. Cyber-espionage cases are intensifying, where cyber-enabled illegal abstraction of data, intellectual properties (IPs)[11] and trade secrets worth billions of dollars is being accomplished.[12] Besides being inexpensive and easy to commit, cyber-espionage is hard

to prove with certitude.[13] The most gripping instance of cyber-espionage in India was the hacking of Prime Minister's Office website in 2011[14] and the breach of 12,000 sensitive email accounts of government officials in 2012.[15] Overseas Indian missions have also reported several instances of cyberattacks.[16]

Cyberwarfare

Cyberwarfare is the use of cyberspace to conduct acts of warfare against other countries.[17] It includes attacks like distributed denial of services,[18] defacing of websites and so on. Cyberspace is considered the fifth dimension of warfare, after land, ocean, air and space. In fact, the Pentagon and North Atlantic Treaty Organization (NATO) have designated cyberspace as an 'operational domain', just like air, land and sea.[19] The United States (US) cybersecurity doctrine provides for the right to military action against cyberattacks.[20] The US has also elevated the United States Cyber Command to the status of a 'Unified Combatant Command'.[21]

Presently, states are working in an environment of threat and detriment in cyberspace.[22] This has triggered a response to prepare themselves for defending their networks against the growing sophistication of cyberattacks they face. More than 140 countries have developed or are in the process of developing their patenting and proficiency in cyberwarfare.[23]

Cyberterrorism

Cyberterrorism, a term first coined by Barry Collin in the 1980s,[24] is the convergence of terrorism and cyberspace. It involves an attack over a computer network(s) for the political objectives of terrorists to cause massive destruction or fear among the masses and target the government(s). Cyberterrorism aims to invade cybernetworks responsible for the maintenance of national security and destroy information of strategic importance. It is one of the biggest threats to the security of any country,[25] capable of causing loss of life and humanity, creating international economic chaos[26] and effecting ruinous environmental casualties by hacking into various critical infrastructure (CI) systems. The notable characteristic of cyberterrorism is to use its economic competence to clinch inordinate effects of terror over cyber and real world through cyber-crafted means, like destruction of cybernetwork, denial of service attacks and data exfiltration.

Dangers created by cyberterrorism warrant immediate global consideration. However, states have been ineffective in advancing a consensual approach by which varied acts of terrorism in cyberspace can be brought under the nomenclature of cyberterrorism. Currently, no universally agreed definition for cyberterrorism exists,[27] even though it has been acknowledged internationally as a major risk to global peace. It is probably because of the saying, 'one man's terrorist is another man's freedom fighter'. Subsequently, different perspectives over the elemental constituents and definitions of cyberterrorism will be contemplated.

Definitions of Cyberterrorism

Cyberterrorism is unlawful attacks and threat of attacks against computers, networks, and information stored therein, that is carried out to intimidate or coerce a government or its people in furtherance of some political or social objectives.[28] It is the 'premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs and data that results in violence against non-combatant targets.'[29] It aims at seriously affecting information systems of private companies and government ministries and agencies by gaining illegal access to their computer networks and destroying data.[30] Cyberterrorism, as a small landmass of the vast territory of terrorism, uses cyberspace as a target or means, or even a weapon, to achieve the predetermined terrorist goal. In other words, it is the unlawful disruption or destruction of digital property to coerce or intimidate governments or societies in the pursuit of religious, political or ideological goals.[31] It is an act of politically influenced violence involving physical damage or even personal injury, occasioned by remote digital interference with technology systems.[32]

Cyberterrorism not only damages systems but also includes intelligence gathering and disinformation. It even exists beyond the boundaries of cyberspace and incorporates physical devastation of infrastructure. The NATO defines cyberterrorism as 'cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or intimidate a society into an ideological goal'.[33] The most acknowledged definition of cyberterrorism is of Professor Dorothy E. Denning, as an unlawful attack against computer networks to cause violence against any property or person(s), intending to intimidate a government.[34]

Scope of the Definition(s) of Cyberterrorism

While studying cyberterrorism, it is imperative to discern the two aspects of usage of cyber technology by terrorists: (i) to facilitate their terror activities; and (ii) to use cyberspace as a weapon to target the virtual population or execute terror activities.

It is clear from the discussion here that cybercrime and cyberterrorism are not coterminous. Most definitions of cyberterrorism establish a restricted functional framework for the scope of cyberterrorism.[35] For a cyberattack to qualify as an act of cyberterrorism, it must be politically motivated; cause physical or other forms of destructions or disruptions, like attacks affecting the unity, integrity and sovereignty of a country; cause loss of life (such as use of cybernetworks in 26/11 Mumbai terror attack);[36] and result in grave infrastructural destruction or severe economic losses. The use of cyberspace and information and communication technologies (ICTs) by terror outfits to facilitate their functional activities (like organisational communications) should be considered as cybercrime. Reckoning the 'facilitating part' under the definition of cyberterrorism would intensify the scope of cyberterrorism and augment the problem to be rectified.

Threats Posed by Cyberterrorism

Cyberterrorism poses critical security threats to the world. The CIs, like nuclear installations, power grids, air surveillance systems, stock markets and banking networks, are dependent upon cyberspace. This functional dependence has made CIs vulnerable to cyberterror attacks and increased the scope for cyberterror footprints exponentially.[37] Most CIs globally are poorly protected.[38] Therefore, cyberterror attacks on CIs can cause egregious damages to the society. Further, today there is a persistent threat of sensitive information of national interests being stolen by terrorists, destruction of computer networks or systems superintending the functioning of CIs.[39]

Objectives of Cyberterror Attack

Cyberterrorism is based on specific objectives, such as:

1. Target CIs[40] of the country, like air traffic, military networks, financial and energy systems, telecommunications and others, to cause physical devastation.

2. Cause disruptions sufficient to compromise the industrial and economic operations of a country. A cyberterror attack thwacks a large part of the world population and causes monetary disorder and loss of data.[41]
3. Cause physical injuries, loss of lives, explosions, crashing of aircraft and other aerial vehicles,[42] theft of technology and privileged information.[43]
4. Move beyond the realms of destruction and send a signal of ferocious disruption and fear to governments.[44]

Possible Targets of Cyberterrorists

Cyberattacks by terrorists majorly focus on two domains: control systems[45] and data in cyberspace. Consequently, the security challenges against cyberterror attacks generally vary across these two scopes. The first possibility is that terror outfits, such as Al-Qaeda and the Islamic State (IS), would exploit the information space to launch a cyberattack to ruin the CI facility of a particular state (Kudankulam Nuclear Power Plant cyberattack).[46] In the second instance, the Internet is abused to attack webspace or other trivial frameworks for their political intents, coalesced with the likeliness that such virtual attacks could turn adamantly grave to the point of being catalogued as a cyberterror attack.[47]

Exploitation of Cyberspace by Terrorists

Terrorist organisations use cyberspace for recruitment,[48] command and control[49] and spreading their ideology.[50,51] Internet being the largest reservoir of knowledge has fuelled terror outfits to use this quality to set up virtual training camps in cyberspace. In 2003, Al-Qaeda established its first online digital repository, providing information on matters ranging from bomb-making to survival skills.[52] Today, the Internet is used by multiple self-radicalised patrons as a resource bank.[53] Cyberspace has emerged as a new operational domain[54] for terror and extremist establishments, appending new dimensions to cybersecurity of precluding online jihadist recruitment,[55] radicalisation[56] and raising of funds.[57] The terror outfit of IS has manoeuvred this stratagem and used it proficiently for itself.[58] The militant group was able to recruit 30,000 fighters through social media.[59] Social media subsequently helped the group to establish its franchises and expand its base in different countries.[60] Additionally, terrorists use Internet proficiency to reach out to masses to inspire acts of terror as well as disseminate their messages.[61]

Cyberterrorism versus Conventional Terror Attacks

Cyberspace offers anonymity, easy access and convenience to terrorists to reach the masses without much monetary expenditure. The ubiquitous cyberworld enables terrorists to launch cyberattacks having far-reaching impacts and causing staggering damages, more critical than physical attacks.[62] Traditional terror attacks are restricted to the physical limits of the place of attack. Also, while people outside the territorial limits of the attack do read and observe such incidents, they do not get affected directly. A cyberterror attack, however, encompasses the potential of affecting millions without any territorial limitations; at times, it is more enigmatic to find the perpetrator and trace the point of origin of cyberterror attacks.[63] Hence, cyberspace facilitates cyberterrorists by enabling them to have a far greater reach than ever before. Further, global interconnectivity of cyberspace results in proliferation of potential targets for terrorists to attack, making it more dangerous than other terror attacks. Such unmatched capabilities of cyberterrorism give terrorists extraordinary leverage to engender more harm to society.

Thus, different factors make cyberattacks a capitative choice of terrorists:

1. Cyberterrorism constitutes a low-cost asymmetric warfare element for terrorists as it requires fewer resources in comparison to physical terror attacks. The terror groups can inflict more damage to people and society with the same amount of funds. Thus, the benefit–cost ratio for a cyberterror attack is very high.[64]
2. Cyberspace provides anonymity, thereby enabling cyberterrorists to hide their identity. The Indian government had admitted in Rajya Sabha that attackers compromise the computer systems situated in different locations of the globe and use masquerading techniques and hidden servers to hide the identity of the computer system from which the cyberattacks are propelled.[65] It is the anonymous nature of cyberspace that makes it arduous to attribute cyberattacks to any state.[66]
3. The CIs and other valuable state resources are not fully protected and thus become an obvious target of cyberterrorists. After designation of the target, the cyberattack can be launched without any unwarranted delay and need for further preparation.[67]
4. The Internet enables cyberterrorists to initiate a cyberattack on any distinct part of the world. Unlike physical terror attacks, there

are no physical barriers or checkpoints that block cyberterrorists in the execution of predetermined cyberattacks on designated targets. Likewise, cyberterrorism involves less risk than physical terrorism.

5. Cyberspace provides broad avenues for disseminating terror organisation propaganda. It provides a larger audience for cyberterror attacks, whose impact goes beyond cyberspace to diverse systems.[68]

Initiatives Taken to Mitigate Cyberterror Attacks Worldwide

The mushrooming menace of cyberterrorism has stimulated states and international organisations to reform the global cybersecurity architecture for combating cyberterrorism.

International Forums

Convention on Cybercrime

The European Union's Convention on Cybercrime, also called the Budapest Convention,[69] is the sole binding international convention on cybercrimes.[70] It aims at harmonising domestic laws,[71] including an international cooperative framework,[72] and also proposes to improvise investigation techniques on cybercrimes for member states. India is not part of this treaty.

United Nations (UN)

1. *UN Global Counter-Terrorism Strategy*:[73] The strategy manifests the commitment of all UN member states to eliminate terrorism in all forms. The resolution aims to expand international and regional cooperation and coordination among states, private players and others in combating cyberterrorism, and also seeks to counter the proliferation of terrorism through cybernetworks. The 2018 resolution over the sixth review of the strategy asks member states to ensure that cyberspace is 'not a safe haven for terrorists'.[74] It urges member states to counter terrorists' propaganda, incitement and recruitment, including through cyberspace.
2. *United Nations Office of Counter-Terrorism (UNOCT)*: The UNOCT was set up on 15 June 2017, vide United Nations General Assembly (UNGA) resolution,[75] following the Secretary-General's report over UN's role to assist member states in implementing UN

counterterrorism strategy.[76] The UNOCT supplements the efforts of member states against terrorism, including cyberterrorism. It provides multi-stakeholder cooperation in securing the cyberspace of respective countries from cyberterror attacks.[77] It has initiated various projects aimed at building and upgrading capacity among states to combat cyberattacks and raising awareness against cyberterrorism among masses.[78]

3. *United Nations Security Council (UNSC)*: In 2017, UNSC adopted a resolution for the protection of CI.[79] The resolution asks the member states to establish cooperation with all stakeholders at international and regional levels to prevent, protect, respond and recover from cyber-enabled terror attacks over the state CI. It also asks the states to share operational intelligence over the exploitation of communication technologies by terror outfits.[80] The UNSC presidential statement in May 2016 recognised the requirement of global effort to stop terror outfits from exploiting cybernetworks.[81]

Brazil, Russia, India, China and South Africa (BRICS) Counter-Terrorism Strategy

The strategy aims to counter international terrorism and its funding, enhance cooperation in mutual legal assistance and extradition against terrorists, improve practical cooperation among security agencies through intelligence sharing, etc. The strategy resolves to 'counter extremist narratives conducive to terrorism and the misuse of the Internet and social media for the purposes of terrorist recruitment, radicalization and incitement and providing financial and material support for terrorists.'[82]

Shanghai Cooperation Organisation (SCO)

The SCO has adopted several significant steps to counter the menace of cyberterrorism.[83] It established the Regional Anti-Terrorist Structure (RATS) in 2001 against terrorism.[84] The 22nd session of SCO RATS council approved various proposals to combat cyberterrorism,[85] and also discussed the proposal to establish a cyberterrorism centre.[86] In 2019, SCO member states conducted anti-cyberterrorism drills to prepare for future cyberterror crisis.[87] Further, in 2015, SCO submitted to UNGA an International Code of Conduct for Information Security,[88] proposing a secured and rule-based order in cyberspace.[89] The code suggests international cooperation among states to combat exploitation of ICTs for

terror-related operations.[90] Furthermore, it specifies a code of conduct,[91] responsibilities of states[92] and rights of individuals[93] in cyberspace.

The US

Cybersecurity and Infrastructure Security Agency (CISA) Act

The act establishes that the CISA will secure American cybernetworks and CIs, devise US cybersecurity formations and develop potential to defend cyberattacks. Further, it secures the federal government's '.gov' domain network. It also houses the National Risk Management Center (NRMC), which addresses most strategic threats to the country's CI and crucial functions whose disruption can have devastating impacts over American national interests, like security and economy.[94] In 2017, the US President issued an executive order (EO 13800) to modernise US cybersecurity proficiencies against intensifying cybersecurity threats over CIs and other strategic assets.[95]

National Cyber Strategy of the US

The strategy, released in 2018,[96] strengthens the US cyberspace to respond against cyberattacks. It focuses on securing federal networks and CIs, as well as combating cyberattacks. The cyber strategy primarily aims to protect American people, preserve peace and advance American interests.[97] It also provides for military action to combat cyberattacks.[98]

Israel

Israel launched its first-ever National Cybersecurity Strategy in 2017. The policy document expounds the country's plan to advance its cyber robustness, systemic resilience and civilian national cyber defence.[99] The objective is to develop an international collaboration against global cyberthreats, which certainly includes cyberterror threats.[100] It also prioritises to defend Israeli economic, business and social interests in cyberspace.[101]

The Israel government passed several resolutions, like 3611,[102] 2443 and 2444, to expand institutional capacity for cybersecurity framework by establishing National Cyber Directorate.[103] Israel's cybersecurity framework focuses on four priority areas:

1. Improving domestic capabilities to confront futuristic and present-day cybersecurity challenges.

2. Continuously upgrading and enhancing defence of CIs in the country.
3. Fostering the republic's standing as an international hub for the development of ICTs.
4. Promoting effective coordination and cooperation among the government, academia and private players.

The United Kingdom (UK)

The UK introduced the National Cyber Security Programme in 2015 to protect its computer networks from cyberattacks. A five-year National Cyber Security Strategy was also revealed in 2016 to make UK's cyberspace resilient from cyberattacks and more secure by 2021.[104] Further, in 2017, National Cyber Security Centre was opened to respond to high-end cyberattacks.[105]

Initiatives Taken in India

Information Technology Act: Cyberterror Law of India

The Information Technology Act (hereafter the Act) sanctions legal provisions concerning cyberterrorism. Section 66F[106] of the Act enacts legislative framework over cyberterrorism. It provides for punishment, extending to life imprisonment, for cyberterrorism,[107] along with three essential elements for an act to constitute as cyberterrorism:

1. *Intention*: The act must intend to afflict terror in people's mind or jeopardise or endanger the unity, integrity, security or sovereignty of India.
2. *Act*: The act must cause:
   (i) unlawful denial of access to any legally authorised person from accessing any online or computer resource or network;[108] or
   (ii) unauthorised attempt to intrude or access any computer resource;[109] or
   (iii) introduce or cause to introduce any computer contaminant.[110]
3. *Harm*: The act must also cause harm, like death, injuries to people, adverse or destructive effect on the critical information infrastructure (CII), damage or destruction of property or such disruptions likely to cause disturbances in such services or supplies which are essential to life.

Further, Section 66F also applies to instances where a person without any authorisation or by exceeding his legitimate authorisation intentionally penetrates or accesses a computer resource and obtains access to such data, or information or computer base which has been restricted for Indian security interests, or whose disclosure would affect the sovereign interests of India, etc.[111]

Protected Systems and CII

The Act has a provision of 'protected systems', empowering the appropriate government to declare any computer resource that either directly or indirectly affects the facility of CII as 'protected system'.[112] Section 70(3) sanctions punishment up to 10 years with fine in case a person secures or attempts to secure access to a protected system.[113] The explanation clause of Section 70 defines CII as: 'The computer resource, incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety.'[114]

The central government, under Section 70A of the Act, has designated National Critical Information Infrastructure Protection Centre (NCIIPC)[115] as the National Nodal Agency in respect of CII protection.[116] The union government has also established Defence Cyber Agency[117] to deal with matters of cyberwarfare and cybersecurity.[118]

Indian Computer Emergency Response Team (CERT-In)

Section 70B of the Act provides for the constitution of CERT-In to maintain India's cybersecurity and counter cybersecurity threats against it. The CERT-In is expected to protect India's cyberspace from cyberattacks, issue alert and advisories about the latest cyberthreats, as well as coordinate counter-measures to prevent and respond against any possible cybersecurity incident.[119] It acts as the national watch and alert system and performs functions like:

1. Collect, analyse and disseminate information on cybersecurity incidents;
2. Forecast and issue alerts on cyber-incidents;
3. Emergency measures to handle cybersecurity incidents;
4. Coordinate cyberattack response activities;
5. Issue guidelines, advisories, over cybersecurity measures, etc.[120]

India has established domain-specific computer emergency response teams (CERTs) to counter domain-specific cyberthreats and create a

more secured cybersecurity ecosystem in respective domains, like power grids and thermal energy.[121] Further, sectoral CERTs in the cybersecurity fields of finance and defence have been constituted to cater to such critical domain's cybersecurity requirements.[122]

National Cyber Security Policy

The National Cyber Security Policy of India, released in 2013, aims to secure Indian cyberspace and concretise its resilience from cyberthreats in all sectors.[123] It aims at developing plans to protect India's CII and mechanisms to respond against cyberattacks effectively. It further focuses on creating a safe and dependable cyber ecosystem in India. The policy has facilitated the creation of a secure computing environment and developed remarkable trust and confidence in electronic transactions. Furthermore, a crisis management plan has been instituted to counter cyber-enabled terror attacks.[124] The Parliament also amended the National Investigation Agency (NIA) Act in 2019, empowering the NIA to investigate and prosecute acts of cyberterrorism.[125]

Moreover, technology and threat Intelligence play major roles to counter terrorism and cyberterrorism. The multi-agency centre (MAC) at the national level, set up after the Kargil intrusion, along with subsidiary MACs (SMACs) at state levels, have been strengthened and reorganised to enable them to function on 24×7 basis. Around 28 agencies are part of the MAC and every organisation involved in counter-terrorism is a member of this mechanism. This is yet another important element of national initiative.

Recommendations and Analyses

Legislative Reforms

The Information Technology Act

India, as a fast-developing economy, aspires to control the global supply chain and internationalise its economy.[126] This vision automatically attracts a big responsibility to protect cyberspace from possible cyberthreats, including acts of cyberterrorism. India, however, has been rather vulnerable to cyberthreats.[127] Currently, with major economic activities transpiring through digital platforms during the COVID-19 pandemic, the dreadful impact of cyberterrorism has intensified.[128] The purpose of cyberterrorists is to cripple the CI of a nation and certain services,

like telecommunications, banking, finance, military complexes[129] and emergency services, are most vulnerable to cyberterror attacks.[130] Thus, it is necessary to comprehend the potential threat of cyberterrorism to a nation like India, keeping in mind that the vulnerability of Indian cyberspace to cyberterror attacks has proliferated enormously.[131] In 2018 too, the then Home Secretary admitted to India's exposure to cyberthreats and its inadequacy in countering them.[132] Therefore, reforming and modernising the existing machinery to counter the strategic challenge of cyberterrorism and providing efficient explications acknowledging global pandemic is peremptory. Though the Act enacts provisions regarding cyberterrorism, in order to make it a more focused legislation to combat cyberterrorism, the following modifications are suggested:

1. The Act was originally enacted to validate e-commerce activities. However, its preamble today must not remain limited to e-commerce only. It must additionally include the objective of combating cyberterrorism.
2. The scope of the definition for cyberterrorism should be made more extensive by including 'the usage of cyberspace and cyber communication'. The section does not cover cyberspace use for communication and related purposes to fulfil and execute terrorist objectives. The Act should incorporate provisions to cover such acts to prevent acts of cyberterrorism.
3. To focus the orientation of the Act to combat cyberterrorism, it must have a dedicated chapter on cyberterrorism, which would deal with all intricate elements and dimensions of the acts amounting to cyberterrorism in detail.

Indian Cybersecurity Act

In 2008, the Information Technology Act was amended to incorporate provisions concerning cyberterrorism. However, from 2008 to 2021, exploitation of cyberspace by terrorists has undergone a systematic transformation. The conglomeration of time and evolution of destructive technologies has made cyberterrorism intricately complex and devastatingly lethal to deal with. Cyberterrorists use innovative methods to exploit cyberspace for youth radicalisation and to propel cyberattacks causing massive destruction. The evolution of destructive technological order aiding cyberterrorism warrants a new modernised legal order, with empowered law enforcement agencies, to protect Indian cyberspace against possible cyberthreats and preserve its cyber sovereign interest.

India must consider enacting a new cybersecurity legislation,[133] Indian Cybersecurity Act, dedicated to deal with present-day cybersecurity challenges and regulate all aspects of cybersecurity, including cyberterrorism. Further, in view of the future consolidation of cyberterror attacks, a new legislation would additionally provide more effective, deterrent and stringent legal framework against cyberterrorism.

Administrative Reforms

Multiplicity of Organisations

Multiple government organisations handle cybersecurity operations of India,[134] resulting in overlapping jurisdictions and operations among organisations. Some reformatory steps—like creating the National Cyber Security Coordinator under National Security Council Secretariat (NSCS) and bringing central agencies under its control—have been adopted. However, it is important to provide the exigent task of cybersecurity exclusively to three central agencies, namely, CERT-In, NCIIPC and Defence Cyber Agency, with well-delineated and defined jurisdictional limits of operations and responsibilities. Instead of creating a parallel hierarchical structure which results in unwarranted overlapping of work, the jurisdictional limits of operations must be detailed through legislation to the extent possible.

Further, there must be a regular review of the jurisdictions of organisations to keep India's cybersecurity mechanism updated as per the continuously evolving cyberspace. Since what today is not a CI might become intrinsically critical for preserving national security tomorrow, the National Cyber Security Coordinator must proactively coordinate the activities of the cybersecurity agencies to intensify capabilities of India to counter cyberterrorism.

Awareness Programmes

The government, like UNOCT, must undertake cybersecurity awareness programmes in the country and establish an informative environment in the country against possible cyberthreats (including cyberterrorism) in cyberspace. The government must consider launching a cyber literacy programme (initially in areas vulnerable to cyberattacks) on lines with 'Sarva Shiksha Abhiyan' to familiarise people about the cybersecurity threats in a time-bound manner. This is particularly important during the COVID-19 pandemic when most businesses are running digitally through online mediums.

Indian Cybersecurity Service

India cannot reform and strengthen its gigantic cybersecurity framework from one central place. Cybersecurity threats are the new normal for people, including those living in distant parts of India. Therefore, India must establish Indian Cybersecurity Service as an all-India civil service. It will provide India with the best professionals (posted in different parts of the country at the grassroots level) to deal with all aspects of cybersecurity, including cyberterrorism. An all-India civil service would further equip the state governments with talented cybersecurity experts to protect their cyber operations and deal with breaches under their jurisdiction. The proposed civil service could also assist the state police in solving cyber-related offences more effectively and expeditiously, thereby improving the administration of justice in cybercrimes.

As these cybersecurity officials will get an opportunity to work in different parts of the country in various capacities, like officers from other all-India services, it will broaden their vision and first-hand operational experience of cybersecurity issues faced by the people at grassroots level, as opposed to the current paradigm (where majority of the officers and their work remains restricted to headquarters). Therefore, just like officers from other all-India civil services get a significant say in the decision making due to their extensive groundwork and direct first-hand experiences bestowing them with actual ground realities, Indian cybersecurity officials will also get a far greater say over most policy decisions concerning cyberthreats, cybersecurity interests and others. Further, cyberspace is ubiquitous and interacts closely with major economic and other operations in society. Therefore, affording greater say to cybersecurity officials in India will make cybersecurity central to our major policy decisions and strengthen our cybersecurity framework on a continuous basis.

Infrastructural Investments

Massive infrastructural investment is obligated to secure Indian cyberspace from possible cyberterror attacks. Considering the excessive use of cybernetworks during the global pandemic in order to avoid physical contact, many sectors of the economy have been thrown open to cyber-enabled terror attack. Therefore, India must establish sectoral CERTs in new sectors of operations, including research and development (R&D), to protect against loss of valuable IP from possible cyberterror attacks during the ongoing pandemic.[135] In addition to protecting IP,

trade secrets and preserving India's data sovereignty, it is imperative to secure financial transactions and communications (including strategic and confidential communications of private entities or government) taking place during the pandemic through cybernetworks. Thus, sectoral CERTs must be operationalised in more fields to protect, preserve and maintain the safety of Indian cyberspace. Additionally, the government must undertake structural reforms and develop disaster recovery capabilities against cyberterror attacks. It must also conduct cybersecurity drills in line with the cybersecurity drills conducted by the SCO.

The state must also change its deterrence strategy against cyber-enabled terror attacks. The security forces must deal with the launchers of cyberterror attacks as cyber militants and the government must consider creating a 'Centre for Cyber Militancy', where qualitative training to counter cyber-enabled terror attacks from these militants can be imparted to security personnel. Furthermore, a long-term cyberspace safety fund, on the lines of 'Rashtriya Rail Sanrakshan Kosh',[136] must be established to meet all cybersecurity contingencies of India.

Judicial and Educational Training

Centrally funded scheme to train judicial and legal officers on law and cyberthreats, with special emphasis on cyberterrorism, must be undertaken by the government. Cybersecurity must be introduced in the curriculum of schools and colleges; and more universities must provide opportunities to undertake specialisations in information or cybersecurity studies. This would increase awareness among the general masses and augment our capacity to produce a greater number of cybersecurity experts to meet future requirements of protecting the cyberworld from cyberterrorist activities.

Constitutional Obligation of State against Cyberterrorism

Defence against Cyberterrorism

Cyberterrorism is detrimental to both global peace and India. It threatens various dimensions of security, like energy, nuclear, water (through dams) and cyber-enabled strategic communications. A cyber-enabled terror attack may not always be an unarmed physical terror attack but, it certainly amounts to an unmanageable terror attack which impairs the virtual life of the people, including critical technological

functions and nation's cyberspace. Therefore, it is beyond doubt that a cyberterror attack, when launched outside the territorial limits of India, amounts to external aggression and is capable of causing internal disturbance in the country.[137] A cyberterror attack patently threatens the unity and integrity of the republic. The union government thus is constitutionally bound under Article 355 of the Indian Constitution to protect states from cyberterrorism amounting to external aggression and internal disturbances. The term 'aggression' under Article 355 not only comprehends armed aggression but also includes bloodless aggression.[138] It is an all-comprehensive word having wide meaning with complex dimensions.[139]

The Supreme Court (SC) ruled in Sarbananda Sonowal *v.* Union of India[140] that:

> The foremost duty of the Central Government is to defend the borders of the country, prevent any trespass and make the life of the citizens safe and secure. The Government has also a duty to prevent any internal disturbance and maintain law and order[141]…The word 'aggression' is not to be confused only with 'war'. Though war would be included within the ambit and scope of the word 'aggression' but it comprises many other acts which cannot be termed as war.[142]

Analysing the judgement, it is a well-established constitutional norm that the union government has the principal function to defend India's sovereign borders, prevent any trespass and make the life of individual citizens safe and secure. In this information age, the Indian cyberspace is not less than India's sovereign territorial domain and therefore, defence against cyber trespass and cyberterror attacks on India's cyberspace, which certainly infringe the security and safety of Indian citizens, is the primary function of the central government. Thus, it is the constitutional obligation of the Union Government under Article 355 of the constitution to secure and protect the Indian Cyberspace from any possible cyberthreats, including cyberterrorism and cyber trespass.

Further, in the current paradigm with significant threats to the republic's sovereignty emanating from cyberspace, it becomes the sovereign duty of the union under the principles of state sovereignty, to protect the Indian cyberspace to secure India's sovereign cyber interests. Moreover, after recognition of the cyberspace as an operational domain of warfare, the union is constitutionally obliged to defend India's operational war domains just like land, air and water.[143] Maintenance of territorial integrity and political independence is a recognised facet of

international customary law. Thus, protection of India's sovereign and territorial frontiers, including Indian cyberspace, is the sacrosanct and inherent duty of the Indian government, as enshrined in constitutional, jurisprudential and international law provisions.

Right to Trade and Business and Cybersecurity

Cyber operations have developed tremendously in the past few years. Today, the use of Internet is not limited to its classic functions, like communications or entertainment, and has expanded manifold in different fields, such as education, healthcare, economy, trade and transportation. This wide operational scope of utility of cyberspace has empowered it to have an undeniable level of impact on the economy. The Internet has become the backbone of everything in society; in fact, it is the lifeblood of the economy and basic infrastructure of everything due to extensive datafication.[144]

Presently, due to the impact of COVID-19 pandemic, most businesses and other offices are running through cybernetworks,[145] thereby designating cyberspace as their operational place of work.[146] This leads us to the question: what is the constitutional responsibility of the state in this regard? Article 19(1)(g) of the Indian Constitution grants the right to trade and occupation to Indian citizens, that is, every individual has the right to practise any profession or carry on any occupation, trade or business.[147]

Let us look at some judgements of the SC in this regard. The SC, while discussing Article 19(1)(g) in Sodan Singh *v.* New Delhi Municipal Committee,[148] ruled:

> The guarantee under Article 19(1)(g) extends to practice any profession, or to carry on any occupation, trade or business. The object of using four analogous and overlapping words in Article 19(1)(g) is to make the guaranteed right as comprehensive as possible to include all the avenues and modes through which a man may earn his livelihood. In a nutshell the guarantee takes into its fold any activity carried on by a citizen of India to earn his living.[149]

The SC also ruled in Anuradha Bhasin *v.* Union of India:[150]

> Moreover, fundamental rights itself connote a qualitative requirement wherein the State has to act in a responsible manner to uphold Part III of the Constitution and not to take away these rights in an implied fashion or in casual and cavalier manner[151] …

> the internet is also a very important tool for trade and commerce. The globalization of the Indian economy and the rapid advances in information and technology have opened up vast business avenues… the freedom of trade and commerce through the medium of the internet is also constitutionally protected under Article 19(1)(g)[152] …We declare that the freedom of speech and expression and the freedom to practice any profession or carry on any trade, business or occupation over the medium of internet enjoys constitutional protection under Article 19(1)(a) and Article 19(1)(g).[153]

The SC, while discussing fundamental rights in State of West Bengal *v.* Committee for Protection of Democratic Rights,[154] ruled:

> Individuals possess basic human rights independently of any constitution by reason of basic fact that they are members of the human race. These fundamental rights are important as they possess intrinsic value. Part-III of the Constitution does not confer fundamental rights. It confirms their existence and gives them protection.[155]

Furthermore, while discussing the obligation of the state to guarantee fundamental rights to everyone, the SC ruled in another case: 'If the film is unobjectionable and cannot constitutionally be restricted under Article 19(2), freedom of expression cannot be suppressed on account of threat of demonstration and processions or threats of violence…'.[156] The SC similarly ruled in Municipal Council, Ratlam *v.* Shri Vardhichand[157] that the Municipal Council cannot demonstrate its inability to maintain public health owing to budgetary constraints.

In the context of Article 19(1)(g) of Indian Constitution,[158] all these cases manifest that the fundamental right to trade and business is an assurance of liberty and a recognition of the autonomy inherent in every citizen. The state is constitutionally obliged to act responsibly to ensure that all avenues and modes admissible under law through which an individual may earn his livelihood are available to every citizen. Thus, in the current context of ongoing COVID-19 pandemic, since most businesses and companies operate through digital platforms, it is conclusive that the state is constitutionally duty-bound to secure India's cyberspace from cyberterror attacks. Today, businesses can only survive under secured cyberspace as every business operation is happening through the digital medium. This makes cybersecurity during COVID-19 pandemic a non-negotiable facet of the right to carry out business and trade.[159] Therefore, the foremost obligation of the state to secure the right to occupation in

an economy operating through cybernetworks is to guard its cyberspace against all possible attacks. Also, in this regard, the state cannot plead its inability in securing cyberspace from cyberterror attacks on any ground, including budgetary constraints. Since, as ruled in Rangarajan and Ratlam case, the State cannot run away from its primary duty, which in the given case is to secure India's cyberspace and allow the Indian citizens to use secured cyberspace to conduct business operations.

Further, the right to occupation also includes the right to a safe environment in the workplace.[160] The government has recognised the right to safe and healthy working conditions as part of fundamental rights.[161] It is matter of general prudence that in a digital workplace, secured cyberspace patently amounts to a secured workplace. Therefore, Indian citizens have the fundamental right to work in a safe and secured cyberspace as part of their right to trade and occupation.

Moreover, Article 19(1)(g) when examined with the Anuradha Bhasin judgement of the Supreme Court enacts that, the fundamental right to free trade and occupation itself connote a qualitative requirement where the state is constitutionally obligated to act in a responsible manner and uphold the fundamental right to occupation for people working in the cyberspace. Thus, to guarantee the right to trade and business to every Indian citizen, the State is under a compulsive constitutional obligation to secure India's Cyberspace from cyberterror attacks. The Supreme Court ruling in Sodan Singh, Anuradha Bhasin and Rangarajan case (in reference to the Right to trade and business in cyberspace), indisputably mandates that Right to carry out trade, occupation and businesses through cyberspace is a constitutionally protected fundamental right. Hence, due to increasing use of cyberspace in trade and commerce there emerges a new constitutional necessity for the state in India to protect its cyberspace from new formidable cyberthreats including, cyberterror attacks to guarantee every individual his fundamental right to trade and occupation.

To conclude, the complete realisation of right to trade and business in the cyberspace shall occur pursuant to a secured cyberspace only. It is the obligated duty of the state under the Indian constitution to ensure that fundamental rights are guaranteed to every individual, including those operating their business, trade and employment through cyberspace. This fundamental right is a constitutional guarantee of liberty against the state, it cannot be supressed on any ground including, cyberterror attacks. Therefore, to fulfil the constitutional necessity established under

the law in the given context that is, ensure that citizens are able to earn their living legitimately (without any form of unlawful obstruction from formidable cyberthreats) through cyberspace, the state is under a compulsive constitutional obligation to ensure provisioning of a secured cyberspace in India. The emergence of this constitutional obligation is due to the modernisation and advances occurring in the cyberspace, economy and society at large.

Cybersecurity and Ease of Doing Business Index

Today, cyberspace is providing boundless economic and business opportunities. The Internet's contribution towards the economy, as well as integration with the monetary framework, has increased stupendously.[162] In the current scenario, businesses are running effectively through cyberspace; several start-ups are internet-based; and the e-commerce industry is flourishing globally.[163] Consider the UK, where digital economy amounted to 7.7 per cent of its economy in 2018.[164] In the US, it exceeded the federal government percentage of gross domestic product (GDP) and accounted about 10 per cent of the total GDP ($2.1 trillion).[165] In 2019, the Internet economy was predicted to be one of the top six industry sectors in China (30 per cent of GDP);[166] and South Korea too was expected to show a similar growth.[167] The digital economy contributes significant share to the national GDPs of US, Brazil, Japan, India and others.[168] Further, its share during global restrictions mushroomed enormously.[169]

It is evident that the rapidly proliferating e-commerce industry has made an enormous contribution to the national GDP of many countries. Moreover, as most commercial and financial operations today operate digitally, data is considered as the new oil which is driving modern economy. Internet has, thus, become an intrinsic and a non-negotiable element to run businesses and economy in this information age. Digitalisation of economy and secured digital operations to effectuate economic development in the country are imperative. The contribution of e-commerce industry does not merely manifest the important role of cyberspace in economic operations but also reflects the indispensable role of the Internet in generating employability in the country. The presence of a secured cyberspace directly aids in the development of economy, businesses and employability in the country. Thus, cybersecurity must be regarded as one of the parameters to decide the ease of doing business index by the World Bank. This would stimulate all the countries to

make structural reforms in securing their cyberspace from all possible cyberthreats, including cyberterrorism. Further, it would significantly aid in effectively securing economic and business operations in the cyberworld. Incorporation of this parameter would act as a catalyst in establishing a secured and rule-based cyberworld in the near future. At the national level, the Indian government can include cybersecurity as one of the parameters to decide ease of doing business index for the Indian states.

International Cybersecurity Cooperation: Harmonisation of Domestic Laws

The transnational character of cyberspace warrants a global cooperative effort to counter cyberterrorism.[170] To thwart the menace of potentially ruinous cyberterrorism, countries must work towards developing a universally acceptable and effective strategy of defence and counter-measures for cyberterrorism. Many countries have progressively effectuated their cyber defences and adopted deterrence strategies to supplement their cyber defences. However, it becomes difficult to counter the threats of cyberterrorism merely on strategic national policies since cyberspace is globally homogenised and attacks may emerge overseas. International cooperation between states, therefore, is an effective cornerstone to develop an effective combat mechanism and legal framework to counteract cyberterrorism. Inadequate international regulations and uncoordinated legal mechanisms of states on cyberterrorism act as the biggest deterrent in devising an effective global strategy against cyberterrorism.

Considering the risks, cyberterrorism warrants immediate global consideration. However, as mentioned earlier, despite being acknowledged internationally as a precarious risk to global peace, no universally agreed definition for cyberterrorism exists today.[171] The next section discusses how dissension over a universal definition of cyberterrorism makes domestic interpretation of cyberterrorism in each state differ from the other. [172]

Cyberterror Law of Other Countries[173]

The UK

The Terrorism Act, 2000 is the UK legislative instrument enacting provisions about terrorism, including cyberterrorism. Section 1 of the

Act enlists three requirements to constitute an act as terrorism: intention, motive and harm. The Act provides that the act committed must intend to influence the government or international governmental organisation, or intimidate public or a section of it.[174] Also, the act should aim to advance a political, religious, radical or ideological cause.[175] Section 1(2) further lists alternative harms that an act may cause to constitute an act of terrorism. It covers terrorist acts which seriously interfere with or disrupt an electronic system.[176] The term 'electronic system' can include Internet service providers, computer providers, financial exchanges, etc.[177]

The UK law thus provides a broad definition of terrorism. It includes cases of cyberattack over non-essential infrastructure. It can be applied to a cyberattack threat in the same manner as an actual cyberattack. It even regards cases of cyberattacks designed merely to 'influence' a government as cyberterrorism, thereby eliminating the requirement of higher intentions, like coercing or intimidating a government.

Australia

Australia enacted anti-terror laws after 9/11 terror attack, as a cluster of five legislations. The Security Legislation Amendment (Terrorism) Act, 2002 inserted the definition of terrorism in Part 5.3 of the Australian Criminal Code. Section 100.1 of the Criminal Code defines terrorism. Australian law sets higher standards for an act to be construed as terrorism than the UK terror law. So, cyberattacks intending to influence only the government do not constitute cyberterrorism in Australia. The Australian law necessitates that to constitute cyberterrorism, a person by his act must intend to coerce or influence a government by intimidation.[178] Thus, the cyberattack must be coercive or intimidatory. The application of the Australian terror law in cases of cyberattacks is restricted only to attacks amounting to serious interference, disruption or destruction of electronic systems.[179] The law also includes 'political protest exemption'. It enacts that any form of protest, dissent or other will not constitute terrorism if it does not intend to cause death, or serious physical harm or endanger life, etc.[180] Thus, unlike its English counterpart, the Australian Criminal Code recognises a narrower range of cyberattacks as cyberterrorism.

Canada

Section 83.01 of the Canadian Criminal Code defines terrorism as an act or omission done in or outside Canada for a political, religious or ideological objective, to intimidate public or segment of people,

causing serious bodily harm, death, endangering a person's life, etc.[181] Further, the Canadian law also incorporates the exemption to political protests like Australia. However, it sets very high standards for an act of terrorism since it provides that such acts should 'compel' a government to act or refrain from acting in a particular way.[182] The scope of terrorism in Canadian law extends to attacks against domestic and international organisations.[183] This establishes a wider operational area against 'international government organisations' as in British law. The Canadian law also comprehends attack against an individual as an act of terrorism.[184] Further, it provides that to constitute cyberterrorism, an act should intend and cause actual interference with the essential system, service or facility.[185] This establishes another high standard in the law to operationalise the definition of terrorism in an incident of cyberattack.

Comparing the Indian Law with Other Jurisdictions

The definition of cyberterrorism put forth by Indian legislation includes a larger scope of cyber-enabled terror activities, unlike the Canadian terror law. The presence of terms 'attempting to penetrate',[186] 'likely to cause'[187] and 'knowingly or intentionally',[188] under Section 66F, provides larger operational scope to the definition of cyberterrorism in India. However, unlike Britain and Canada, the range of cyberterror activities in India does not go beyond the scope of unity, security, integrity and sovereignty of India. Also, cyber-espionage acts are covered within the ambit of cyberterrorism under Section 66F(1)(B) of the Act. The Indian law, unlike the UK and Canada, does not expressly provide for cyberattacks against international organisations as cyberterrorism. Further, the standards for an act to qualify as an act of cyberterrorism in India are much higher than in the UK terror law.

Thus, different countries provide different definitions for the act of cyberterrorism. This diversity among terror laws hinders global cooperation as these varied definitions provide different standards for an act to qualify as cyberterrorism. So, what would amount to cyberterrorism in the UK might not always amount to cyberterrorism in Canada. Therefore, to overcome this hindrance in global cooperative cybersecurity strategy, the following steps must be adopted:

1. States must accept a universally acceptable definition of cyberterrorism. This would ensure that the standards for an act amounting to cyberterrorism would be same in the domestic laws of every country. Thus, an act amounting to cyberterrorism

in one nation would also amount to cyberterrorism in another. Hence, if a country becomes a victim of a cyberterror attack originating from other nation, then the country attacked could use the legal instruments of the other country to punish the culprit(s) or even extradite the designated culprit(s).

2. States must also harmonise their domestic terror laws with each other. It would provide common procedures for prosecution and investigation of cyberterrorism and help in the global fight against cyberterrorism. This would lead to an effective, efficient and transparent mechanism for investigation and information sharing related to cyberterrorism. In addition to cooperation in investigations, it would also enable accelerated cooperation between law enforcement agencies of different countries for other purposes, like capacity-building programmes and training of officials.
3. Supplementarily, states must accelerate global prevention against cyberterrorism through more aligned synergy in intelligence sharing, cybersecurity governance, cooperation in building cybersecurity preparedness and resilience, through mutual treaties and other instruments. Each state must denominate international cooperative cybersecurity framework as a priority area in their foreign policy.
4. Efforts must also be made to evolve a universally binding and practically implementable international instrument on cyberterrorism to cease the acts of cyberterrorism globally. In order to protect its strategic cyberspace, India must strengthen international cooperation among other states and take steps to internationalise its domestic laws on cyberterrorism.

Conclusion

Cyberspace has developed as a decentralised network of communication, without any restriction over geographical boundaries of any country. Therefore, international regulation and cooperative cybersecurity framework is essential to deal with cyberterrorism effectively. Since the current framework is incapable of dealing with the menace,[189] it is time to strengthen international law to equip it to deal with cyberterrorism. India must also think about reforming its legal framework or legislating exclusive cybersecurity legislation, which may provide provisions for cyberterrorism.[190]

With the prime minister advocating the use of technology for development and administration,[191] and also due to the global pandemic, cyberspace has been integrated into various fields, like governance, public administration and trade and business operations. In addition, there is continuous integration of cyberspace with CI. Thus, a multidimensional cybersecurity framework must be introduced. The outbreak of COVID-19 has also accelerated the digitisation of economic businesses and other activities. Cyberattacks by terrorists can virtually paralyse the financial and economic operations (including Indian Goods and Services Tax [GST] network[192]) of the country. Hence, to boost the adoption of counter-measures by states against cyberterrorism and strengthen the cybersecurity framework, the World Bank must consider 'cybersecurity' as one of the parameters to decide ease of doing business index. India must also try to reduce overlapping among cybersecurity organisations and harmonise its process and laws as per the international best practices.

Further, the accelerated digital operations of business due to the pandemic has made the state constitutionally bound to protect the cyberspace of India. Article 19(1)(g) of the Constitution, read with Sodan Singh and Anuradha Bhasin cases, grants the right to practice or do any form of livelihood within the realms of law. Thus, the state must make sure that the constitutionally protected fundamental right of occupation in cyberspace of Indian citizens is protected in the current scenario. It must be noted that any business can survive and flourish in a digital platform only when there is secured cyberspace in place. Thus, the government is constitutionally bound to protect India's cyberspace from cyberthreats, including cyberterrorism.

Cyberspace, today, interacts with significant economic, business and other interests of India. So as to secure India's strategic, sovereign, economic and business interests in cyberspace, the union must incorporate stringent deterrent strategies and cybersecurity reforms at all levels of operation. It is important to look at the big picture while analysing cyberterror threats; and new mechanisms must be developed and reformatory steps need to be introduced with focus on the constitutional obligation of the state under Article 19(1)(g) and Article 355 of the Indian Constitution.

Notes

1. UNDOC, *The Use of The Internet for Terrorist Purposes*, New York: United Nations, 2012, p. iii; Kendall Scherr, 'UN Report Identifies the Internet

as a Major Tool of Terrorists and Discusses Counterterrorism Strategies', *Homeland Security Digital Library*, 24 October 2012, available at https://www.hsdl.org/c/un-report-identifies-the-internet-as-a-major-tool-of-terrorists-and-discusses-counterterrorism-strategies/, accessed on 8 June 2021.

2. Jim Garamone, 'Cyber Tops List of Threats to U.S., Director of National Intelligence Says', *DOD News*, 13 February 2018, available at https://www.defense.gov/Explore/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/, accessed on 24 April 2021; and 'India Most Attacked in the Online Sphere: National Cyber Security Coordinator Lt Gen Rajesh Pant', *The New Indian Express*, 29 January 2020, available at https://www.newindianexpress.com/nation/2020/jan/29/india-most-attacked-in-the-online-sphere-national-cyber-security-coordinator-lt-gen-rajesh-pant-2095911.html, accessed on 24 April 2021.
3. See Paul Mee and Til Schuermann, 'How a Cyber Attack could Cause the Next Financial Crisis', 14 September 2018, available at https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis, accessed on 6 March 2021.
4. James A. Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', Center for Strategic and International Studies, Washington, DC, 2002; and Nicole Perlroth and David E. Sanger, 'Cyberattacks Seem Meant to Destroy, Not Just Disrupt', *The New York Times,* 28 March 2013, available at https://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html, accessed on 28 April 2021.
5. Daniel Wagner, 'Cyber-attacks: A Battle against a Nameless, Ever-changing Foe', *The Straits Times*, 26 July 2018, available at https://www.straitstimes.com/opinion/cyber-attacks-a-battle-against-a-nameless-ever-changing-foe, accessed on 3 March 2021.
6. Rus Schuler, 'How does the Internet Work?', Standford University, 2002, available at https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm, accessed on 3 March 2021.
7. M. Glenny, *McMafia: Crime without Frontiers*, London: Random House, 2008. Also see Peter Grabosky, 'The Global Dimension of Cybercrime', in M. Galeotti (ed.), *Global Crime Today: The Changing Face of Organised Crime*, United Kingdom: Routledge, 2005, p. 146.
8. See Filippo Parodi, 'The Concept of Cybercrime and Online Threat Analysis', *International Journal of Information Security and Cybercrime*, Vol. 2, No. 1, 2013, p. 59.

9. See Erika Kraemer-Mbula, Puay Tang and Howard Rush, 'The Cybercrime Ecosystem: Online Innovation in the Shadows?', *Technological Forecasting and Social Change*, Vol. 80, No. 3, 2013, pp. 541–55. Also see Harsh Mehta, 'Stay Alert! Hackers' Most Innovative Ways to Clean your Bank Accounts', *The Economic Times*, 11 December 2019, available at https://bfsi.economictimes.indiatimes.com/news/banking/stay-alert-hackers-most-innovative-ways-to-clean-your-bank-accounts/72467533, accessed on 31 January 2021.
10. See Karishma Mehrotra, 'PM Narendra Modi's Twitter Account Hacked by "John Wick"', *The Indian Express*, 3 September 2020, available at https://indianexpress.com/article/india/twitter-account-pm-narendra-modi-hacked-6580967/, accessed on 5 March 2021; 'Twitter Accounts of Obama, Biden, Elon Musk, Bill Gates and Others Hacked to Run Bitcoin Scam', *The Economic Times*, 16 July 2020, available at https://economictimes.indiatimes.com/tech/internet/twitter-accounts-of-obama-biden-elon-musk-bill-gates-and-others-hacked-to-run-bitcoin-scam/videoshow/76990591.cms?from=mdr, accessed on 25 April 2021; Scott Steinberg, 'Cyberattacks Now Cost Companies $200,000 on Average, Putting Many Out of Business', CNBC, 13 October 2019, available at https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html, accessed on 25 April 2021; James Lewis, 'Economic Impact of Cybercrime: No Slowing Down', Center for Strategic and International Studies, Washington, DC, 2018, pp. 5–9; and 'Net Losses: Estimating the Global Cost of Cybercrime', Center for Strategic and International Studies, Washington, DC, 2014.
11. United States (US) Department of Defense, 'Department of Defense Strategy for Operating in Cyberspace', July 2011, available at https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, accessed on 20 February 2021. It states: 'Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies.'
12. Priyanka Sangani, 'Increase in State-sponsored Cyber Security Attacks on Government Bodies', *The Economic Times*, 28 April 2020, available at https://economictimes.indiatimes.com/tech/internet/increase-in-state-sponsored-cyber-security-attacks-on-government-bodies/articleshow/75431703.cms, accessed on 5 March 2021. Also see Pierluigi Paganini, '10 Biggest Cyber Espionage Cases', 11 December 2017, available at https://securityaffairs.co/wordpress/66617/hacking/cyber-espionage-cases.html, accessed on 5 March 2021.
13. David Weissbrodt, 'Cyber-Conflict, Cyber-Crime, and Cyber-Espionage', *Minnesota Journal of International Law*, Vol. 22, No. 2, pp. 371–80; Siraj

Ahmed Shaikh, 'Cyber-espionage is more difficult to pin to a state than spying in the physical world', *The Conversation*, 21 October 2004, available at https://theconversation.com/cyber-espionage-is-more-difficult-to-pin-to-a-state-than-spying-in-the-physical-world-32977, accessed on 9 June 2021; Praveen Dalal, 'Cyber Espionage Policy of India', 29 June 2016, available at http://ptlb.in/csrdci/?p=362, accessed on 2 March 2021.

14. Saikat Datta, 'PMO Fights Largest Cyber-attack', DNA, 22 August 2011, available at https://www.dnaindia.com/india/report-dna-investigation-pmo-fights-largest-cyber-attack-1578348, accessed on 25 January 2021.
15. Phil Muncaster, '10,000 Indian Government and Military Emails Hacked', *The Register*, 21 December 2012, available at https://www.theregister.com/2012/12/21/indian_government_email_hacked/, accessed on 25 January 2021.
16. 'Indian Embassy's Website Hacked by Chinese Hackers', *The Economic Times*, 18 April 2010, available at https://economictimes.indiatimes.com/tech/internet/indian-embassys-website-hacked-by-chinese-hackers/articleshow/5828342.cms, accessed on 9 June 2021. Also see 'Websites of Seven Indian Missions "Hacked", Data Dumped Online', *India TV*, 7 November 2016, available at https://www.indiatvnews.com/news/world-websites-of-seven-indian-missions-hacked-data-dumped-online-355609, accessed on 25 January 2021.
17. See Petr Hruza and Jiri Cerny, 'Cyberwarfare', *International Conference Knowledge-Based Organization*, Vol. 23, No. 1, 2017, p. 155.
18. See Joy Reo, 'DDoS Attacks can be Weapons in Cyber Warfare', n.d., available at https://www.corero.com/blog/ddos-attacks-can-be-weapons-in-cyber-warfare/, accessed on 25 January 2021. Also see David Larson, 'Cyber Warfare or Hacktivism? DDoS Attacks can be Used either Way', n.d., available at https://www.corero.com/blog/cyber-warfare-or-hacktivism-ddos-attacks-can-be-used-either-way/, accessed on 25 January 2021.
19. David Alexander, 'Pentagon to Treat Cyberspace as an Operational Domain', *Reuters*, 14 July 2011, available at https://www.reuters.com/article/us-usa-defense-cybersecurity/pentagon-to-treat-cyberspace-as-operational-domain-idUSTRE76D5FA20110714, accessed on 25 January 2021; NATO, 'Cyber Defence', available at https://www.nato.int/cps/en/natohq/topics_78170.htm, accessed on 25 January 2020.
20. See David Alexander, 'U.S. Reserves Right to Meet Cyber-attack with Force', *Reuters*, 16 November 2011, available at https://www.reuters.com/article/us-usa-defense-cybersecurity/u-s-reserves-right-to-meet-cyber-attack-with-force-idUSTRE7AF02Y20111116, accessed on 28 January 2021.

21. See 'Statement by President Donald J. Trump on the Elevation of Cyber Command', 18 August 2018, available at https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/, accessed on 28 January 2021. See, generally, Thomas Spoehr and James Di Pane, 'Elevating Cyber Command: An Overdue Step towards Enhancing Military Cyber Operations', 1 October 2018, available at https://www.heritage.org/cybersecurity/commentary/elevating-cyber-command-overdue-step-towards-enhancing-military-cyber, accessed on 28 January 2021.
22. See Steve Andriole, 'Cyberwarfare will Explode in 2020 (because it's Cheap, Easy and Effective)', *Forbes*, 14 January 2020, available at https://www.forbes.com/sites/steveandriole/2020/01/14/cyberwarfare-will-explode-in-2020-because-its-cheap-easy--effective/#478e70456781, accessed on 28 January 2021; Yuvraj Malik, 'World Coronavirus Dispatch: Govt-backed Hacking on the Rise amid Pandemic', *The Business Standard*, 28 May 2020, available at https://www.business-standard.com/article/international/world-coronavirus-dispatch-govt-backed-hacking-on-the-rise-amid-pandemic-120052800843_1.html, accessed on 16 May 2021; 'With Trump's Approval, Pentagon Launched Cyber Strikes against Iran', *The Strait Times*, 23 June 2019, available at https://www.straitstimes.com/world/united-states/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran, accessed on 16 May 2021.
23. Susan W. Brenner and Leo L. Clarke, 'Civilians in Cyberwarfare: Casualties', *SMU Science and Technology Law Review*, Vol. 13, No. 3, 2010, p. 249.
24. Maura Conway, 'Cyberterrorism: The Story so Far', *Journal of Information Warfare*, Vol. 2, No. 2, 2003, p. 36.
25. See Kendall Scherr, 'UN Report Identifies the Internet as a Major Tool of Terrorists and Discusses Counterterrorism Strategies', 24 October 2012, available at https://www.hsdl.org/c/un-report-identifies-the-internet-as-a-major-tool-of-terrorists-and-discusses-counterterrorism-strategies/, accessed on 28 January 2021.
26. See Andrew Michael Colarik, *Cyber Terrorism: Political and Economic Implications*, London: IGI Publishing, 2006, pp. 124–28.
27. United Nations Office on Drugs and Crime (UNODC), 'Counter-Terrorism', available at https://www.unodc.org/e4j/en/terrorism/module-1/key-issues/intro.html, accessed on 28 January 2021. It states: 'When considering the concept of terrorism, it is important to note that as yet, there is no global consensus regarding an agreed definition of the term "terrorism" for legal purposes.'

28. R. Rajan, 'Cyber Terrorism', in R. Rajan (ed.), *Cyber Terrorism and Military Preparedness: An International Perspective*, India: Sumit Publication, 2016, p. 7.
29. Mark M. Pollitt, 'Cyberterrorism—Fact or Fantasy', *Computer Fraud & Security*, Vol. 1998, No. 2, 1998, p. 3.
30. Foreign Broadcasting Information Service, 'Government Sets up Anti-Cyberterrorism Homepage', *Sankei Shimbun*, 10 April 2002 (FBIS-EAS-2002-0410).
31. Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell and Greg Gagnon, 'Cyberterror: Prospects and Implications', White Paper, Center for the Study of Terrorism and Irregular Warfare, Monterey, CA, 1999.
32. Daniel Ralph, Simon Ruffle, Tamara Evan, Andrew Coburn, Eireann Leverett, James Bourdeau, Rohan Gunaratna, 'Cyber Terrorism: Assessment of the Threat to Insurance', Cambridge Risk Framework Series, Centre for Risk Studies, University of Cambridge, 2017, p. 6.
33. See Peter W. Singer, 'The Cyber Terror Bogeyman', 1 November 2012, available at https://www.brookings.edu/articles/the-cyber-terror-bogeyman/, accessed on 9 June 2021. Also see Margaret Rouse, 'Cyberterrorism', available at https://searchsecurity.techtarget.com/definition/cyberterrorism, accessed on 18 February 2021.
34. For full definition, see John J. Klein, 'Deterring and Dissuading Cyberterrorism', *ASPJ Africa & Francophonie*, Vol. 9, No. 1, 2018, p. 22. Also see Rebekah Tanti-Dougall, 'Cyber Terrorism: A New Threat against the Maritime Industry', 17 July 2017, available at https://www.lexisnexis.com/legalnewsroom/public-policy/b/public-policy-law-blog/posts/cyber-terrorism-a-new-threat-against-the-maritime-industry, accessed on 21 February 2021.
35. See Sarah Gordon and Richard Ford, 'Cyberterrorism', *Computers and Security*, Vol. 21, No. 7, 2002, pp. 640–64; and Jonalan Brickey, 'Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace', *Combating Terrorism Centre Sentinel*, Vol. 5, No. 8, 2012, pp. 4–6.
36. 'VOIP Used by 26/11 Planners, 150 Test Calls made before Attack', *India Today*, 17 August 2009, available at https://www.indiatoday.in/latest%20headlines/story/VOIP-used-by-26-11-planners-150-test-calls-made-before-attack-54592-2009-08-17, accessed on 21 February 2021.
37. See n. 10.
38. E. Vigano, M. Loi and E. Yaghmaei, 'Cybersecurity of Critical Infrastructure', in Markus Christen, Bert Gordijn and Michele Loi (eds), *The Ethics of Cybersecurity*, Switzerland: Springer, 2021, pp. 159–68.
39. George Osborne, 'Chancellor's Speech to GCHQ on Cyber Security', National Cyber Security Plan, Government Communications

Headquarters, 17 November 2015, available at https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security, accessed on 21 February 2021.

40. See Norman Ermy, 'The Myth of Cyberterrorism', *Journal of Information Warfare*, Vol. 4, No. 1, 2015, pp. 80–89; and Dan-Calin Besliu, 'Cyber Terrorism—A Growing Threat in the Field of Cyber Security', *International Journal of Information Security and Cybercrime*, Vol. 6, No. 2, 2017, pp. 35–39.
41. Jian Hua and Sanjay Bapna, 'The Economic Impact of Cyber Terrorism', *The Journal of Strategic Information Systems*, Vol. 22, No. 2, 2013, pp. 175–86.
42. Jorge Valero, 'Hacker's Bombard Aviation Sector with Over 1,000 Attacks Per Month', *Euractiv*, 11 July 2016, available at https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/, accessed on 21 February 2021. Also see Danielle Stormy K. Friday, 'Cyber-Terrorism for Beginners: A Rising Threat', *Homeland Security Today*, 24 June 2020, available at https://www.hstoday.us/subject-matter-areas/cybersecurity/cyber-terrorism-for-beginners-a-rising-threat/, accessed on 21 February 2021.
43. Aviv Cohen, 'Cyberterrorism: Are We Legally Ready?', *The Journal of International Business & Law*, Vol. 9, No. 1, 2009, pp. 6–10.
44. Debarati Halder, 'Information Technology Act and Cyber Terrorism: A Critical Review', in P. Madhava Soma Sundaram and Syed Umarhathab (eds), *Cyber Crime and Digital Disorder*, Tirunelveli, Tamil Nadu: Manonmaniam Sundaranar University, Publications Division, 2011, p. 79.
45. Computer systems which superintend the working CI or CI itself.
46. Monkey Cage and Debak Das, 'An Indian Nuclear Power Plant Suffered a Cyberattack. Here's What You Need to Know', *The Washington Post*, 4 November 2015, available at https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/, accessed on 19 May 2021.
47. Kerian Hardy and George Williams, 'What is Cyberterrorism? Computer and Internet Technology in Legal Definitions of Terrorism', in Thomas M. Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism: Understanding, Assessment, and Response*, New York: Springer, 2014, p. 2.
48. Andrew Dornbierer, 'How Al-Qaeda Recruits Online', *The Diplomat*, 13 September 2011, available at https://thediplomat.com/2011/09/how-al-qaeda-recruits-online/, accessed on 21 February 2021. Also see Antonia Ward, 'ISIS's Use of Social Media still Poses a Threat to Stability in the Middle East and Africa', 11 December 2018, available at https://www.

rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html, accessed on 21 February 2021.

49. Murat Dogrul, Adil Aslan and Eyyup Celik, 'Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism', in C. Czosseck, E. Tyugu and T. Wingfield (eds), *2011 3rd International Conference on Cyber Conflict: Proceedings*, Tallinn, Estonia: IEEE Publications, 2011, p. 31. Also see Martha Crenshaw Hutchinson, 'The Concept of Revolutionary Terrorism', *Journal of Conflict Resolution*, Vol. 16, No. 3, 1972, p. 384.
50. 'How Terrorists are Using Social Media', *The Telegraph*, 4 November 2014, available at https://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html, accessed on 21 February 2021.
51. Swaran Singh and Jayanna Krupakar, 'Indo-US Cooperation in Countering Cyber Terrorism: Challenges and Limitations', *Strategic Analysis*, Vol. 38, No. 5, 2014, p. 704.
52. Hardy and Williams, 'What is Cyberterrorism? Computer and Internet Technology in Legal Definitions of Terrorism', n. 47. Also see Anne Stenersen, '"Bomb-Making for Beginners": Inside an Al-Qaeda E-Learning Course', *Perspectives on Terrorism*, Vol. 7, No. 1, 2013, pp. 25–37.
53. Anne Stenersen, 'The Internet: A Virtual Training Camp?', *Terror and Political Violence*, Vol. 20, No. 2, 2008, pp. 215–33.
54. See United Nations (UN), 'Secretary-General calls Cyberterrorism using Social Media, Dark Web, "New Frontier" in Security Council Ministerial Debate', 25 September 2019, available at https://www.un.org/press/en/2019/sgsm19768.doc.htm, accessed on 8 March 2021.
55. Yujin Sung, 'Cyber War against Terrorism: Do Citizen Hackers Really Help?', *Minnesota Journal of International Law*, 27 November 2015, available at https://minnjil.org/2015/11/27/cyber-war-against-terrorism-do-citizen-hackers-really-help/, accessed on 9 June 2021.
56. Shruti Pandalai, 'ISIS in India: The Writing on the (Facebook) Wall: India Needs to take the Threat of ISIS Recruitment on Social Media Seriously', *The Diplomat*, 6 May 2016, available at https://thediplomat.com/2016/05/isis-in-india-The-writing-on-the-facebook-wall/, accessed on 21 February 2021.
57. Anne Speckhard, 'ISIS and the Militant Jihad on Instagram', *Modern Diplomacy*, 3 August 2020, available at https://moderndiplomacy.eu/2020/08/03/isis-and-the-militant-jihad-on-instagram/, accessed on 16 May 2021.
58. 'How Terrorists are Using Social Media', n. 50; Tamar Mitts, 'From Isolation to Radicalization: Anti-Muslim Hostility and Support for ISIS

in the West', *American Political Science Review*, Vol. 113, No. 1, 2019, pp. 173–94; and Charles Hymas, 'ISIL Extremists using Instagram to Promote Jihad and Incite Support for Terror Attacks on the West', *The Telegraph*, 11 May 2019, available at https://www.telegraph.co.uk/news/2019/05/11/isil-extremists-using-instagram-promote-jihad-incite-support/, accessed on 16 May 2021.

59. Efraim Benmelech and Esteban F. Klor, 'What Explains the Flow of Foreign Fighters to ISIS?', *Terrorism and Political Violence*, Vol. 32, No. 7, 2018, pp. 3–7, 22–23; Jessica Trisko Darden, 'Tackling Terrorists' Exploitation of Youth', AEI, 2019, pp. 3–9; Salim Abbadi, 'Jordan in the Shadow of ISIS', *Counter Terrorist Trends and Analyses*, Vol. 7, No. 2, 2015, pp. 9–10; and Emerson T. Brooking and P.W. Singer, 'How Social Media is being Weaponized across the World', *The Atlantic*, November 2016, available at https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/, accessed on 16 May 2021.
60. Liam Stack, 'How ISIS Expanded its Threat', *The New York Times*, 14 November 2015, available at https://www.nytimes.com/interactive/2015/11/14/world/middleeast/isis-expansion.html, accessed on 3 March 2021.
61. Ibid.; 'From Jordan to Jihad: The Lure of Syria's Violent Extremist Groups', Mercy Corps, 2015, pp. 4–10.
62. See Melanie Schweiger, 'India's Cyber Challenge: Indian Mujahideen', *The Diplomat*, 9 December 2014, available at https://thediplomat.com/2014/12/indias-cyber-challenge-indian-mujahideen/, accessed on 8 March 2021. Also see Shubham Chaudhary, 'Cyber Terrorism: World Wide Weaponisation!', *International Journal of Law and Legal Jurisprudence Studies*, Vol. 3, No. 2, 2016, pp. 283–86.
63. Nelson, Choi, Iacobucci, Mitchell and Gagnon, 'Cyberterror: Prospects and Implications', n. 31.
64. Dogrul, Aslan and Celik, 'Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism', n. 49.
65. Shri Motilal Vora, 'Unstarred Question No. 3469', Rajya Sabha, 26 April 2013, available at https://rajyasabha.nic.in/rsnew/Questions/ShowQn.aspx?tk=3ccd178a-c72a-4599-953f-e9dbf5380a70, accessed on 22 February 2021.
66. Ibid.
67. See, generally, Phillip W. Brunst, 'Use of the Internet by Terrorists: A Threat Analysis', in Centre of Excellence—Defence Against Terrorism (ed.), *Responses to Cyber Terrorism*, Ankara, Turkey: IOS Press, 2008, p. 38.
68. Ibid.

69. Council of Europe, 'Convention on Cybercrime', European Treaty Series No. 185, available at https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, accessed on 8 March 2021.
70. See Council of Europe, 'Budapest Convention and Related Standards', available at https://www.coe.int/en/web/cybercrime/the-budapest-convention, accessed on 5 March 2021.
71. Council of Europe, 'Convention on Cybercrime', n. 69, Chapter II.
72. Ibid., Chapter III.
73. United Nations General Assembly (UNGA), 'United Nations Global Counter-Terrorism Strategy', UN Doc A/Res/60/288, 20 September 2006.
74. UNGA, 'United Nations Global Counter-Terrorism Strategy Review', A/RES/72/284, 2 July 2018.
75. UNGA, 'Strengthening the Capability of the United Nations System to Assist Member States in Implementing the United Nations Global Counter-Terrorism Strategy', UN Doc A/Res/71/291, 15 June 2017.
76. UN Secretary-General, 'Capability of the United Nations System to Assist Member States in Implementing the United Nations Global Counter Terrorism Strategy', UN Doc A/71/858, 3 April 2017.
77. See UNOCT, 'Cybersecurity', available at https://www.un.org/counterterrorism/cybersecurity, accessed on 5 March 2021.
78. See UNOCT, 'Programmes and Projects on Cyberterrorism', available at https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity, accessed on 11 March 2021.
79. UNSC, SC Res 2341, SCOR, UN Doc S/Res/2341, 13 February 2017. See also UNSC, SC Res 2370, SCOR, UN Doc S/Res/2370, 2 August 2017. The UNSC noted its concern over the use of Internet to facilitate terrorist acts, as well as its use to incite, recruit, fund or plan terrorist acts.
80. See UNSC, SC Res 1373, SCOR, UN Doc S/Res/1373, 28 September 2001. Also see UNSC, SC Res 1624, SCOR, UN Doc S/Res/1624, 14 September 2005.
81. UNSC, 'Statement by the President of the Security Council', UN Doc S/PRST/2016/6, 11 May 2016.
82. Ministry of External Affairs, Government of India, 'BRICS Counter-Terrorism Strategy', 17 November 2020, available at https://www.mea.gov.in/bilateral-documents.htm?dtl/33204/BRICS_CounterTerrorism_Strategy, accessed on 17 May 2021.
83. 'SCO Responds to Cyber Challenges', *InfoSCO*, 9 June 2011, available at http://infoshos.ru/en/?idn=8349, accessed on 8 March 2020.

84. 'Structure of the Shanghai Cooperation Organisation', *SCO*, available at http://eng.sectsco.org/structure/20170109/190929.html, accessed on 18 March 2021.
85. 'SCO Fighting Cyber Terrorism', *CCDCOE*, 2013, available at https://ccdcoe.org/incyder-articles/sco-fighting-cyber-terrorism/#identifier_1_2561, accessed on 8 March 2021. Also see 'SCO RATS Council in Tashkent Approves Initiatives to Counter Cyberterrorism', *Interfax*, 15 March 2019, available at https://interfax.com/newsroom/top-stories/21028/, accessed on 8 March 2021; 'The 22nd session of Council of Regional Anti-terror Structure of SCO hosted in Tashkent', UZREPORT, 2 April 2013, available at https://uzreport.news/politics/the-22nd-session-of-council-of-regional-anti-terror-structure-of-sco-hosted-in-tashkent, accessed on 9 June 2021.
86. See Aygul Ospanova, 'Kazakhstan Proposes Establishing Cyberterrorism Center at SCO Summit', *Caspian News*, 16 June 2019, available at https://caspiannews.com/news-detail/kazakhstan-proposes-establishing-cyberterrorism-center-at-sco-summit-2019-6-15-20/, accessed on 8 March 2021.
87. See Liu Xuanzun, 'SCO Carries out Online Anti-Terrorism Drill', *Global Times*, 12 December 2019, available at https://www.globaltimes.cn/content/1173369.shtml, accessed on 8 March 2021.
88. UNGA, 'Letter, 9 Jan. 2015, from China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan', UN Doc A/69/723, 22 January 2015.
89. See Bruce Sterling, 'An International Code of Conduct for Information Security', *Wired*, 2 February 2014, available at https://www.wired.com/beyond-the-beyond/2020/02/international-code-conduct-information-security/, accessed on 8 March 2021.
90. UNGA, 'Letter, 9 Jan. 2015, from China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan', n. 88, Article 2(4).
91. Ibid., Article 2.
92. Ibid., Article 2(6).
93. Ibid., Article 2(7).
94. 'About CISA', available at https://www.dhs.gov/cisa/about-cisa, accessed on 8 March 2021.
95. CISA, 'Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure', 28 October 2020, available at https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure, accessed on 8 March 2021.

96. Terri Moon Cronk, 'White House Releases First National Cyber Strategy in 15 Years', DOD News, 21 September 2018, available at https://www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/, accessed on 8 March 2021.
97. US Government, 'National Cyber Strategy of the United States of America', Washington, DC, September 2018, p. 3.
98. Ibid., p. 21.
99. Jasper Frei, 'Israel's National Cybersecurity and Cyberdefense Posture', Center for Security Studies, ETH Zurich, 2020, pp. 9–12.
100. Ibid.
101. 'Success Story: Israel National Cyber Directorate', *NIST*, 15 October 2019, available at https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate, accessed on 9 June 2021.
102. This resolution forms the basis for the Israel cybersecurity framework of 2017.
103. Deborah Housen-Couriel, 'National Cyber Security Organisation: ISRAEL', NATO Cooperative Cyber Defence Centre of Excellence, 2017, pp. 7–11.
104. 'National Cyber Security Strategy 2016 to 2021', available at https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, accessed on 8 March 2021.
105. Gordon Corera, 'Cybersecurity: Queen Opens Centre to Protect against Attacks', BBC, 14 February 2017, available at https://www.bbc.com/news/uk-38964996, accessed on 11 March 2021.
106. Added via amendment to the Act in 2008 after 26/11 terror attack.
107. Information Technology Act, 2000 (Act 21 of 2000), Chapter III, Section 66F(2).
108. Ibid., Section 66F(1)(A)(i).
109. Ibid., Section 66F(1)(A)(ii).
110. Ibid., Section 66F(1)(A)(iii).
111. Ibid., Section 66F(1)(B).
112. Ibid., Section 70.
113. Ibid., Section 70(3).
114. Ibid.
115. The NCIIPC is an organisation under the National Technical Research Organisation (NTRO).
116. S.R. Bhansali, *Commentary on the Information Technology Act*, India: Universal Law Publishing, 2015, pp. 308–308A.

117. 'Govt Approves Setting up of Defence Cyber Agency', *The Times of India*, 17 November 2019, available at http://timesofindia.indiatimes.com/articleshow/72264836.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, accessed on 8 March 2021.
118. Rajat Pandit, 'Agencies take Shape for Special Operations, Space, Cyber War', *The Times of India*, 16 May 2019, available at https://timesofindia.indiatimes.com/india/india-begins-setting-up-new-tri-service-agencies-to-handle-special-operations-space-and-cyberspace/articleshow/69346012.cms, accessed on 8 March 2021.
119. Information Technology Act, 2000 (Act 21 of 2000), Section 70B(4); and Ministry of Home Affairs, 'Cyber Security', 18 December 2018, available at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474, accessed on 28 March 2021.
120. Read Information Technology Act, 2000 (Act 21 of 2000), s. 70b, cl. 4.
121. See Ministry of Power, 'Four Sectoral Computer Emergency Response Teams to Mitigate Cyber Security Threats in Power Systems', 20 March 2017, available at https://pib.gov.in/PressReleasePage.aspx?PRID=1484949, accessed on 8 March 2021.
122. See Shri Rajkumar Dhoot, 'Reply to Unstarred Question No. 979', *Rajya Sabha*, 13 December 2013, available at https://rajyasabha.nic.in/rsnew/Questions/ShowQn.aspx, accessed on 10 June 2021. Also see Ministry of Finance, 'Report of the Working Group for Setting up of Computer Emergency Response Team in the Financial Sector (Cert-Fin)', 2017, pp. 47–51, available at https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf
123. Ministry of Communication and Information Technology, 'National Cyber Security Policy—2013', 2013, p. 5, available at https://dit.tripura.gov.in/sites/default/files/National%20Cyber%20Security%20Policy_0_0.pdf, accessed on 10 June 2021.
124. Shri Anil Desai, 'Q No. 2852: Cyber Attacks on Organisations in the Country', *Rajya Sabha*, 22 March 2013, available at https://rajyasabha.nic.in/rsnew/Questions/ShowQn.aspx, accessed on 8 March 2021.
125. 'Amended NIA Act with Powers to Probe Abroad Comes into Force', *The Economic Times*, 2 August 2019, available at https://economictimes.indiatimes.com/news/defence/amended-nia-act-with-powers-to-probe-abroad-comes-into-force/articleshow/70498926.cms, accessed on 8 March 2021.
126. See Nayanima Basu, 'Self-reliant India will Automatically be More Internationalist: Foreign Secretary Shringla', *The Print*, 15 May 2020, available at https://theprint.in/diplomacy/self-reliant-india-will-

automatically-be-more-internationalist-foreign-secretary-shringla/422461/, accessed on 28 March 2021.

127. Yuthika Bhargave, 'India Third Most Vulnerable Country to Cyber Threats', *The Hindu*, 5 April 2018, available at https://www.thehindu.com/news/national/india-third-most-vulnerable-country-to-cyber-threats/article23437238.ece, accessed on 28 March 2021.
128. Neeraj Chauhan, 'Almost 300% Rise in Cyber Attacks in India in 2020, Govt tells Parliament', *Hindustan Times*, 23 March 2021, available at https://www.hindustantimes.com/india-news/almost-300-rise-in-cyber-attacks-in-india-in-2020-govt-tells-parliament-101616496416988.html, accessed on 19 May 2021; Devina Sengupta, 'Cyber-attacks in India Surge since Lockdown', *The Economic Times*, 25 June 2020, available at https://economictimes.indiatimes.com/tech/internet/cyber-attacks-in-india-surge-since-lockdown/articleshow/76591994.cms, accessed on 28 March 2021; and UNSC, 'ISIL must be Defeated in Cyberspace, Under-Secretary-General tells Security Council, as Terrorist Group takes Advantage of Pandemic-related Disruptions', Security Council SC/14433, 10 February 2021, available at https://www.un.org/press/en/2021/sc14433.doc.htm, accessed on 9 June 2021.
129. See Amrita Nayak Dutta, 'Indian Army Faced Two Cyberattack Attempts Every Month in 2019', *The Print*, 25 November 2019, available at https://theprint.in/defence/indian-army-faced-two-cyberattack-attempts-every-month-in-2019/325008/, accessed on 28 March 2021.
130. Amaresh Pujari, 'Cyber Terrorism: World Wide Weaponisation!', n.d., available at https://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf, accessed on 28 March 2021.
131. 'India Faces Serious Threat from Cyber Terrorism, Warns Expert', *Firstpost*, 31 January 2017, available at https://www.firstpost.com/business/biztech/india-faces-serious-threat-from-cyber-terrorism-warns-expert-1869729.html, accessed on 28 March 2021.
132. Kamaljit Kaur Sandhu, 'India Vulnerable to Cyber-attacks but doesn't have Capacity to Deal with it: Home Secretary', *India Today*, 31 May 2018, available at https://www.indiatoday.in/india/story/india-vulnerable-to-cyber-attacks-but-doesn-t-have-capacity-to-deal-with-it-home-secretary-1247247-2018-05-31, accessed on 28 March 2021.
133. Pavan Duggal, 'India Needs a Dedicated Cyber Security Law', *The Tribune*, 24 February 2021, available at https://www.tribuneindia.com/news/comment/india-needs-a-dedicated-cyber-security-law-216669, accessed on 17 May 2021; and Mohd Ujaley, 'Dedicated Legislation for Cyber Security is Needed: Pavan Duggal', *Express Computer*, 25 July 2018, available at https://www.expresscomputer.in/magazine/dedicated-legislation-

for-cyber-security-is-needed-pavan-duggal/13378/, accessed on 17 May 2021.

134. Sudhi Ranjan Sen, 'Centre may Create Single Agency for Cyber Defence', *Hindustan Times*, 12 November 2019, available at https://www.hindustantimes.com/india-news/centre-may-create-single-agency-for-cyber-defence/story-pD3QUcNvU2a9THFCF01SMO.html, accessed on 28 March 2021. Also see Sanjay Chhabra, 'India's National Cyber Security Policy (NCSP) and Organisation—A Critical Assessment', *Naval War College Journal*, Vol. 26, 2014, pp. 64–68.
135. Sectoral CERT for R&D is very essential considering the huge financial investments in R&D of COVID-19 vaccines, and similarly other dimensional subjects.
136. 'Rashtriya Rail Sanrakshan Kosh', available at https://pib.gov.in/Pressreleaseshare.aspx?PRID=1592434, accessed on 15 March 2021.
137. Cameron H. Bell, 'Cyber Warfare and International Law: The Need for Clarity', *Towson University Journal of International Affairs*, Vol. 51, No. 2, 2018, pp. 28–31, 38. Also see Joshua A. Mendoza, 'Cyber Attacks and the Legal Justification for an Armed Response', Master's Thesis, United States Army Command and General Staff College, 2017; Jonathan A. Ophardt, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield', *Duke Law & Technology Review*, Vol. 9, No. 1, 2010, pp. 1–28; and Oona A. Hathaway, Rebecca Crootof, Philip Levitz and Haley Nix, 'The Law of Cyber-Attack', *California Law Review*, Vol. 100, No. 4, 2012, p. 817.
138. Justice A.K. Patnaik (ed.), *DD Basu Shorter Constitution of India*, Haryana: Lexis Nexis, 2018, p. 1857.
139. Ibid.
140. Sarbananda Sonowal *v.* Union of India, AIR 2005 SC 2920.
141. Ibid., para 32.
142. Ibid., para 355.
143. Read Oscar Schachter, 'The Right of States to Use Armed Force', *Michigan Law Review*, Vol. 82, No. 5, 1984, p. 1620. See also Thomas M. Franck, 'Terrorism and the Right of Self-Defense', *American Journal of International Law*, Vol. 95, No. 4, 2001, pp. 839–43.
144. Read Clare Southerton, 'Datafication', in Laurie A. Schintler and Connie L. McNeely (eds), *Encyclopedia of Big Data*, Springer, 2020, available at https://link.springer.com/referenceworkentry/10.1007/978-3-319-32001-4_332-1?error=cookies_not_supported&code=c89f29f0-c31b-4211-bce3-f6a675da1538, accessed on 9 June 2021.

145. 'Google Report: Digital Dependence is Growing in Lockdown', *The Economic Times*, 30 April 2020, available at https://brandequity.economictimes.indiatimes.com/news/digital/google-report-digital-dependence-is-growing-in-lockdown/75441489, accessed on 10 March 2021.
146. 'The New Digital Workplace—Overcoming the Limits of Time and Place', 23 September 2020, available at https://www.verizon.com/about/news/new-digital-workplace-overcoming-limits, accessed on 11 March 2021; and 'Digital Workplace in the Era of Covid-19', 2 April 2020, available at https://www.rolandberger.com/en/Point-of-View/Digital-workplace-in-the-era-of-Covid-19.html, accessed on 11 March 2021. See also Saurabh Kumar Mallick v. The Comptroller and Auditor General of India, 151 (2008) DLT 261 and Biplab Kumar Das *v.* IDBI Bank Ltd. and Ors., 2017 LLR 114.
147. M.P. Singh (ed.), *V.N. Shukla's Constitution of India*, 13th edition, Lucknow: EBC, 2017, p. 175.
148. Sodan Singh *v.* New Delhi Municipal Committee, 1989 SCC (4) 155: AIR 1989 SC 1988. Also see State of Bombay *v.* R.M.D. Chamarbaugwala, AIR 1957 SC 699. The SC had observed: 'It is the duty of the State to secure to every citizen, men and women, the right to an adequate means of livelihood.'
149. Sodan Singh v. New Delhi Municipal Committee, 1989 SCC (4) 155: AIR 1989 SC 1988, para 1.
150. Anuradha Bhasin v. Union of India, 2020 SCC Online SC 25, Writ Petition (Civil) No. 1031/2019.
151. Ibid., para 15.
152. Ibid., para 27.
153. Ibid., para 152(b).
154. State of West Bengal v. Committee for Protection of Democratic Rights, 2010 (2) SCALE 467.
155. Ibid., para 41.
156. S. Rangarajan v. P. Jagjivan Ram, 1989 SCR (2) 204, 1989 SCC (2) 574.
157. Municipal Council, Ratlam v. Shri Vardhichand, 1980 AIR 1622, 1981 SCR (1) 97.
158. Right to practise any profession or to carry on any occupation, trade or business.
159. John Xavier, 'Interpol Says Cybercriminals are Targeting Large Corporations, Governments', *The Hindu*, 11 August 2020, available at https://www.thehindu.com/sci-tech/technology/interpol-says-cybercriminals-are-targeting-large-corporations-governments/article32324092.ece, accessed on 11 March 2021.

160. 'International Covenant on Economic, Social and Cultural Rights', 1966, Article 7(b), available at https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx, accessed on 10 June 2021. See also Ministry of Labour and Employment, 'National Policy on Safety, Health and Environment at Work Place', 6 August 2013, available at https://www.ilo.org/asia/WCMS_182422/lang--en/index.htm, accessed on 10 June 2021. It states, 'Government of India firmly believes that without safe, clean environment as well as healthy working conditions, social justice and economic growth cannot be achieved and that safe and healthy working environment is recognized as a fundamental human right.'
161. Ibid.
162. United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2019*, UNCTAD/DER/2019, September 2019, pp. 15–21, available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf, accessed on 21 January 2021. Also see World Economic Forum, *The Global Information Technology Report 2016: Innovating in the Digital Economy*, Geneva: World Economic Forum, 2016, p. 39.
163. Sanjeev Saxena, 'The Next Wave of Digitization in E-Commerce Fulfilment', *The Economic Times*, 30 October 2018, available at https://retail.economictimes.indiatimes.com/news/e-commerce/e-tailing/the-next-wave-of-digitization-in-e-commerce-fulfillment/66427562, accessed on 27 March 2021.
164. 'Digital Sector Worth More than £400 Million a Day to UK Economy', 5 February 2020, available at https://www.gov.uk/government/news/digital-sector-worth-more-than-400-million-a-day-to-uk-economy, accessed on 23 March 2021.
165. The Boston Consulting Group, 'Report on the Internet Economy in the G20', March 2012, available at https://www.bcg.com/publications/2012/technology-digital-technology-planning-internet-economy-g20-4-2-trillion-opportunity, accessed on 9 June 2021; David Shepardson, 'Internet Sector Contributes $2.1 Trillion to U.S. Economy: Industry Group', *Reuters*, 27 September 2017, available at https://www.reuters.com/article/us-usa-internet-economy-idUSKBN1WB2QB, accessed on 10 June 2021.
166. Longmei Zhang and Sally Chen, 'China's Digital Economy: Opportunities and Risks', IMF Working Paper Series WP/19/16, 2019, p. 4.
167. UNCTAD, *Digital Economy Report*, New York: United Nations Publications, 2019, pp. 13–20.
168. Ibid.
169. See 'Global e-Commerce Jumps to $26.7 Trillion, Fuelled by COVID-19', *UN News*, 3 May 2021, available at https://news.un.org/en/story/2021/05/1091182, accessed on 9 June 2021.

170. 'Need for Coordinated Global Action against Cyber Terrorism: Jaishankar', *The Economic Times*, 12 November 2019, available at https://government.economictimes.indiatimes.com/news/secure-india/need-for-coordinated-global-action-against-cyber-terrorism-jaishankar/72032131, accessed on 11 March 2021.
171. UNODC, 'Counter-Terrorism', n. 27.
172. Hardy and Williams, 'What is Cyberterrorism? Computer and Internet Technology in Legal Definitions of Terrorism', n. 47, p. 4.
173. The problem of dissension over the definition of cyberterrorism exists with most countries. However, to understand it better, discussion over cyberterror laws is limited to the countries from commonwealth jurisdiction.
174. Terrorism Act, 2000, Section 1(1)(b).
175. Ibid., Section 1(1)(c).
176. Ibid., Section 1(2)(e).
177. Also see Department of Home, 'The Definition of Terrorism: A Report by Lord Carlile of Berriew Q.C. Independent Reviewer of Terrorism Legislation', March 2007, p. 40.
178. Australian Criminal Code Act, 1995 (Act 12 of 1995), Section 100.1(1)(c).
179. Ibid., Section 100.1(2)(f).
180. Ibid., Section 100.1(3).
181. Canadian Criminal Code, 1985, Section 83.01(1).
182. Ibid., Section 83.01(1)(b)(i)(B).
183. Ibid.
184. Ibid., Section 83.01(1)(b)(ii)(B).
185. Ibid., Section 83.01(1)(b)(ii)(E).
186. Information Technology Act, 2000 (Act 21 of 2000), Chapter III, Section 66F(1)(A)(ii).
187. Ibid., Section 66F(1)(A).
188. Ibid., Section 66F(1)(B).
189. 'International Law Not Ready to Deal with Cyberattacks, Says India to the Security Council', *The Indian Express*, 14 February 2017, available at https://indianexpress.com/article/technology/tech-news-technology/international-law-not-ready-to-deal-with-cyberattacks-says-india-4524015/, accessed on 11 March 2021.
190. Ujaley, 'Dedicated Legislation for Cyber Security is Needed: Pavan Duggal', available at https://www.expresscomputer.in/magazine/dedicated-legislation-for-cyber-security-is-needed-pavan-duggal/13378/, accessed on 11 March 2021.

191. 'Make the Best of Technology to Deal with Administrative Delays: Modi Tells Bureaucrats', *Livemint*, 21 April 2018, available at https://www.livemint.com/Politics/IowVurhH8rTaOPqc7GqNMJ/Make-the-best-of-technology-to-deal-with-administrative-dela.html, accessed on 12 March 2021; and 'Prime Minister Narendra Modi Advocates Use of IT for Speedy Delivery of Justice', *NDTV*, 3 April 2017, available at https://www.ndtv.com/india-news/prime-minister-narendra-modi-advocates-use-of-it-for-speedy-delivery-of-justice-1676448, accessed on 12 March 2021.
192. M. Rajendran, 'GST Network could be Vulnerable to Cyber-attacks: Experts', *The New Indian Express*, 28 June 2017, available at https://www.newindianexpress.com/nation/2017/jun/28/gst-network-could-be-vulnerable-to-cyber-attacks-experts-1621637--1.html, accessed on 12 March 2021.