VOL. I/ISSUE I/2024

A PAVAN DUGGAL ASSOCIATES INITIATIVE

INTERNATIONAL JOURNAL ON CYBERLAW, CYBERCRIME & CYBERSECURITY

WWW.PAVANDUGGALASSOCIATES.COM

CYBER FORENSICS, CYBER-CRIMES AND CYBER-TERRORISM: 3 "CS" AND THE FUTURE OF WORLD ORDER

- **Abstract**

We live in a world where right from a child to an elderly, most populations are extremely dependent on the internet and cannot survive without exchange of information and networking, on a daily basis. We are constantly at a threat of losing to the global information and network battle. Cybercrimes, especially cyber terrorism have become growing concerns since mankind is no more constantly vulnerable to the havoc of a physical war but is now exposed to the new possibilities of the large-scale damage that cybercrimes can cause to world order. Over the years, cyber terrorism has become the mass medium to promote and perpetrate terrorism. The ever-growing dependence on technology and its constant assimilation into the changing environment can come with both negative and positive consequences. The negative consequences cannot be mitigated merely by changing laws but also by making sure the associated forces are in tandem with the law and are equipped to respond to the growing threats that cybercrimes pose. There is a need for us to form intellectual armies and forces to fight new age wars. This paper examines and analyses the intersection of cyber forensics and counter-terrorism measures in the area of cybercrimes, particularly keeping the Indian perspective in mind and, how the transatlantic and international mechanisms affect it.

Keywords: *Cybercrimes, cyberterrorism, cyber forensics, intellectual armies, information and networking.*

- **Introduction, Background, Aims and Objectives-Context**

With the rise in issues of grave concern like cyber terrorism, cyber stalking, cyber extortion, etc., cyber forensics acts as an aid in investigating criminal cases concerning national security, public order etc. and also for adducing solid admissible evidences.[1] The economic and political prospects to adversely use the network for malicious purposes have also increased, which is why today, cybersecurity plays a very important role at the international/national decision-making level.

Modern problems require innovative solutions to address emerging crimes and these solutions can be found in the research and development of digital/cyber forensics. International actors, specifically the superpowers with immense amounts of technological expertise or potential must and should make changes to their security policies and contribute to build technical and legal capacities of prosecutors and forensic teams to meet the challenges of vague liability and accountability in cyberspace[2]. Forensic science can largely contribute in bridging the gap between the laws and the dynamic environment of

[1] Dr. Anjani Singh Tomar, Tools used in Cyber Forensics, Cyber Forensics in Combating Cybercrimes, 3 PIJR, (Sept. 2014).

[2]*Cyber-defense Strategies for Contending with Non-state Actors: A Review and Assessment of Existing Proposals*, YALE REV. INT'L STUD., (Dec. 2017).

cyberspace, since cybercrime is an evolving form of transnational crime and is multifaceted. UNODC identifies the availability of investigation tools like forensic software as essential law enforcement tools[3].

The research seeks to explore the issue of lack of adequate cyber forensic intervention to combat cybercrimes, specifically cyber terrorism. Owing to the inadequacy of sufficient information, research and official reports extensively dealing with the topic, through this research, an effort is made to throw light upon this area and provide suggestions to mitigate the threats that cybercrimes pose.

- **Significance of the Research and Research Issues**

Cybercrimes are a direct threat to humankind and have multi-dimensional impacts like penal, human rights and national security implications[4]. Cyber forensics can solve both short and long-term consequences of such crimes since it is not only a preventive tool but also a mitigating tool, developing with changing sciences and its advancements.

- These complex notions of what cyberterrorism is have complicated how law enforcement agencies and government organizations in various countries conceptualize and defend against potential cyberterror attacks. As such, the purpose of this chapter is to examine the legal challenges that this criminal phenomenon has brought to national and international communities, in addition to describing forensic practices related to cyberterrorism. This chapter concludes with a discussion of criminological and theoretical aspects currently applied to the study of cyberterrorism
- These complex notions of what cyberterrorism is have complicated how law enforcement agencies and government organizations in various countries conceptualize and defend against potential cyberterror attacks. As such, the purpose of this chapter is to examine the legal challenges that this criminal phenomenon has brought to national and international communities, in addition to describing forensic practices related to cyberterrorism. This chapter concludes with a discussion of criminological and theoretical aspects currently applied to the study of cyberterrorism
- These complex notions of what cyberterrorism is have complicated how law enforcement agencies and government organizations in various countries conceptualize and defend against potential cyberterror attacks. As such, the purpose of this chapter is to examine the legal challenges that this criminal phenomenon has brought to national and international communities, in addition to describing forensic practices related to cyberterrorism. This chapter concludes with a discussion of criminological and theoretical aspects currently applied to the study of cyberterrorism
- These complex notions of what cyberterrorism is have complicated how law enforcement agencies and government organizations in various countries conceptualize and defend against potential cyberterror attacks. As such, the

[3] Chernukhin Ernest, *Department on New Challenges and Threats*, Expert Group on Cybercrime, (17-21 Jan. 2011).

[4] Jeffrey Thomas Biller, *Cyber-Terrorism: Finding a Common Starting Point*, 280-81, 4, Case W. Res. J.L. TECH. and INTERNET, (2013).

purpose of this chapter is to examine the legal challenges that this criminal phenomenon has brought to national and international communities, in addition to describing forensic practices related to cyberterrorism. This chapter concludes with a discussion of criminological and theoretical aspects currently applied to the study of cyberterrorism

The understanding of cybercrime or particularly cyberterrorism has complicated how law and order are maintained by any government. In such a scenario, forensic analysis can expose the '*smoking gun'* which makes or breaks a case and aids investigation by providing links or nexus to establish facts of a corroborative nature.[5] The mix of technical and investigative methodologies rightly aid discovery of hidden clues which often cannot be uncovered by means of basic forensics, prosecutors or even police officials.

The research framework primarily focuses on the following questions:

- What is the scope and significance of cyber forensics in combating cybercrimes?
- What is the international standing of cyber forensics, its framework and developments;
- Whether the Indian framework of cybercrimes and cyberterrorism includes the extensive usage of cyber forensics?
- Whether cyber forensics should be included largely in the legal framework of combating cyberterrorism across borders?

The paper also seeks to identify viable solutions with respect to the lacunae of cyber forensics as a means to prevent and mitigate cybercrimes.

- **Methodology of Study**

The research comprises descriptive, explorative and analytical content and used both primary and secondary sources of information. The author has triangulated various methods of research whereby both doctrinal and non-doctrinal studies were conducted. As primary sources, using the qualitative method of data collection, representatives of the United Nations, diplomats, lawyers, academicians and other stakeholders were consulted for preliminary research based on which the author's understanding of the topic increased and the author was able to identify different target areas of the topic. As secondary sources, using doctrinal research methodology, official reports, past studies, books, journals, case studies, news, articles, and other documents were analyzed. Most inputs in the research have been derived from secondary sources.

The empirical study employed both formal and informal data collection methods, and collected qualitative data from 95 respondents[6]. The demography consisted of diplomats, humanitarian and gender rights workers, advocates, academicians and officials who have worked in the concerned areas related to cybercrimes and forensic science or have knowledge of the same. Law students and other stakeholders were also interviewed to understand the topic from different angles and perspectives.

---

[5] Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 IJCC, (2015).

[6]Ref. Chapter 9, Annexure-Survey Results.

- **What is Digital/Cyber Forensics?**

Digital Forensics (DF) or cyber forensics has grown from a textbook concept to an essential part of several investigations. Cyber forensics tools are used on a day to day basis by experts, technicians and analysts within local, state and Federal functions and also by the private industry providing e-security solutions. DF or cyber forensics can be defined as "the collection and analysis of data from networks, communication streams, computer systems, and media that is admissible in the Court as per the laws". It is the gift that computer science and the law have given to the world after its amalgamation resulting in the birth of cyber forensics. It includes the analysis of digital evidence and has various components within, viz. network forensics, computer forensics, malware forensics, mobile-device forensics etc.[7]

Cyber forensics investigations have several applications and the use of forensic techniques in the realm of cyberspace is increasingly becoming an essential component of digital investigations. After the discovery of DNA technology, it is only cyber forensics as a part of forensic science that has created a huge impact on investigations and prosecutions.[8]
To combat/ tackle issues like cyber terrorism, spams, cyber stalking, etc., cyber forensic tools help in inspecting such criminal cases and also for finding admissible evidences. Some of the tools include: X-Ways WinHex, First on Scene, Rifiuti, Forensic Acquisition Utilities (FAU), NMap, BinText, PyFlag Tools, Encrypted disk detector etc.[9]

- **Cybercrimes and Cyber terrorism**

Cybercrime and computer-supported criminal acts have been increasing with the increasing potential of technology. Since many criminals and terrorists are now educated, with increased access to education, it becomes easier for them to use such means to perpetrate crime and they often have more access to advanced technological tools, than the existing government defense establishments, through illegal means or sources. Electronic evidence and gathering of information have become key problems in conflict regions and in regions of high vulnerability or sensitivity. Cybercrime constitutes more or less the same as the commission of a traditional crime with the use of different means i.e. computer/technology and is often at a transnational level[10].

---

[7]Diana S. Dolliver & Kathryn Seigfried-Spellar, *Legal,Forensic, and Criminological Aspects of Cyberterrorism*, 11-12, (2014).

[8]Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*,9, IJCC, 73, 55-119, (Jan.–June 2015).

[9]K.L. Thomas, *Cyber Forensics- An Introduction*, CDAC, https://www.cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2010-0164.pdf

[10]ITU (2012). *ITU-D development - Committed to connecting the world*. [online] Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

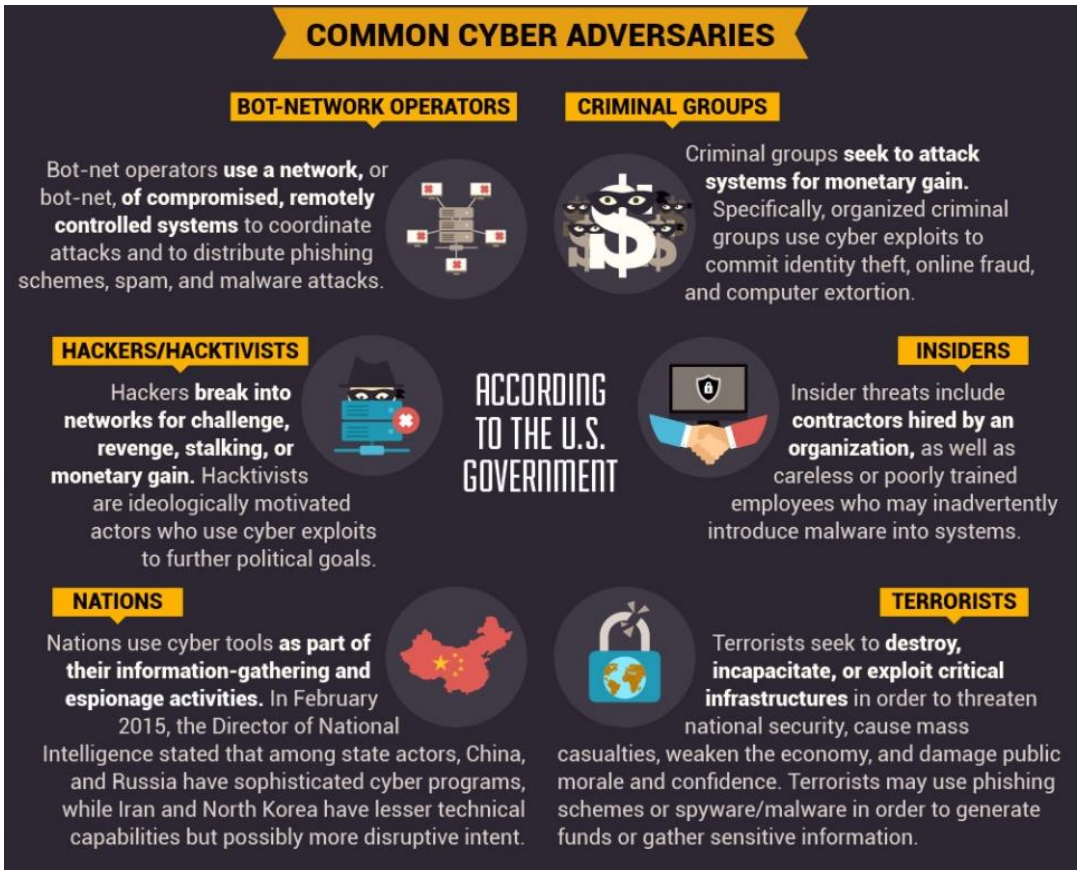


Fig.: The Rise of Cyber Threats[11]

Cyberthreats can be loosely defined as usage of cyberspace or technology to do activities that can weaken a society's internal or external order.[12] Over the past 50 years multiple solutions have been identified to tackle cybercrimes however, the issue still continues to be challenging due to dynamic or ever-changing technological developments and the varying methods in which the offences are perpetrated.[13]

Cyber terrorism is a well-planned and systematized use of technology by cyber experts operating from any location, for anti-national activities[14] Cyber terrorism, unlike cybercrimes, has larger consequences and the motive is usually more socio-political than personal. Cybercrimes may involve personal level vendetta but when it comes to cyber terrorism, it is usually with a larger motive and for a larger cause. The technology used by such terrorists is usually illegal or stolen which is why countries often aren't well-

[11]Norwich University Online. (2020). *The Rise of Cyber Threats*. [online] Available at: https://online.norwich.edu/academic-programs/resources/rise-cyber-threats [Accessed 21 Dec. 2020].

[12] Susan W. Brenner, *Cybercrime, cyberterrorism and cyberwarfare*, Revue internationale de droit penal, 77 CAIRN INFO, (2006).

[13]*Supra* note 9, 12.

[14] Dr. Shrish Kumar Tiwari, *Cyber Crimes- A Threat to Humanity*, Humanities & Social Sciences Reviews, 2 (1) GIAP, (Dec. 2014).

equipped to deal with the situation since they rely mainly on traditional forensic science and basic law and order machinery.

Although there is no universally accepted definition of cyber terrorism, upon examining various definitions, one would find that there are certain common elements of this cybercrime, including, data theft, hacking, attacks on information systems and on computer networks, cyber and planning of terrorist attacks. All these attacks would not qualify as cyber terrorism unless there is an intention to coerce or intimidate a government or its subjects to further a larger socio-political scheme or agenda.[15] Cyber terrorism networks are present in various corners that are only accessible via internet tools and such networks are accessed or run by organized groups since terrorism is highly organized and systemic.[16]

- **Growing need for Cyber Forensics**

Cyber forensics provides detailed information for understanding both the technical and legal aspects of crimes committed in cyberspace. Cyber forensics has proved to be helpful in tracing spam emails, child pornography and various other anti-social activities on the dark web or other platforms.[17]

Mere traditional forensics or outdated mechanisms to fight terrorism are often ineffective and cyber forensics are equipped to deal with some level of cyber terrorism based on the know-how or research and development the country has invested in. Not only do such forensics aid in stopping the act from further getting penetrated but also helps in forming evidence for the justice officers to hold the perpetrator liable, without an aorta of doubt. For example, when there is a situation where one hacker has access to someone else's computer system without their authorization it may cause problems at different levels. The computer forensics alerts the owner and in case the system is broken into, their traces are captured through various applications and software that have been developed to track virtual movements.[18]

Cyber forensics can help in ensuring the reliability of the computer systems. It is extremely resourceful in tracking down cyber terrorism and up to a certain level can also prevent attackers/terrorists from committing cybercrimes. Increasing incidents of cybercrimes such as ransom ware, phishing, spamming etc. have cost India $4 billion during 2012-2013, (as per a Symantec report).[19] From 2019 to 2023, it has been estimated that approximately 5.2 trillion dollars in global value will be at a risk due to cyberattacks

---

[15] Vida M. Vilic, *Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyber Space*, 10 BALKAN SOC. SCI. REV., 7 (2017).

[16] Laura Mayer Lux,*Defining Cyberterrorism,* 7 REV. CHIL. DERECHO TECNOL., (2018).

[17] Dr. Anjani Singh Tomar, Tools used in cyber forensics, Cyber Forensics in Combating Cybercrimes, 3 PARIPLEX-INDIAN J. OF RES., (Sept. 2014).

[18]Norwich University Online. (2015). *Role of Computer Forensics in Crime*. [online] Available at: https://online.norwich.edu/academic-programs/resources/role-of-computer-forensics-in-crime [Accessed 21 Dec. 2020].

[19]*Supra* note1.

and it is not only going to affect investors and financial institutions, but also other essential sectors like health, national security etc.[20] This just goes on to show how although there is technology that exists to counter cybercrimes, since cyber forensics are not actively pursued by various nations for the same objective, the existing framework/machinery being used by governments in various countries, is lagging behind and needs the intervention of cyber forensics.

- **International Framework and Standing on Cyber Forensics**

All efforts to address the issue of terrorism across borders are futile without international cooperation and understanding. The need for an international treaty or agreement on cybercrime and terrorism, and the lack thereof, is alarming. The presence of such an instrument is essential to bring terrorists to justice and in furtherance of the same, governments need collaborate and cooperate with each other in facilitating investigations and necessary data sharing.[21] The United Nations Office on Drugs and Crime had collaborated with the Counter-Terrorism Task Force to develop a technical assistance tool on the Use of Internet for Terrorist Purposes however, it does not include the scope of cyber forensics or forensic science in general and it has multiple shortcomings in terms of cyber security solutions.[22]

Universities across the globe are trying to come up with effective frameworks to assimilate cyber forensics into existing cybercrime legislations. Countries like Russia, Japan, Australia, Ireland, Canada, USA, Cameroon, Namibia, Kenya, Bangladesh, Jordan, UAE, Jamaica, Portugal and Norway have either passed laws relating to cyberspace or revised the existing domestic legislations to suit the growing needs. Regional organizations the Council of Europe, ITU, ASEAN, NATO, OECD etc. have tried to formulate uniform policies dealing with cyberspace[23] however, those do not simultaneously regulate cyber forensics to bring law enforcement in tandem with the actual law against cybercrimes. Although there are several international frameworks dealing extensively with counter terrorism measures, barely any of them mention the need for cyber forensic inclusivity. Bahrain's structure can be taken as a good example of a country that has used cyber forensics extensively[24] whereby, they have established cybersecurity frameworks and strategies to ensure technological advancements are regulated and streamlined with

---

[20]Iman Ghosh (2019). *This is the true cost of cybercrime, according to experts*. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/ [Accessed 21 Dec. 2020].

[21]UNODC ANNUAL REPORT Covering activities during 2015. (n.d.). [online] Available at: https://www.unodc.org/documents/AnnualReport2015/Annual_Report_2016_WEB.pdf [Accessed 21 Dec. 2020].

[22]*Supra* note 14.

[23]IDSA Taskforce Report, IDSA (2012),*India's Cyber Security Challenge*, [online] Available at: https://idsa.in/system/files/book/book_indiacybersecurity.pdf [Accessed 21 Dec. 2020].

[24]Adel Al-Alawi, *Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status*, RESEARCH JOURNAL OF BUSINESS MANAGEMENT, (2014).

national policies, similar to that of Netherlands, having a strong National Cyber Security Agenda (NCSA)[25].

Although the European Convention on Cybercrimes and Geneva Convention can be taken as foundational or guiding forces, one cannot ignore the fact that a framework dealing with cyber forensics as part of cyber security is long overdue, considering the growing transborder exchange of information and borderless cyberspace. The Convention on Cybercrimes (Budapest Convention) is very outdated and does not cover cyber forensics, making it difficult to assess the proof and extent of liability.[26] Provisions relating to the treatment and admissibility of cyber forensic evidence, in both common law and civil-law countries lack uniformity and, in many cases, do not even exist.[27]

The United Nations General Assembly's approval for commencement of the process for a draft treaty to combat cybercrime is a ray of hope for all the stakeholders fighting against the perils of technology. The approved resolution called for the establishment of an inter-governmental committee of experts and the suggestions given by member nations would decide the fate of cyber forensics in combating cybercrimes.[28]

- **Situation of Cyber Forensics in India**

India may have several forensic labs and technicians but not many are aware of the trajectories of forensic science as a discipline. In the *Tandoor murder* case[29], *Talwar* case[30], *Nirbhaya* case[31] etc. forensic science has majorly helped in solving cases, since it consists of forward-looking contemporary medical and technological tools[32].
Way back in 1975 India became aware of the advent of technology in our lives and various legislations were enacted or amended to meet the needs of the dynamic technological environment. A special unit i.e. the Indian Computer Emergency Response Team (CERT) was established in 2004 and the Information Technology (Amendment) Act, 2008 was also enacted to accommodate the needs of the highly technologically dependent society. A National Cyber Security Policy was formulated in, as late as, 2013. The States of

[25]Hathaway, M. and Spidalieri, F. (2017). *THE NETHERLANDS CYBER READINESS AT A GLANCE*. [online] Available at: https://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf [Accessed 21 Dec. 2020].

[26]*Supra* note 9, 219.

[27]*Supra* note 13.

[28]United Nations : Office on Drugs and Crime. (2019). *Cybercrime Ad Hoc Committee*. [online] Available at: https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html [Accessed 21 Dec. 2020].

[29]Sushil Sharma v State of Delhi (2014) 4 S.C.C. 317 (India).

[30]Dr. Rajesh Talwar & Anr v CBI (2013) 82 A.C.C. 303 (India).

[31]Mukesh v State (NCT of Delhi) (2017) 6 S.C.C. 1 (India).

[32]Gowsia Farooq Khan, *Role of Forensic Science in Criminal Investigation: Admissibility in Indian Legal System and Future Perspective,* 7 IJARSE, 1135, 1124-1138, (Mar. 2018).

Karnataka and Telangana were the first ones in India to realize the need for State driven initiatives in the digital sector.[33]

A crime qualifies as a cybercrime only if it falls under Section 66 of the Information Technology Act, 2008 (IT Act).[34] Specific intention has to be established using provisions of the Indian Penal Code before invoking Section 43 of the IT Act. There are very few provisions enabling the interpretation of certain crimes as cybercrimes, making it even more difficult to extensively apply cyber forensic tools.

The Indian Evidence Act, 1872 was amended to include provisions dealing with the admissibility and recognition of electronic evidence by the courts. The Act was amended to make way for technological advancements however, it only includes the provisions guiding the treatment or usage of electronic records, documents and proof, however, cyber forensics is not merely about the existence of electronic or computer records and transactions. Cyber forensics is not restricted to computer applications. It has multiple tools and a huge scope yet to be discovered (as discussed in the previous sections) which are not covered under any of the Indian laws.[35] There are no enabling provisions or regulatory provisions to cover the larger scheme of cyber forensics.
Similarly, Part A and G of the National Cyber Security Policy of India (2013), mention the need for a forensically developed infrastructure however, it does not mention the scope, usage and regulation of cyber forensics to combat cybercrimes[36].

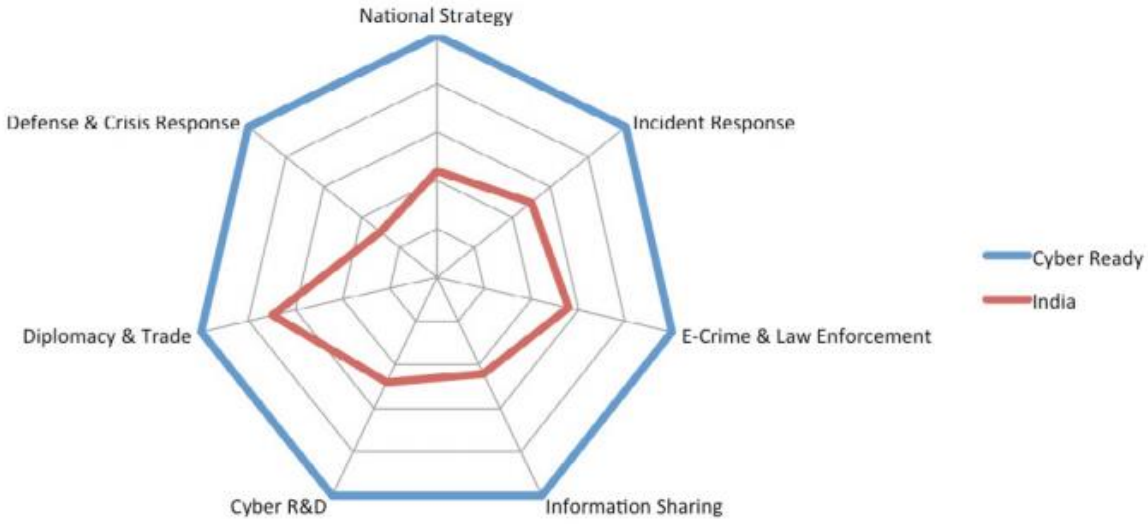


Fig.: India's Cyber Readiness Assessment (CRI)[37]

[33]*Supra* note 15.

[34]The Information Technology (amendment) Act of 2008, No. 10, Act of Parliament ,2009 (India).

[35]Cyberforensics.in. (2020). *Cyber Forensics- Access Denied*. [online] Available at: http://www.cyberforensics.in/AccessDenied.aspx?ReturnUrl=%2flaw%2fsecondschedule.aspx%3fAspxAutoDetectCookieSupport%3d1&AspxAutoDetectCookieSupport=1 [Accessed 21 Dec. 2020].

[36]*National Cyber Security Policy of 2013*, National Strategies Repository, ITU, [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/India_2013_National_cyber_security_policy-2013(1).pdf [Accessed 21 Dec. 2020]

In spite of the efforts of the government to set up various forensic centers and strengthen the cyber forensics infrastructure, the cybercrime countering framework remains inadequate, requiring further discovery and development.

- **Recommendations and the Way Forward-**

It is a fact known to all that we are constantly at a threat of losing the war against cybercrimes. Cyberterrorism is a concern not only for conflict countries but for all nations existing in the international realm. Cyber forensics, cybercrimes and cyber terrorism are interlinked in such a way that the underdevelopment of one could lead to the ineffectiveness of another and cannot exist in isolation.

The Indian government should robustly pursue the policy dealing with cybercrimes to enable prosecution of cyber criminals and cyber terrorists. Capacity building is essential in the area of cybercrime and cyber forensics in terms of training and coordination between the law enforcement authorities and judiciary[38]. The policy needs to be tweaked to accommodate the application of cyber forensics wherever possible and should be framed in such a manner that does not restrict the growth and development of the field with changing technological infrastructures. The legal implications of cyber forensics need to be discussed by law makers and other relevant stakeholders must be included in the process of law making.
The United States of America holds a higher rank[39] as compared to other super powers in the cyber security index due to their highly aligned and structured policies dealing with cybercrimes and digital cyber security solutions. To increase accountability and cyber security readiness, countries should be encouraged to adhere to the standards of the index. All national policies must be regulated according to the guidelines and standards of the same.

The International Strategy for Cyberspace should be used to provide assistance to the countries that do not have the capacity to enact laws related to cybercrimes. This strategy can also be in the Treaty to combat cybercrimes since it also discusses the need for an international framework for data sharing, privacy implications, etc.,[40] which are essential for any holistic and inclusive multilateral agreement. Without an international treaty, no country would be obligated to follow guidelines and principles regulating the cyberspace and hence, member states should seriously expedite the process and discussions around the

---

[37]Hathaway, M., Demchak, C., Kerben, J., Mcardle, J. and Spidalieri, F. (2016). *CYBER READINESS AT A GLANCE*. [online] Available at: https://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf [Accessed 21 Dec. 2020].

[38]*Supra* note 35.

[39]Global Cybersecurity Index (GCI) 2018 ITU Publications Studies & research. (n.d.). [online] Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [Accessed 21 Dec. 2020].

[40]International Strategy for Cyberspace, The Comprehensive National Cybersecurity Initiative, UNODC, (2011), [online] Available at: https://sherloc.unodc.org/res/cld/lessons-learned/usa/international_strategy_for_cyberspace_html/international_strategy_for_cyberspace.pdf [Accessed 21 Dec. 2020].

treaty on cybercrimes. Regional cooperation and understanding are essential since cybercrimes do not take place within borders. National, regional and international laws must include enabling provisions for the usage of cyber forensics in all aspects of law since they are all interrelated and interconnected.

There is a pressing need for investments in the research and development infrastructure of cyber forensics to effectively deal with cybercrimes at its roots. Such initiatives can also help in dealing with the lacunae and shortcomings of cyber forensics, to fix faults in algorithms. The World Bank Cybercrimes Combating toolkit can be used by governments to ensure various means and sources of conducting crimes are eliminated for terrorists and attackers, with regular monitoring[41].

Women and children should be specifically addressed in the legislations related to cybercrimes since they are the most at risk of falling prey to cybercrimes due to lack of education, awareness and proper means of safe internet access[42].

- **Conclusion**

We have come a long way in terms of development in the field of forensic science. We have gone from traditional methods of investigation to DNA testing and cyber forensics. This isn't the end since there is an ocean of potential and opportunities to discover the multi-dimensional uses of cyber forensics in fighting the dark side of cyberspace. Unless we invest in research and development of digital sciences and properly train the members of the justice system to utilize such technology and promote the usage of the same, there is no scope for the effective application of cyber forensics in combating cybercrimes.
With India's election to the Security Council as a non-permanent member, it is essential for India to realize the potential of cyber forensics in combating cybercrimes with increasing attacks on national security electronically. By largely including cyber forensics in their national cybersecurity infrastructure, India can become a game changer in the discussions on the international cybercrime treaty since so far, most international bodies have not explored the potential of forensics in cyber law. With the use of technology in every aspect of crime, lacunae of international and national laws in evidence collection can be addressed. Looking at the impact cybercrimes have on socio-economic and political infrastructure, there is a need to reassess the investments on physical security and shift the focus on investing in technological security infrastructure. The sky is the limit when it comes to cyber forensics and it is the only effective means of achieving global peace and security to a large extent.

---

[41]ITU,*Combatting Cybercrime Tools and Capacity Building for Emerging Economies*, (2017), [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf [Accessed 21 Dec. 2020].

[42]Rajesh Moudgil (2020). *Cyber crimes against women, kids a major threat: Experts*. [online] Hindustan Times. Available at: https://www.hindustantimes.com/chandigarh/cyber-crimes-against-women-kids-a-major-threat-experts/story-YsBR0bVGED6W66burEk7yH.html [Accessed 21 Dec. 2020].

- **References**

Case laws-

1. Sushil Sharma v. State of Delhi (2014) 4 S.C.C. 317 (India).
2. Dr. Rajesh Talwar & Anr v. CBI (2013) 82 A.C.C. 303 (India).
3. Mukesh v. State (NCT of Delhi) (2017) 6 S.C.C. 1 (India).
4. Acts-
5. The Information Technology (Amendment) Act of 2008 (India).
6. Indian Evidence Act of 1872 (India).

Reports and policies-

1. International Strategy for Cyberspace, The Comprehensive National Cybersecurity Initiative, (2011), https://sherloc.unodc.org/res/cld/lessons-learned/usa/international_strategy_for_cyberspace_html/international_strategy_for_cyberspace.pdf.
2. Global Cybersecurity Index (GCI) 2018, ITU PUBLICATIONS, 62, (2019), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
3. Annual Report of the United Nations Office on Drugs and Crime, UNODC, (2015), https://www.unodc.org/documents/AnnualReport2015/Annual_Report_2016_WEB.pdf
4. National Cyber Security Policy of 2013, National Strategies Repository, ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/India_2013_National_cyber_security_policy-2013(1).pdf
5. Combatting Cybercrime Tools and Capacity Building for Emerging Economies, ITU, (2017), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf
6. Convention on Cybercrime, ETS No. 185, Council of Europe, (2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Articles, research papers and other documents-

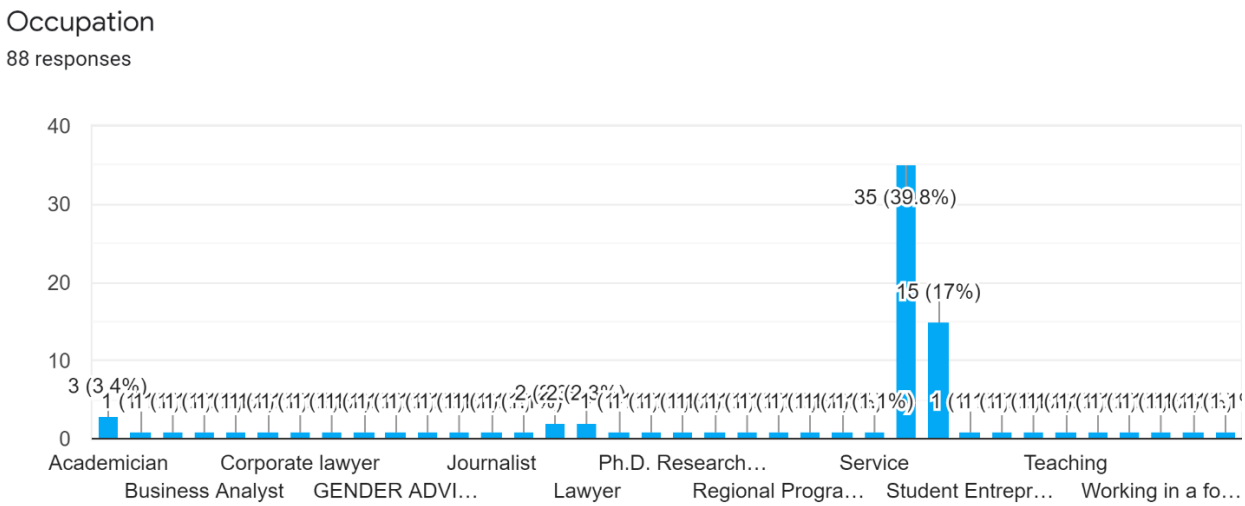
1. Cybersecurity Framework in Bahrain, e-Government Bahrain, (Oct. 1, 2019), https://www.bahrain.bh/wps/portal/!ut/p/a1/lZJdT8IwFIb_ilzscvSw7qPzbhJECR8GRFlvyDa6MjPa0RWQf2-BxGgiAr1r87ztc84pomiGqEi2BU90IUVSHvbUnz-NwG85xOkRPMUQjfz2OOxAqwueAeKfAGDcOQDBS_AWOj6B6_LgDNqtZ9fkBwOAiDyM-6-PbYAuvpR_RxTRTOhKL1HMuNxWUumknDNhQZmIRSH4XZVwVluQ7VOmapZtVKH3h1iVFQsUe57DHDfz7cDF2HZdQmwS4tCG3E09EuZ-wr41z6zoYpkTJk6qF5p1BP7rxgk47xEb0eCsiblhcmPlvSsmWHys1zQyc5BCs0-NZrcMwjzAS5keP1sciRQTjqhiOVNMNTfKHC-1rup7CyzY7XZNLiUvWTOTKwv-iixlbQx-k6haTacrgvd2r5MPhzZNvXLbjxqNL4D4HgU!/dl5/d5/L2dBISEvZ0FBIS9nQSEh/
2. Laws and Rules, Cyber Forensics-India, RCCF, http://www.cyberforensics.in/law/secondschedule.aspx
3. Ad hoc committee established by General Assembly Resolution 74/247, UNODC, (2020), https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

4. Gowsia Farooq Khan, Role of Forensic Science in Criminal Investigation: Admissibility in Indian Legal System and Future Perspective, 7 IJARSE, 1135, 1124-1138, (Mar. 2018), http://www.ijarse.com/images/fullpdf/1524846716_JK1433IJARSE.pdf
5. India's Cyber Security Challenge, IDSA Taskforce, (March 2012), https://idsa.in/system/files/book/book_indiacybersecurity.pdf
6. Adel Al-Alawi , Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status, Research Journal of Business Management, (2014), https://scialert.net/abstract/?doi=rjbm.2014.139.156.
7. The Netherlands Cyber Readiness at a Glance, CRI, POTOMAC INSTITUTE FOR POLICY STUDIES, (2017),
8. https://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf
9. Cameron S. D. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice,9, IJCC, 73, 55-119, (Jan.–June 2015), http://cybercrimejournal.com/Brown2015vol9issue1.pdf
10. Dr. Anjani Singh Tomar, Tools used in cyber forensics, Cyber Forensics in Combating Cybercrimes, 3 PARIPLEX-INDIAN J. OF RES., (Sept. 2014), https://www.worldwidejournals.com/paripex/article/cyber-forensics-in-combating-cyber-crimes/MjY0Ng==/?is=1
11. Susan W. Brenner, Cybercrime, cyberterrorism and cyberwarfare, Revue internationale de droit penal, 77 CAIRN INFO, (2006), https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm#.
12. Dr. Shrish Kumar Tiwari, Cyber Crimes- A Threat to Humanity, Humanities & Social Sciences Reviews, 2 (1) GIAP, (Dec. 2014), https://giapjournals.com/hssr/article/view/hssr214
13. Vida M. Vilic, Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyber Space, 10 BALKAN SOC. SCI. REV., 7 (2017), https://heinonline.org/HOL/P?h=hein.journals/bssr10&i=8
14. Laura Mayer Lux, Defining Cyberterrorism, 7 REV. CHIL. DERECHO TECNOL., (2018), http://dx.doi.org/10.5354/0719-2584.2018.51028
15. The Role of Computer Forensics in Crime, Cybersecurity, NORWICH UNIVERSITY ONLINE, (Dec. 7, 2015), https://online.norwich.edu/academic-programs/resources/role-of-computer-forensics-in-crime
16. Iman Ghosh, This is the Crippling Cost of Cybercrime on Corporations, WORLD ECONOMIC FORUM, (Nov 7, 2019), https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/
17. Diana S. Dolliver & Kathryn Seigfried-Spellar, Legal, Forensic, and Criminological Aspects of Cyberterrorism, 11-12, (2014), https://www.researchgate.net/publication/314350231_Legal_Forensic_and_Criminological_Aspects_of_Cyberterrorism.
18. K.L. Thomas, Cyber Forensics- An Introduction, CDAC, https://www.cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2010-0164.pdf
19. Understanding Cybercrime: Phenomena, challenges and legal responses, Telecommunications Development Sector, ITU, (Sept. 2012), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
20. The Rise of Cyber Threats, NORWICH UNIVERSITY ONLINE, (Sept. 30, 2020), https://online.norwich.edu/academic-programs/resources/rise-cyber-threats

21. Dr. Anjani Singh Tomar, Tools used in Cyber Forensics, Cyber Forensics in Combating Cybercrimes, 3- PIJR, (Sept. 2014),
22. https://www.worldwidejournals.com/paripex/article/cyber-forensics-in-combating-cyber-crimes/MjY0Ng==/?is=1.
23. Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 IJCC, (2015), http://cybercrimejournal.com/Brown2015vol9issue1.pdf
24. Cyber-defense Strategies for Contending with Non-state Actors: A Review and Assessment of Existing Proposals, YALE REV. INT'L STUD., (Dec. 2017), http://yris.yira.org/comments/2214.
25. Chernukhin Ernest, Department on New Challenges and Threats, Expert Group on Cybercrime, (17-21 Jan. 2011), https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Russia_1_Cybercrime_EGMJan2011.pdf.
26. Jeffrey Thomas Biller, Cyber-Terrorism: Finding a Common Starting Point, 280-81, 4, Case W. Res. J.L. TECH. and INTERNET, (2013). https://heinonline.org/HOL/P?h=hein.journals/caswestres4&i=288.

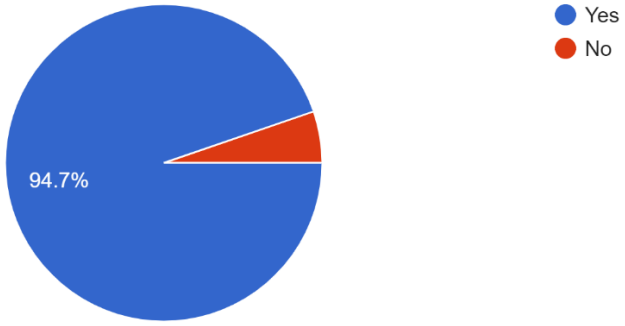
- **Annexure-Survey Results**

Apart from the below given results, the author also asked responders to provide their understanding of the issue and suggestions to tackle the same through open ended questions which could not be included due to the length of the responses.



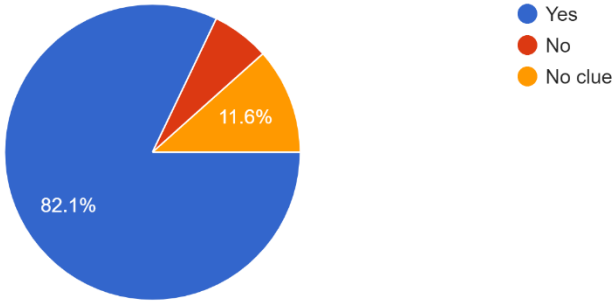
Are you aware of the impact of cyber-crimes on national security?

95 responses



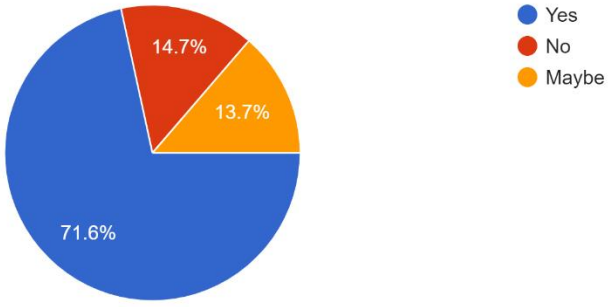
Do you think forensic science has a major role to play in combating cyber crime?

95 responses



Are you aware of the existence of cyber-forensics?

95 responses



Do you think legislators/policy makers have looked at various trajectories of cyber forensics?

93 responses

Do you think governments are well-equipped (legally) to deal with intervention of cyber forensics in counter-terrorism measures?

94 responses