
PAVAN DUGGAL ASSOCIATES
A PAVAN DUGGAL ASSOCIATES INITIATIVE
INTERNATIONAL E-JOURNAL ON CYBERLAW, CYBERCRIME & CYBERSECURITY
WWW.PAVANDUGGALASSOCIATES.COM

EMERGING GLOBAL CYBERLAW TRENDS IN 2021

- **Introduction**

The year 2021 has emerged from the shadows of the year 2020 and it is expected to be an important year in the growth of Cyberlaw jurisprudence at a global level.

This year is likely to see a focus on various thrust areas that are likely to contribute to evolving Cyberlaw jurisprudence.

- **Legal Regulation of Cyber Security**

One of the key Cyberlaw trends globally in the year 2021 will be an increasing focus on legal regulation of cybersecurity. The year 2020 has seen massive cybersecurity breaches. Cybersecurity breachers have started focusing on attacking the Critical Information Infrastructure, apart from the healthcare sector.

Consequently, countries have begun to start legislating on cybersecurity laws to regulate cybersecurity at national levels. The year 2021 is going to see a consolidation of the trends, where countries are going to see an increasing trend towards the enactment of national legislations targeting cybersecurity.

For those countries who already have dedicated cybersecurity laws, they are also likely to work on enhancing the ambit of such laws, apart from coming up with secondary legislations in the form of rules and regulations to support such legislations.

Some countries may continue to go for a softer approach of coming up with national cybersecurity policies and strategies, as compared to dedicated legislations in this regard.

For Countries which have still not made up their minds of coming up with dedicated laws on cybersecurity, the route of national cybersecurity policies and strategies looks more comfortable achievable targets and low hanging fruits.

- **Legally Protecting Critical Information Infrastructure and Healthcare Infrastructure**

The year 2021 is also likely to see a specific focus on coming up with legal frameworks on protection of Critical Information Infrastructure and healthcare infrastructure, given the tremendous attacks that have been targeted during Covid-19 times at the Critical Information Infrastructure and health related infrastructure in different countries. In 2021, the time has come up for countries to start having dedicated Critical Information Infrastructure protection legal frameworks. The year 2021 is likely to see more developments in this regard.

- **Golden Age of Cybercrime and Increasing Cybercrimes**

The year 2021 will see the extension of the growth of cybercrimes. The Golden Age of cybercrimes, which has begun with Covid-19, is going to last for some time. This golden age has demonstrated the inefficacy of existing cybercrime laws to deal with the emerging challenges of cybercrimes. Hence, the year 2021 would see a focus on cybercrime

regulation as an important thrust area of growing policies. Countries could potentially be looking up in the direction of having dedicated cybercrime laws.

- **Covid-19 Legal Issues**

The year 2021 is a year where countries are likely to start addressing the distinctive issues thrown up by Covid-19 and the Work From Home paradigm. Covid-19 has propelled increased digitization and has completely changed the Work From Home paradigm. The practical teething problems, that the Work From Home has thrown during Covid-19, is likely to engage the attention of governmental stakeholders as they come up with more enabling legal frameworks to promote the growth and consolidation of Work From Home during Covid-19 and beyond.

- **Increasing Regulation of Artificial Intelligence**

The year 2021 is also likely to see an enhanced trend of legal regulation of Artificial Intelligence. The year is going to build on the efforts made in the year 2020 towards regulating Artificial Intelligence. This year is likely to see the Ad hoc Committee on Artificial Intelligence of the Council of Europe (CAHAI) to consolidate their work on coming up with an international regulatory framework on Artificial Intelligence.

Further, countries are increasingly likely to keep the US as an example in mind and come up with more enabling legal frameworks for regulating Artificial Intelligence in their respective national territorial boundaries.

We are likely to see more developments concerning and acceptance of principles, pertaining to enabling regulation of Artificial Intelligence in the year 2021.

The year 2021 is also likely to see other nations starting coming up with distinctive legislations, even though narrow in nature, which are likely to be focused on different aspects pertaining to regulation of Artificial Intelligence.

- **Regulating IOT Cyber Security**

The year 2021 is further likely to build on the experiences of the world in the year 2020 in terms of regulating cybersecurity in the context of the Internet of Things (IoT). The passing and implementation of the US IoT Cybersecurity Improvement Act, 2020 could potentially act as a catalyst for other countries to come up with similar legislations, to regulate the use of the Internet of Things (IoT) and cybersecurity atnational levels.

- **International Policy Vacuum to Continue**

At the international level, the fragmented policy vacuum pertaining to cyber legal issues is likely to continue to keep on subsisting.

At a time when different countries have already been busy in fighting Covid-19, the chances of these countries to agree to common minimum norms of behavior in cyberspace are not likely to be more bright.

Under normal times during the pre-Covid-19 era, it had taken years and still, no concrete agreement had come forward amongst countries on agreeing to norms of behavior in cyberspace.

Covid-19 provides justifiable opportunities that countries to defer considering the issue of coming to an agreement on international cyber legal norms, including norms concerning the behavior of cyber actors in cyberspace.

- **Legal Frameworks To Promote Use Of Blockchains**

The year 2021 is further likely to see a more enhanced focus on blockchain. As blockchains have entered into a new level of maturity and are increasingly being used in different electronic governance initiatives, the year 2021 could see more countries coming up with enabling legal frameworks for promoting the use of blockchains in electronic governance and other applications in the digital ecosystem.

- **Emergence of New Cyber World Order**

The year 2021 is further likely to see the emergence of different aspects of the New Cyber World Order. In my book "New Cyber World Order Post COVID-19", I have argued how distinct changes are taking place in cyberspace in Covid-19 times, which are likely to result in the New Cyber World Order, by the time the world concludes its fight against Covid-19.

The year 2021 is further likely to see more focus on more enhanced elements of New Cyber World Order emerging. The year 2021 is also likely to see states getting more powerful concerning cyber matters. The same in some cases could have a prejudicial impact upon the enjoyment of digital rights and liberties of netizens.

The year 2021 could also see a migration of users from the superficial net to the darknet.

- **Vaccine Cyber Nationalism**

The year 2021 is also likely to see struggle amongst different nations, in trying to receive the maximum volumes of doses of Covid-19 vaccines. Vaccine cyber nationalism is also likely to increase. Vaccine cyber nationalism refers to a phenomenon where countries will increasingly start using cyberspace and its various facilities for having access to various vaccines, and their related R&D information for the benefit of their populations.

As such, the year 2021 is also likely to see more attacks on the supply chain of vaccines. We are likely to see more cyber attacks on vaccine related data and supply of vaccines, by cybercriminals and state and non-state actors, which will be aimed to disrupt the process of vaccine distribution and dissemination. Hence, the year 2021 is likely to see more countries coming up with enabling legal frameworks to protect the supply chain of vaccine distribution.

Further, with new vaccines continuing to develop across the world, we are likely to see more focus on hacking and unauthorizedly accessing the data pertaining to such vaccines for unauthorized sale or dissemination on the darknet.

- **Consolidation of Cyber Sovereignty**

The year 2021 is further likely to see the consolidation of the trends on cyber sovereignty. More and more countries are increasingly going to put forward expansive definitions of the concept of cyber sovereignty, to enhance the protection of cyber sovereign interests. It is also possible that some countries may want to come up with specific legal frameworks, to enhance the ambit and applicability of cyber sovereign interests.

- **Growing Data Localization Trends**

The year is also likely to see massive data localization trends emerging. These trends could also contribute in the direction of further balkanization of the internet. These trends are built on the fundamental premise that data is the new oil of data economy and that countries need to extensively rely upon data as an element of enhancing the scope and ambit of data sovereignty. More and more countries are likely to discover the benefits of data localization as an effective tool of consolidation of their sovereign interests and are likely to explore options to ensure that data of their citizens does not leave the physical territorial boundaries of those countries.

Russia is further likely to see the consolidation of the implementation of RuNET law which is a legal framework to support building a separate Russian internet to be up and about, in the event Russian internet to the Western World is disconnected.

- **Increasing Interception, Monitoring and Impact on Privacy**

The year 2021 is going to see more and more countries consolidating powers and increasingly relying upon interception and monitoring of data as part of their sovereign functions. This effectively means that this year is likely to see instances where some countries could come up with procedures and processes that are likely to curtain the enjoyment of personal freedoms and digital privacy. Hence, digital privacy is likely to be evaporating more in the year 2021.

- **Data Protection Legal Frameworks Under Focus**

Further, the year 2021 is also likely to see more focus on data protection. The General Data Protection Regulations (GDPR) of the European Union is further going to consolidate its position. The GDPR is further likely to encourage member countries to come up with dedicated national laws on data protection.

- **Legal Challenges of Emerging Technologies**

Further, the year 2021 is also likely to see new challenges thrown up by emerging technologies like Quantum Computing which will increasingly bring forward the need for effectively addressing the legal, policy and regulatory issues pertaining to such emerging technologies.

- **Internet Governance Issues Likely To Be Inconclusive**

The internet governance debates at global levels are likely to remain non-conclusive as countries are increasingly using the Internet for covert and overt activities.

- **Increasing Cyber Resilience**

In the year 2021, stakeholders will increasingly have to start adopting a new mindset of cyber resilience, as they struggle to meet the challenges of growing cybercrimes and cybersecurity breaches.

- **Enhancing Cyber Capacity Building**

The year 2021 has once again broughtforward the focus on capacity building. We need to change our mindset concerning cyberspace. There is no denying the fact that cyberspace is now an integral part of our life. Our approaches to cyber resilience and cyber hygiene will have to now substantially change. The year 2021 could start seeing movement in this direction as the year progresses.

The aforesaid are some of the important Cyberlaw trends that one sees on the horizon in the year 2021. Needless to say, one is not a soothsayer and one cannot predict as to what will happen. However, there is no denying the fact that the trends mentioned above should be featuring significantly in the cyberspace landscape in the year 2021.

All said and done, Covid-19 and related developments will have a direct significant impact upon cyberspace as also on Cyberlaw in the year 2021. It will be interesting to see how Cyberlaw jurisprudence evolves in the year 2021.

ARTIFICIAL INTELLIGENCE IN CYBER SECURITY – THE NEW APPROACH TO CYBER CRIME REGULATION

- **Abstract**

The World is fast moving toward a digital age, where there is a growing dependence on digital technology and use of internet. The recent pandemic situation has further increased this dependence. But as the familiarity to the digital world increases, so does the probability of frequent and more advanced cybercrime. There is hence, a need to upgrade the security measures to be able to face the advanced nature of cyber-attacks. This paper attempts to determine whether introduction of Artificial Intelligence in cybersecurity will create a better safeguard against cybercrime. The author will be using the doctrinal form of research for this paper, using secondary resources such as other papers, articles, case studies and existing legal provisions. The paper focuses on three main areas of research – possible positives and negatives of artificial intelligence in cybersecurity; the existing regulation measures and possible issues in regulation if artificial intelligence is used. The conclusion of the paper is formed from the author's opinion and suggestions.

Keywords*: Artificial Intelligence, Cybersecurity, Cybercrime, Hacking.*

- **Introduction And Background**

The 21st century has already been branded as the 'tech-savvy' century and the age of digital and technological advancement. Everything from banking to applying for a license to even ordering clothes and food can now be done online. Post the recent outbreak of the Coronavirus and the subsequent lockdown, several businesses suffered, and as a result, many of them started online services. This growing technological and digital industry now includes online gyms, online distribution of fresh produce and even online education for schools and colleges. The pandemic has thus increased our dependence on the digital and technological industry.

But with this growing dependence, there has been an increase in sharing and exchanging of data online, which has led to an increase in the incidence of cybercrime. And as the industry advances further, newer and more advanced forms of cybercrime have appeared. Hence, a major concern today is the security of data exchanged and the security of the devices involved in the exchange. Cybersecurity - and adequate cybersecurity, at that – is nowadays a hot topic today.

Another growing topic since the past few years is Artificial Intelligence (AI). Artificial Intelligence is essentially a mechanism or program that enables a hardware to think for itself and make its own decisions. Although AI is a discipline in itself, it has a very wide ambit and can include anything from an application that can figure out and solve a problem by itself to an application that can develop emotional intelligence and function accordingly.[1] It has several subset disciplines too, such as Machine Learning and Deep Learning.

[1]IBM Cloud Education (2020). *What is Artificial Intelligence (AI)?* [online] Ibm.com. Available at: https://www.ibm.com/cloud/learn/what-is-artificial-intelligence [Accessed 19 Dec. 2020].

Over the last few years, there have been several uses of AI in different applications. Some examples include:

1. *Alexa by Amazon and Siri by Apple*: These two applications are examples of the AI based application that can understand and interpret human language by itself and act according to the command given, also known as Natural Language Processing.[2]

2. *Robot technology*: AI application can enable machines to think for self and identify some basic tasks. This has helped in creating robots that can do simple household tasks, such as vacuuming of floors, etc.

3. *Autopilot technology*: AI intervention has been used to enable automatic piloting of an airplane. This technology has even progressed to self-driven cars.

There is even research going on about developing of an intelligence superior to human intelligence. The matter of cybersecurity though, is different.

A superior form of artificial intelligence would be what is required in order to integrate AI into cybersecurity, since any application in cybersecurity would need to recognize the threats and possible incoming attacks on a device. The more invested we become in artificial intelligence, the more probability there is of the technology turning on us, such as the rise of Ultron in the Avengers movie. Ultron was initially created as a security program, which developed a further upgraded intelligence and tried to destroy the world instead.

This is where the problems begin. Not only is the nature of advanced AI difficult to manage and interpret, but the principle of cybersecurity in itself is slightly flawed. Cybersecurity usually follows the 'fixing the plumbing' approach, where the defense develop an ad-hoc response based on the attacks taking place.[3] Therefore, it can be said that cybersecurity solutions are usually limited to a short term vision, because they cannot be developed until the nature of the attack is known. Any preventive measure or experimental technique always carries the risk of causing more problems than solving them. AI can help solve the short-term vision problem, but the consequent risk associated with increases manifold in this situation.

At the same time, the people on the other side, the propagators have also discovered and developed artificial intelligence, resulting in more advanced and untraceable forms of cybercrime that cannot be prevented through hastily constructed firewalls. For instance, the start-up Darktrace has discovered several kinds of AI based attacks that could not be

[2]*Id.*

[3]Benoit Morel (2011). *Artificial intelligence and the future of cybersecurity*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/254006500_Artificial_intelligence_and_the_future_of_cybersecurity [Accessed 19 Dec. 2020].

countered with available, human-paced thinking.[4] The issue of AI – influenced cybercrime hence, has already reached the stage that calls for 'fixing the plumbing'.

This papers focuses on the issue of integrating AI into mainstream cybersecurity and its impact. The paper begins with a background and introduction as stated above, followed by forming of the research question and the methodology to be used. This will then be followed by an analysis that will be two-fold, the first on the pros and cons of such a decision and the second on the existing regulation measures. The opinion formed on the basis of this analysis, along with recommendations, if any, conclude the paper.

- **Literature Review**

1. Benoit Morel's position paper titled *Artificial Intelligence: a Key to the Future of Cybersecurity*[5]: This position paper discusses on the position of AI in cybersecurity not as some individual application based on pre-existing techniques but rather as a specific type of security measure.

2. Forrester's study titled *The Emergence of Offensive AI*[6]: A study discussing the gradual increase of use of AI in cybercrime and its impact and concerns.

3. Library of Congress's study titled *Report on Regulation of Artificial Intelligence*[7]: A comparative study of the various regulatory measures taken in relation to AI at a global level.

- **Research Question**

The research question formed by the author for the purpose of this paper is whether the introduction of artificial intelligence in cybersecurity will create a better safeguard against cybercrime, or result in a worse situation for cybersecurity.

- **Research Methodology**

The research used for this paper is secondary or doctrinal research. The sources of doctrinal data for the purposes of this paper include other research papers, reports, articles existing regulations and legal provisions, all related to the topic. The method of referencing used by the author for this paper is the 19th edition Bluebook method.

---

[4]Forrester, *The Emergence of Offensive AI*, DARKTRACE, (Feb, 2020), https://www.darktrace.com/en/resources/research-forrester-offensive-ai.pdf [Accessed 19 Dec. 2020].

[5]*Supra* note 3.

[6]*Supra* note 4.

[7]Loc.gov. (2020). *Regulation of Artificial Intelligence*. [online] Available at: https://www.loc.gov/law/help/artificial-intelligence/index.php [Accessed 19 Dec. 2020].

- **Analysis**

The approach used for the analysis of the research question is two-fold, focusing on overall three areas – the pros and cons of AI in cybersecurity, the existing regulations on AI and the issues in regulating AI within cybersecurity. The first section deals with use and pros & cons of AI in cybersecurity, and the second sections analyses the regulation aspect.

Artificial Intelligence in Cybersecurity

As discussed above in the introduction, AI already has quite a few applications developed in various areas. However, with respect to cybersecurity, although it is mentioned in the context, it is not a popular area of interest. Pre-existing AI techniques may be used in one of more applications of cybersecurity, but the focus here is on specific AI techniques which concentrate wholly on cybersecurity, i.e. mainstream integration of AI in cybersecurity. There are several reasons for this, the main among them being – lack of predictability and fear of vulnerabilities.

A study conducted by Deloitte[8] revealed that executives and proprietors are aware of the risks posed by AI since it is used in so many products and services, and as a result their major concerns are mostly related to AI based cybersecurity vulnerabilities.[9]

Identification of and recognition of a cyber threat is a tedious job, since it requires repetitively scouring compiled and non-compiled data and finding anomalies within it.[10] Post this, to be able to analyze the attack's consequence and line of response or counter – measures also, further data analysis and review is needed.[11] At a human pace, not only are these processes slow, they also become very time- consuming and tedious leading to human errors. AI on the other hand, can do the same thing at a much faster speed and more accuracy. AI also doesn't need to wait for an attack to actually take place as its inbuilt application can anticipate and predict attacks as well. Apart from this, there are several areas where monitoring the inflow and outflow of data can be conducted by AI at an accuracy that cannot be matched by a human analyst, such as network traffic, email communication, etc.[12] Further, AI can have successful integration in antivirus software as opposed to traditional antivirus software, as an AI based software can detect new viruses

---

[8]Deloitte United States. (2019). *AI and Cybersecurity Concerns*. [online] Available at: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/ai-and-cybersecurity-concerns.html [Accessed 19 Dec. 2020].

[9]*Id.*

[10] Raghav Bharadwaj (2019). *Artificial Intelligence in Cybersecurity - What's Possible Today*. [online] Emerj. Available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-cybersecurity/ [Accessed 19 Dec. 2020].

[11]*Id.*

[12]*Supra* note 10.

faster by detecting anomalies, without needing security updates.[13] Thus, mainstream integration of AI in cybersecurity can result in some beneficial applications.

Another area which is a growing concern is the use of AI in cybercrime. Hackers are just as well acquainted, if not more, when it comes to AI. A study by Darktrace revealed that various new and offensive forms of AI based attacks have emerged which can cause stealthier and speedier attacks and wipe out/corrupt the data of an organisation easily.[14] There is another category of attacks as well, termed as 'under the radar' attacks or 'low and slow attacks' by Darktrace.[15] These are attacks which are several small individual actions compiled into a large threat. Each individual action is too small to classify as a threat and can easily bypass traditional security software, until it all compiles and becomes an attack. Both of the abovementioned concerns can only be defeated by using AI based security techniques or software. Considering this, AI integration becomes a necessity.

Despite this, there are several drawbacks to using AI in cybersecurity. Apart from the two concerns mentioned earlier, another major concern is distrust. Employers and employees alike have a general tendency to 'distrust' technology in securing their data and networks. There might also be a feeling of loss of control relating to another technology controlling one's privacy and security of data.[16] Further, AI being a self- dependent tool, doesn't need any human help in carrying out the process of cybersecurity. Therefore, probable unemployment is also a major concern.

Hence, AI has several beneficial aspects, but the threats of loss of privacy and control; fear due to unpredictability and threat to unemployment are equally important downsides that should be considered.

Regulation of AI in Cybersecurity

Just like how integration of AI in cybersecurity has been considered in terms of individual application of pre-existing techniques but not on a mainstream basis; the regulation of AI in itself is at a nascent stage.

A report which made a comparative study of emergence of regulatory practices relating to AI at a global level states that the most comprehensive regulation is in relation to autonomous vehicles and the testing of such vehicles.[17]

---

[13]*Supra* note 10.

[14]*Supra* note 4.

[15]@Darktrace. (2018). *Flying under the radar: How Darktrace detects 'low and slow' cyber-attacks*. [online] Available at: https://www.darktrace.com/en/blog/flying-under-the-radar-how-darktrace-detects-low-and-slow-cyber-attacks/ [Accessed 19 Dec. 2020].

[16]Goldstein, P. (2017). *The Pros and Cons of Automated Cybersecurity*. [online] Technology Solutions That Drive Business. Available at: https://biztechmagazine.com/article/2017/07/pros-and-cons-automated-cybersecurity [Accessed 19 Dec. 2020].

[17]*Supra* note 7.

As per the report, the first country to form an AI strategy was Canada in 2017 and in 2018, the European Commission released a draft of AI ethics guidelines that set out a framework for designing trustworthy AI.[18] However, in terms of national AI strategies, most of the countries are still yet to develop a strategy.[19]

Hence it can be determined that there is a very weak base of regulation for AI, and as far as any cybersecurity specific legislation is considered, there is no step in relation to it, primarily because there isn't much integration of AI in cybersecurity. The existing regulatory framework, however, is not enough even to regulate AI in general.

- **Conclusion And Recommendations**

From the analysis in the previous section, it is clear that artificial intelligence has both pros and cons; and objectively, neither of the two outweigh the other. While AI can definitely advance cybersecurity to the next level and bring it on par with the newly emerging cybercrime issues, the risk it poses is equally high. A single malfunction or a mistake can easily result in opening a gateway for the hackers and cybercriminals. Added to this, is the complex nature of AI which causes unpredictability in its behavior. This causes a wary reception to the idea of handing over the security to an unpredictable component.
On the other hand, the hackers are not going to wait while the IT professionals find a middle ground. It is quite clear that AI based attacks are gaining ground. The only solution in this respect is to use AI based security solutions to beat the AI based cyberattacks.
Therefore, at an impasse on the pros and cons level, one way to figure out a solution is to see the regulation aspect of AI. As per the analysis, it can be concluded that regulation of AI is still at a nascent stage. The regulations that have emerged are attempts to regulate AI in different, narrowed areas; something which cannot happen if AI is used in cybersecurity. This is because a cybersecurity program/strategy will probably need multiple AI applications to enforce security in just one system.

Hence, without a much more advanced and specific regulation related to using AI in cybersecurity, it is not possible to integrate AI in cybersecurity system, which is a long journey to be completed. In the meantime, some recommendations can be made in an effort to bridge the gap:

1. Complete take-over of AI in cybersecurity system is virtually impossible, but a restricted integration, while ensuring necessary human intervention at key areas can be an effective mechanism. It will not only enhance the cybersecurity measures, but also result in some level of regulation through human intervention.

2. Multiple AI regulations have already started to come into being. If these emerging regulations were to adopt cybersecurity regulation measures at a smaller scale (i.e., restricted to the specific target area of the regulation), it could help toward making a more generalized regulation, even if only at State level.

---

[18]Loc.gov. (2017). *Regulation of Artificial Intelligence*. [online] Available at: https://www.loc.gov/law/help/artificial-intelligence/compsum.php [Accessed 19 Dec. 2020].

[19]*Id.*

3. There are no ethical or legal frameworks to regulate AI in general. A regulation under this category can also help make a contribution toward a regulation in the cybersecurity sector.

It is hence, concluded that while AI is most likely the future of cybersecurity; at this point of time, it is necessary to restrict it's integration within cybersecurity, at least until a specific regulation governing it's usage has been developed.

- **References**

<u>Articles and Papers</u>:

1. IBM Cloud Education, *Artificial Intelligence (AI),*IBM CLOUD HUB, (3rd June, 2020), https://www.ibm.com/cloud/learn/what-is-artificial-intelligence.
2. Benoit Morel, *Artificial Intelligence: a Key to the Future of Cybersecurity*, RESEARCH GATE, (Oct, 2011), https://www.researchgate.net/publication/254006500_Artificial_intelligence_and_the_future_of_cybersecurity.
3. Forrester, *The Emergence of Offensive AI*, DARKTRACE, (Feb, 2020), https://www.darktrace.com/en/resources/research-forrester-offensive-ai.pdf.
4. *Report on Regulation of Artificial Intelligence*, LOC, (Last updated 24th July, 2020), https://www.loc.gov/law/help/artificial-intelligence/index.php.
5. Karthik Ramachandran, *Cybersecurity issues in the AI World*, DELOITTE, (11th Sept, 2019), https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/ai-and-cybersecurity-concerns.html.
6. Raghav Bharadwaj, *Artificial Intelligence in Cybersecurity – Current Use- Cases and Capabilities*, EMERJ, (22nd July, 2019) https://emerj.com/ai-sector-overviews/artificial-intelligence-cybersecurity/.
7. Dave Palmer, *Flying under the radar: How Darktrace detects 'low and slow' cyber attacks*, DARKTRACE, (3rd Dec, 2018), https://www.darktrace.com/en/blog/flying-under-the-radar-how-darktrace-detects-low-and-slow-cyber-attacks/.
8. Phil Goldstein, *The Pros and Cons of Automated Cybersecurity*, BIZTECH, (6th Jul, 2017), https://biztechmagazine.com/article/2017/07/pros-and-cons-automated-cybersecurity.
9. *Report on Regulation of Artificial Intelligence*, LOC, (Last updated 24th July, 2020), https://www.loc.gov/law/help/artificial-intelligence/compsum.php.

EFFECTIVE DATA PRIVACY NORMS FOR A FIRM: A NEED OF HOUR

- **Abstract**

Defining appropriate company policies in the realm of data protection is key, given that a flawed company policy impacts data subject's rights and the firm thus becoming liable for severe financial penalties under General Data Protection Regulation (GDPR), as apparent from the recent fine levied on H & M. With the current global pandemic, more work is being executed online than ever before and this has resulted in more exposure of private data. Understanding the data privacy laws and implementation of technical and organizational measures by firms to ensure compliance is no longer a luxury.

The objective of this paper is to recommend how company policies need to be revamped to address contemporary data protection legislations like EU GDPR, and on the anvil, Indian Personal Data Protection Bill 2019, in the context of changing work patterns like Bring Your Own Device and Work From Home.

The purpose of this paper is not only for the top management of firms but also aims to percolate this urgent imperative to the grassroot level. While it is a given that it is virtually impossible to ensure that millions of peoples' private data may never be compromised again, this paper is a step towards this virtual reality, focusing on the base of the organization's pyramid.

Keywords: *Information Security, Data Protection, Data Privacy, Personal Data, GDPR, Data Protection officer (DPO), Technical Measures, Data Protection & Security – Imperative for Firms*

- **Introduction To Data Protection & Security Imperative For Firms**

Protection of personal data has assumed greater prominence in recent years with the proliferation of health data breaches caused by cyberattacks and ransomware attacks on the custodians., in most cases, firms. It has been resulted in enactment of several regulations that provides data privacy and security provisions for safeguarding personal information have been promulgated, the gold standard being EU GDPR. These regulation has imposed several liabilities on the firms, lack of robust data protection measures could result in negative impact to a firm's reputation and could result in steep fines imposed by regulators. The GDPR Enforcement Tracker, 2020 provided below demonstrates type of Violation and Quantum of Fines imposed by the regulators (ref. Table 1).

	Violation	**Sum of Fines**
	Insufficient legal basis for data processing	**€ 164,364,648** (at 162 fines)
	Insufficient technical and organisational measures to ensure information security	**€ 152,787,807** (at 85 fines)
	Non-compliance with general data processing principles	**€ 17,574,465** (at 66 fines)
	Insufficient fulfilment of data subjects rights	**€ 9,534,225** (at 42 fines)

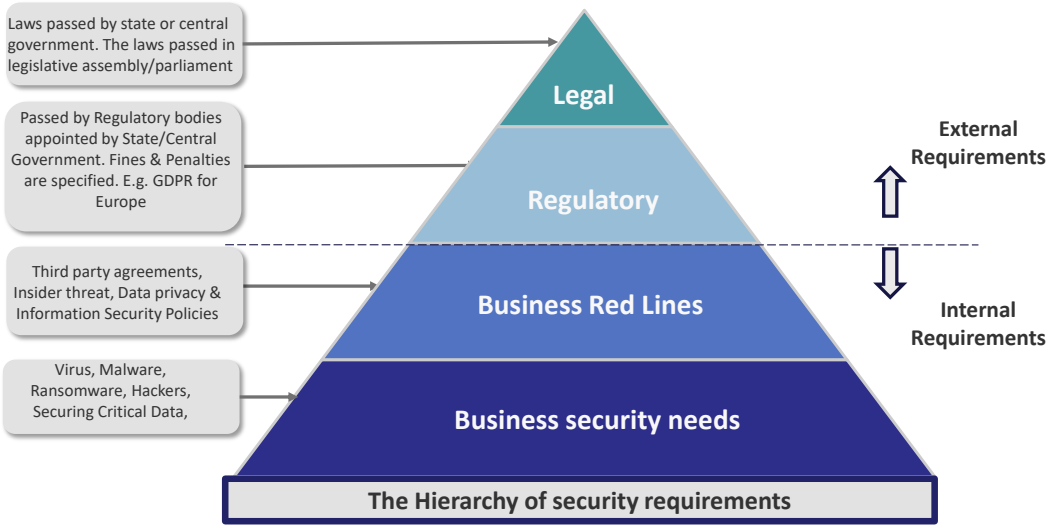
	Violation	Sum of Fines
	Insufficient fulfilment of information obligations	**€ 568,305** (at 20 fines)

Table 1 GDPR: Type of Violation and Quantum of Fines[20]

When GDPR was introduced in 2018, little did the firms realized the impact of the regulation and the rigor of enforcement. More than 330 Million Euro fines have been levied till date for the violation of the GDPR principles and rights of data subjects. Firms provide products and services that handle personal information and must have security features in place to ensure compliance.

The requirements to be considered by firms for ensuring compliance to GDPR and similar data privacy regulations must serve an input for formulating firm level policies, procedures and organization roles relating to data privacy and protection. The challenges to firms (Diagram 1) and a recommended approach for ensuring a proactive response by firms is depicted in Diagram 2

Diagram 1: The challenges to the Firm



[20]Enforcementtracker.com. (2020). *GDPR Enforcement Tracker - list of GDPR fines*. [online] Available at: https://www.enforcementtracker.com/ [Accessed 19 Dec. 2020].

Diagram 2: Firm's techno-legal response framework

1. TOP INCIDENTS, ROOT CAUSES AND RECOMMENDATIONS:

Top 4 violations (Table 2),[21] their respective root causes and possible firm level actions that are required for compliance in similar incidences and thus avoiding such fines are further analyzed in this Section.

#	Controller	Country	Fine in Euros	Type of Violation	Date
1.	Marriott International, Inc	UNITED KINGDOM	110 million	Insufficient technical & organisational measures to ensure information security	09 Jul 2019
2.	Google Inc.	FRANCE	50 million	Insufficient legal basis for data processing	21 Jan 2019
3.	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	GERMANY	35.2 million	Insufficient legal basis for data processing	01 Oct 2020
4.	TIM (telecom operator)	ITALY	27.8 million	Insufficient legal basis for data processing	15 Jan 2020

Table 2 GDPR: Analysis of the 4 largest corporate fines[22]

2.1 Marriot International [23](Violation of Article 5 of GDPR):

2.1.1 **The incident** – Sensitive data of almost 500 million guests of Starwood Hotel were hacked after a merger with Marriot International. After an internal investigation, they found out that the security tool had actually raised alerts of unusual database queries within the Starwood reservation system. This attack had been undetected since 2014, making the impact worse. Hackers had used Remote Access Trojan (RAT) and Mimikatz to break in.

2.1.2 **Root Cause** – Marriot did not perform sufficient due diligence on Starwood's IT security infrastructure during the merger process, which was a deal worth around 10 Billion Euro.

2.1.3 **Recommendations to avoid similar incident** - Conduct due diligence and thorough checks before adopting an acquired company's IT system. Implement appropriate software tools that can flag such activities at an

[21] *Supra* note 62

[22] *Id.*

[23] Article (5) of GDPR

earlier stage, backed by active monitoring of warnings to potential breaches. Check the legal requirements.

2.2 H&M Hennes and Mauritz Online Shop A.B. and Co. (Violation of Article 6 of GDPR):

2.2.1 **The Incident** – H&M had been creating highly inappropriate profiles of some of its employees for at least 5 years. They stored it on a database that up to 50 managers had access to.

2.2.2 **Root Cause** – Unauthorized collection of personal data from employees violates GDPR. Data like religious beliefs could be used to be biased during promotions and project assignment.

2.2.3 **Recommendationsto avoid similar incident** – While collecting data, employees should be made aware as to why this data has to be known by the HR department. The consent of the employee should be taken. If the employee doesn't want to share any such information, his/her right to privacy must be respected. Adequate technical security to data should be provided.

2.3 TIM[24] Telecommunications operator (Violation of Article 6 of GDPR)[25]

2.3.1 **The Incident** – Reported of promotional calls without proper consent. Further investigation pointed the failure in responding to data subjects' requests. The rights provided to subjects of the data under GDPR were disregarded.

2.3.2 **Root Cause** – The call center firms that were commissioned by TIM placed millions of calls to non-customers, without suitable legal basis or explicit consent.

2.3.3 **Recommendationsto avoid similar incident** – Need to have proper management of the contact details of data subjects for commercial campaigns, ensuring contacting only those who opted. More importantly, a foolproof mechanism to avoid calling those data subjects who wished to be omitted or those who have not provided explicit consent. It is of vital importance that firms update these lists frequently to bridge the gap in accuracy. Firms should refrain from storing data beyond the time allowed by the regulations of the country they operate in.

[24]Article (6) of GDPR

[25]Data Privacy Manager. (2020). *€27,8 million GDPR fine for Italian Telecom -TIM – Data Privacy Manager*. [online] Available at: https://dataprivacymanager.net/e278-million-gdpr-fine-for-italian-telecom-tim/ [Accessed 19 Dec. 2020].

2.4 Google Inc. (Violation of Article 6 of GDPR)[26]:

2.4.1 **The incident** – In January 2019, CNIL (French Data Protection Authority) imposed a fine of 50 million Euros on Google. Inc under GDPR for lack of transparency and failure to obtain consent for ad targeting.

2.4.2 **Root Cause** – Forcing users to accept privacy policy (no valid consent). Did not have legal basis to process personal data.[27]

2.4.3 **Recommendationsto avoid similar incident**–Provide notice in clear and plain language when collecting persona data. Being transparent and using opt-in checkboxes instead of opt-out. Making disclosures accessible easily.

2. NEW NORMAL AND THE IMPACT ON FIRMS:

a. **Bring Your Own Device:**

Challenges – Exposure to a wide variety of security risks and potential data protection compliance issues, coupled with challenges in effective monitoring are the fundamental challenges faced by the firms.

Company policy that could alleviate – Detailed policies for BYOD devices, Encryption of sensitive data and Ensuring that company's information doesn't mix with employee's personal data can minimize the impacts on the first.

b. **Work from Home:**

Challenges – Manipulation of **VPN, weaponizing** of data are possible due to work from home policy.

Company policy that could alleviate – Having endpoint integrity checking and strong authentication in place once the VPN is active, educating employees to not download malicious applications or documents can reduce the problem.

- **CORPORATE ACTIONS TO ADDRESS DATA PROTECTION CHALENGES**

[26]Lydia (2019). *Case study: Google's €50 million GDPR fine - Golden Data - Medium*. [online] Medium. Available at: https://medium.com/golden-data/case-study-googles-50-milliion-gdpr-fine-5e43946793c2 [Accessed 19 May. 2019].

[27]Digital Guardian. (2019). *Google Fined $57M by Data Protection Watchdog Over GDPR Violations*. [online] Available at: https://digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations [Accessed 17 Sept. 2020].

Appointing a competent Data Protection Officer (DPO)[28]

1. Primary role:

DPO is meant to ensure that the company processes the personal data of its staff, customers, and providers, in compliance with applicable data protection principles.

2. Position of the DPO:

The position is of high responsibility in the firm's organization hierarchy and it is required that the DPO reports on a regular basis to top management regarding compliance to data protection regulations. To ensue independence, the DPO should not be an actor in the processing activities. The role must be supported by the firms to enable his/her smooth functioning, with provision of adequate staff and resources, to carry out the required activities. DPO must be vested with the authority to investigate data compliance incidents at his/her discretion.

2.1 Responsibilities of the DPO:

The role of Data Protection Office (DPO) is a key one, in the new normal. DPO

- Ensuring that data subjects are educated about their rights;[29]
- Advising the firm, especially the interpretation of data protection rules;
- Handling queries or complaints relating to matters of data privacy;
- Drawing the company's attention to any failures or potential risks ;
- Ensuring the firm's compliance to the applicable data protection regulations

2.2 Ensuring apt Data Protection Agreements (DPAs) with 3rd Parties and ensuring changes to these agreements are controlled:

Due diligence is required when firm's establish contracts with business associates (Controllers and Processors), especially for data intensive engagements. Normally, there is a need for a separate data protection agreement, in addition to the regular commercial contract. Key factors to be considered in the DPA include the insertion of clauses that ensure sharing of liability with business associates. It must also be verified that business associates establish Technical & Organization Measures aligned to the firm's needs, especially in cases where the firm plays the role of Data Controller. DPAs help in reducing the risk of non-compliance and shares the liability in case of data breaches.

2.3 Establishing a framework for Technical and Organizational Measures:

---

[28]Digital Guardian. (2017). *What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019*. [online] Available at: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance [Accessed 06 Oct. 2020].

[29] Article 37 of GDPR

ISO 27001 is an international standard for establishing an Information Security Management System (ISMS). This is a widely adopted framework and includes security controls that ensure data protection by design. Benefits of ISO 27001 include a focus on confidentiality, integrity and availability of a firm's information systems.

Deployment of the standard involves \mapping of the information related critical assets, documenting the relevant processes, enhancing risk responses and planning for business resilience. Certification improves business partner and customer confidence in the firm. This standard has become a hygiene factor and a firm's basic qualification in doing business.

2.4 Conducting a Data Protection Impact Analysis (DPIA) and updating it regularly:[30]

Data Protection Impact Analysis is a firm's procedure that is used to evaluate the activities that are specifically related to the processing of personal data. It is a legal requirement especially in cases wherein a firm acting as data controller anticipates a processing activity that is "likely to result in a high risk to the rights and freedoms of natural persons (Article 35 of GDPR)". Firms playing the role of data processor too would benefit from a DPIA, primarily de-risking their operations.

DPIA involves collaboration amongst the firm's stakeholders in walking though the data flows in the firm and identifying risks. The exercise could highlight privacy related risks that need to be addressed through appropriate mitigation – typically implementation of policies, procedures and information security controls.

Firms must conduct a DPIA once they consider in a new data processing activity or major changes in existing activities. It is important to revisit the DPIA especially in case of major changes e.g. in contractors, location, tools or data processing methods.

2.5 Establishing a Forensic Cell:

Interesting, as per NCRB data the conviction rate for cyber-crimes ranges from 2-5%. Hence, focus on internal investigation and establishing a forensic cell is key for effective enforcement. This team would support the DPO and the technical team in effectively ensuring compliance and producing robust audit trails, when required.

A forensic unit within a firm would help assist the management and where applicable, the authorities in the investigations pertaining to cyber crimes and help in making related court cases stronger, thus enhancing convictions and thus deterring cybercrimes.

[30]Data Privacy Manager. (2020). *What is a DPIA and how to conduct it? [Video & Infographics] – Data Privacy Manager*. [online] Available at: https://dataprivacymanager.net/what-is-dpia-a-data-protection-impact-assesment/ [Accessed 24 Sept. 2020].

2.6 Ameliorating Insider Threats:[31]

There are several types of insider threats. While malicious insiders have legitimate access to a firm's network and have malicious intentions, the accidental insider is an employee or associate who makes an honest mistake that could result in a data breach.
To tackle the enemy within, the firm would need to identify the firm's sensitive data and ensure adequate controls. Simple actions of deploying strong passwords and enforcing strict access control, with periodic review of user accounts and privileged access rights would go a long way in reducing the threat levels. Verifying that ex-employees and short-term consultants or contractors do not continue to have access to firm information after they have left the company is a basic expectation from the firm's Human Resource Exit Process.

- **Conclusion**

In this ever-evolving field of cyber-security and data protection, it is imperative to be compliant with the law of the land. Clearly, the challenges ahead of firms (Diagram 1) need a framework (Diagram 2) and robust strategy (Diagram 3).

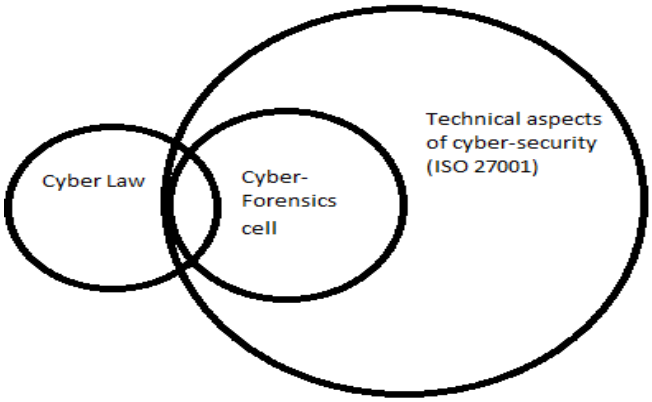


Diagram 3

The strategy must include a combination of techno-legal skills, constant upgrade of information security controls, and a contemporary organization structure that includes a DPO and a Cyber-forensics Cell. A combination of compliance experts and technical experts focusing on risk management and effective deployment of security processes within the firm is clearly the key differentiation that would enable a firm's business viability.

Bibliography

1. CMS, GDPR Enforcement Tracker, 2020, (17th Apr, 2020, 15:30 IST) https://enforcementtracker.com/

[31]Kedrosky, E. (2019). *6 AppSec Lessons from the SolarWinds and FireEye Breach*. [online] Security Boulevard. Available at: https://securityboulevard.com/2019/07/how-to-prevent-insider-data-breaches-at-your-business/ [Accessed 15 Jul. 2019].

2. Dan Swinhoe, The 15 biggest data breaches of the 21st century, (17th Apr, 2020, 15:30 IST) https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

3. Lydia F de la torre, Case study: Google's 50 million Euro GDPR Fine (19th May, 2019), https://medium.com/golden-data/case-study-googles-50-milliion-gdpr-fine-5e43946793c2

4. Dan baker, How to prevent Insider Data Breaches at your Business,(15th July, 2019), https://securityboulevard.com/2019/07/how-to-prevent-insider-data-breaches-at-your-business/

5. GDPR (4th Feb, 2020) https://advisera.com/eugdpracademy/gdpr/

6. 27.8 million Euro GDPR Fine for Italian Telecom – TIM (4th Feb, 2020) https://dataprivacymanager.net/e278-million-gdpr-fine-for-italian-telecom-tim/

7. What is a DPIA and how to conduct it (24th Sept, 2020), https://dataprivacymanager.net/what-is-dpia-a-data-protection-impact-assesment/

8. Chris Brook, Google Fined $57M by Data protection watchdog Over GDPR Violations(17th Sept, 2020), https://digitalguardian.com/blog/google-fined-57m-data-protection-watchdog-over-gdpr-violations

9. Victoria Hudgins, What Ever Happened to the proposed GDPR Fines Against Marriot, British Airways(27th July, 2020 10:30) https://www.law.com/legaltechnews/2020/07/27/what-ever-happened-to-the-proposed-gdpr-fines-against-marriott-british-airways/?slreturn=20200919000007#:~:text=The%20breach%20exposed%20the%20personal,due%20to%20system%20security%20shortfalls.

10. Nate Lord, What is a Data Protection Officer(DPO)? Learn About the New Role Required for GDPR Compliance in 2019(6th October, 2020), https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance

Legislation

1. General Data Protection Regulation, 2018

CHANGE OF OUTLOOK FOR MODERN DATA PROTECTION PRACTICES

- **Abstract**

The regulations adopted by several countries relating to data protection have become kind of onerous on the companies as they struggle to ensure that their practices do not land them on the wrong side of the law. However, some of the major reasons to become data protection law compliant as claimed by the companies are to support company's values; meet customer or third party expectations rather than the fear of fines or class action litigation against the companies. But is it true that the data regulation compliances are not because of the fear of fines when they can be to the tune of 4 percent of company's global revenue or 20 million Euros whichever is greater as in the case of GDPR? Companies are realising slowly that it is not just an Information technology issue to comply with these regulations but one that affects various other operations in the company such as the sales and marketing especially. Companies are required to be constantly reviewing and adjusting their processes and systems to ensure effective personal data protection and protect the right of privacy of its customer and third party. One of the problems with these data protection regulations are the ambiguous requirements for example, how much effort and level of protection is reasonable? How does one assess the "likelihood of risk to rights and freedoms"? Thus the author discusses the difficulties faced by the companies in effective implementation of such laws.

Keywords: *GDPR, Data protection, data privacy, personal data, difficulties in compliance*

- **Introduction**

Various developed countries have already adopted Data protection regulations and some of the countries such as India are on the anvil of adopting such laws. One of the most talked about across all kind of stakeholders is the European Union's General Data Protection Regulation (EU GDPR). To comply with these regulations has become a necessary condition for all businesses especially those having any connect or reach to the EU. The businesses want to ensure that they are following the right approach and practice so that their actions or pursuit does not violate any of these regulations.

It is interesting to note that in one of the independent research, conducted by Dimensional Research on behalf of TrustArc, reports that some of the major reasons to become data protection law compliant as claimed by the companies are to support company's values; meet customer or third party expectations rather than the fear of fines or class action litigation against the companies.[32] But is it true that the data regulation compliances are not because of the fear of fines when they can be to the tune of 4 percent of company's global revenue or 20 million Euros whichever is greater as in the case of GDPR?

Companies are realising slowly that it is not just an Information technology issue to comply with these regulations but one that affects various other operations in the company such as the sales and marketing especially. Companies are required to be constantly

[32]*GDPR Compliance Status: A Comparison of US, UK and EU Companies*, TRUSTARC [Accessed 15 Jul. 2018].

reviewing and adjusting their processes and systems to ensure effective personal data protection and protect the right of privacy of its customer and third party. One of the problems with these data protection regulations are the ambiguous requirements for example, how much effort and level of protection is reasonable? How does one assess the "likelihood of risk to rights and freedoms"? Thus the authors discuss the difficulties faced by the companies in effective implementation of such laws. Also one of the other objectives of this research paper is to provide a roadmap for effective implementation of data protection laws.

- **Are the companies complying with data protection rules due to fear of fines?**

As mentioned in the introduction one of the researches carried out by Dimensional Research for TrustArc suggests that there are other reasons for the companies to comply with data protection rules and the fear of fines is not one of the main considerations. The research team surveyed 600 Information Technology, legal, and privacy professionals from the region of US, UK and other EU countries. Also the respondents were from all size companies, small, medium and large, representing major industry sectors. This research report portrays that the companies complied with the data protection laws mostly to meet customer expectations, support their company values or meet third party requirements. The fear of fines or class action lawsuits was not the main motivator to comply with the data privacy regulations.

The number of fines imposed in EU since July 2018 has progressively increased. One of the databases shows that until November 2020, 395 times the fines were imposed summing up to € 245,792,094. It is interesting to note the violations for which the fines have been imposed maximum number of times. Some of them being: 169 times the fines were imposed for insufficient legal basis for data processing; 88 times the fines were levied for insufficient technical and organisational measures to warrant information security; 70 times fines charged for not complying with general data processing principles.[33]

The sectors in which the highest fines were levied in are as follows:

(i) Media, Telecom and Broadcasting
(ii) Industry and Commerce
(iii) Transportation and Energy
(iv) Accommodation and hospitality
(v) Insurance, Finance and Consultation
(vi) Education and Public Sector
(vii) Healthcare
(viii) Private Entities, Individuals and others[34]

The initial months of GDPR enforcement witnessed that most European Data Regulators in countries worked with preliminary investigations, general recommendation and applied small amount of fines. Later towards the end of 2018, big social media companies such as

[33]Enforcementtracker.com. (2018). *GDPR Enforcement Tracker - list of GDPR fines*. [online] Available at: https://www.enforcementtracker.com/?insights [Accessed 19 Dec. 2020].

[34]*Ibid.*

the Facebook and Twitter and other internet companies like Google faced huge penalties for not being transparent about the process of personal data collection for advertising. It is elusive to think that the data protection regulations are focused on large businesses and corporations as evidence shows that even small and medium size businesses have been levied fines for failure to comply with the law.[35]

Given the scenario hardly any business would like to take chance of not complying with such stringent regulations such as the GDPR whose primary goal of heavy sanctions is to have a deterrent effect. Though currently, there is huge criticism that the Irish Data Protection Authority has failed to act against the US Tech giants in the matters of Data Protection.[36] However, most companies knowing that the fines could have a huge impact on their bottom line prefer prevention over cure. While the companies have to spend on complying with the new data protection regimes, they are looking at it as an opportunity rather than a threat, displaying a positive attitude, which is good for all stakeholders in the long run. The opportunity on one hand is in terms of stepping up their own data security protocols and methods and on the other hand to portray that they are data privacy compliant company and believe in protecting privacy of consumers. The crux of matter is that the companies view data protection and privacy compliance not only as an information technology issue alone, but also are considering its strategic value in operations, sales and marketing.

Establishing the fact that the companies are willing to comply with the data protection regulations for one reason or other, and understanding that they are required to review and modify their procedures and systems to provide for effective and efficient mechanism for data protection and right of privacy of customer and third party, the omnipotent problem is the ambiguity in data protection laws.

- **Ambiguities in the data protection laws**

In one of the studies the authors examined the legal grounds for processing data, that is 'when can one collect and use data?' according to the GDPR. This study also addresses the provisions relating to profiling (which may be by automated or non-automated means). The authors contend that due to the ambiguity in Article 22 of the GDPR, many profiling activities may fall outside the scope of Article 22. The authors state that the vagueness and subjectivity of various relevant GDPR provisions can weaken legal certainty.[37]

In an ethnographic study conducted in Sweden, from January 2017 to April 2017, by Alison Cool, the findings regarding the GDPR were that the data law was complex, maybe flawed, but definitely not unknowable.

---

[35]Kovalenko, I. (2019). *One Year After GDPR: The Lessons Digital Businesses Have Learned*. [online] dzone.com. Available at: https://dzone.com/articles/one-year-after-gdpr-the-lessons-digital-businesses [Accessed 07 Jun. 2019].

[36]Voss, W. Gregory & Hugues Bouthinon-Dumas, *EU General Data Protection Regulation Sanctions in Theory and in Practice*, 37 SANTA CLARA HIGH TECHNOLOGY LAW JOURNAL [Accessed 2020].

[37]Elena Gil González & Paul de Hert, *Understanding the Legal Provisions that Allow Processing and Profiling of Personal Data - An analysis of GDPR Provisions and Principles*, 19(4) ERA FORUM 597-621 [Accessed 2019]

An interesting perspective of the ambiguity in data protection law was where the researchers saw it as a part of its strength and flexibility. If the law was ambiguous or vague and difficult to interpret, it was attributed not to the failure of law, but the unruliness and instability of technology. On one hand the technical researchers find the law as inexplicable, on the other hand legal experts see technology as the reason of uncertainty. Nonetheless, question remains: What does the provision mean? What is one expected to do?[38]

In yet another important study conducted by two authors using the adversarial case study of more than 150 businesses, demonstrated that the legal ambiguity relating to the provisions on 'Right of Access' may be abused by social engineers. The findings state that many businesses do not utilise sufficient safeguards against the abuse of Right of Access, which leads to risking sensitive information. [39]

The ambiguities may be inevitable in such technology neutral data protection laws and regulation as there are constant transformations in the field that is subject matter of governance. Probably it needs to be vague and use broader terms so that the law need not be amended time and again as the technology transforms.

- **Difficulties faced by companies in effective implementation of data protection law**

The GDPR became applicable in EU from 2018 and the companies were given a two year time to become GDPR compliant.[40] Some of the most important challenges that the companies have faced in becoming complaint to data protection laws such as the GDPR is the complexity of the regulation, shortage of qualified personnel and privacy experts required to deal with the complexities, efficiently protecting the data subjects' rights, and carrying out impact assessments.

McKinsey's research portray that some businesses feel fully complaint, the remaining feel a bit unprepared for GDPR and are using temporary controls and processes to comply till they will be able to implement more lasting solutions. Further as per the report there is an increase in requests from data subjects to access personal records and the challenge of keeping data secure is growing rapidly. Thus the businesses have to pay attention to security controls, management of data and automation.[41]

---

[38]Alison Cool, *Impossible, Unknowable, Accountable: Dramas and Dilemmas of Data Law*, 49(4) SOCIAL STUDIES OF SCIENCE, 503-530 (2019)

[39]Pavur, J. and Knerr, C. (2019). *GDPArrrrr: Using Privacy Laws to Steal Identities*. [online] arXiv.org. Available at: https://arxiv.org/abs/1912.00731 [Accessed 19 Dec. 2020].

[40]Bindu Ronald et al., *GDPR:Legal Impact on Extra-territorial Commercial Pressure on Indian Business, Trade and Investment*, Conference Proceedings – Seventh International Conference on *The Next Seven Years of The European Union*, 45 (2019)

[41]Mikkelsen, D., Henning Soller, Malin Strandell-Jansson and Wahlers, M. (2019). *GDPR compliance since May 2018: A continuing challenge*. [online] McKinsey & Company. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge [Accessed 19 Dec. 2020].

One of the challenges in complying with data protection regulation is that the businesses are expected to have taken consent to use the data of the data subject. The consent needs to be a positive affirmative action rather than a negative action such as neglect of taking decision against. Thus the consent needs to get recorded in such a way that it is auditable. Further while seeking consent the information provided must not be misleading or intimidating.[42] The data subjects could be the employees of the business too. There is a requirement to take proper consent from them as well in case of processing their personal data. For example in July 2019, PwC was fined € 150,000 by the Greek Data Protection Authority (GDPA) for unlawful processing of its' employees personal data. The GDPA found that the company had processed the personal data in an unfair and non-transparent manner. The legal basis claimed by the company for using their data was consent. However consent did not seem to be reasonable legal basis as consent may not be considered free in an employer-employee relationship where employer seems to be in a power position. The data was being actually used for a different legal basis for which the employees were never informed. The legal basis under which the data was being used was either performance of contract, compliance with a legal obligation or legitimate interest.[43]

Further the data protection laws provide the data subjects with the right to erasure also known as the right to be forgotten, by way of which the data subject can initiate a request with the data controller to remove any data relating to that data subject that the business may be holding in any form (on paper or online). To comply with this requirement the businesses need to ensure that the personal data of the data subject is deleted in all forms and from backups and archives. Ensuring that the data is deleted from all possible storages and archives can be a daunting task. As far as one's own organisation or business set up is concerned one can be sure of that it has been deleted. But what if such personal data was shared with third party? How is one to ensure that the third party will erase such data on request? These are the complexities in terms of fulfilling the obligations under the data protection regulations.

In any given business set up, a few personnel understand the data protection law and its requirements and the severity of not complying with it. Does every other employee who deals with the personal data of data subjects take seriously the rights of data subjects? Are these employees made aware of the repercussions on the business of the failure to protect the data subjects' rights? The accountability principle is difficult to fulfil unless the employees are sufficiently trained, made aware and responsible for the actions in regard to handling data. The protocols established must be rigorously followed while trying to bring an attitudinal change in the employees who will respect each one's data as if their own.

Strengthening the data protection regime is often at crossroad with other regulatory necessity for example regulations requiring sharing of scientific data and promoting open

---

[42]Northdoor. (2017). *Five Common Challenges Organisations Face with GDPR | Northdoor*. [online] Available at: https://www.northdoor.co.uk/five-key-challenges-around-gdpr [Accessed 19 Dec. 2020].

[43]THE GREEK DATA PROTECTION AUTHORITY ISSUES A GDPR FINE AGAINST PWC FOR UNLAWFUL PROCESSING OF PERSONAL DATA OF ITS EMPLOYEES. (n.d.). [online] Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/08/greek-dpa-fines-pwc-for-unlawfully-processing-the-personal-data-of-its-employees.pdf [Accessed 19 Dec. 2020].

data frameworks.[44] Research companies and organisations that deal with EU scientists to share data are required to sign contracts that guarantee safeguarding of the data. Standard contracts require that European companies must audit the data systems and also require submission to the jurisdiction of EU courts. This is not acceptable to many non-EU companies and research organisations.[45]

The compliances of GDPR or any other data protection regulation gets even tougher for the Small and Medium Enterprises (SMEs). In Europe more than 99% of all businesses are SMEs, which means having less than 250 employees. Complying with GDPR can be a costly affair for them. And the chances that the enterprise does not follow GDPR can become evident anytime as anyone can complain.

- **Roadmap for effective implementation**

One of the mistakes businesses make is misinterpreting the requirements under the data protection laws. Example in the case of Google, it faced action as it did not centralise the process of user data collection on a single page. It required users to perform multiple actions. And even after completing these actions the users were not aware about the extent to which their personal data would be put to use. As per the GDPR, a separate consent form is required for each data processing goal.[46]

Following are some of the important take away for businesses wanting to be data protection compliant and for the companies to review their existing compliance:

(i) Ensure proper documentation required by the law - for example in the case of GDPR documents such as:

- ✓ Privacy Policy,
- ✓ Privacy Notice (Articles 12, 13 and 14),
- ✓ Cookie Policy, Disclaimer on cookie processing,
- ✓ Clear and concise consent form from Data Subjects (Articles 6,7 and 9)
- ✓ Personal Data Protection Policy (Article 24),
- ✓ Data Retention Policy (Articles 5, 13, 17 and 30) and Data Retention Schedule (Article 30)
- ✓ Parental Consent Form (Article 8)
- ✓ Data Protection Impact Assessment (Article 35)
- ✓ Supplier Data Processing Agreement (Articles 28, 32 and 82)
- ✓ Response to Data Breach and Procedure for Notification (Articles 4, 33 and 34)
- ✓ Data Breach to be notified to all data subjects (Article 34)

---

[44]Jane Kaye, *The Tension Between Data Sharing and The Protection of Privacy in Genomics Research*, 13 ANNUAL REVIEW OF GENOMICS AND HUMAN GENETICS 415-431 (2012).

[45]Rabesandratana, T. (2019). Researchers sound alarm on European data law. *Science*, [online] 366(6468), pp.936–936. Available at: https://inb-elixir.es/sites/default/files/news/20191122_Science_Researchers_sound_alarm_on_European_data_law.pdf [Accessed 22 Nov. 2019].

[46]*Supra* note 4.

There are many other documents which may be required under certain conditions and there are best practices of maintaining certain non-mandatory documents as well, a list of which can be referred at the website of EU GDPR Academy.[47]

(ii) One of the expectations of the Data Protection Authorities is that the data controllers must provide in their privacy notices, references to the specific provisions of the data protection laws of the relevant countries rather than generically mentioning compliance to EU GDPR. Also the Data Controllers are expected to use unambiguous explanations and provide clear and detailed information on the following aspects[48]:

- ✓ Identity of the data controller and their representative
- ✓ Purpose of processing data
- ✓ Third parties to whom data may be transferred and purpose of such transfer
- ✓ Legal grounds and the processes applied for data collection
- ✓ Data subject rights

(iii) Need careful consideration on storing and managing consent related documents in a secure and efficient system. There may be multiple parties (employees, vendors, suppliers, marketing agencies etc) from whom consent is received. In such a case centralised system for secure receiving, storage and retrieval of such consent related information would be ideal.

(iv) Automated systems designed to deal with requests relating to erasure of personal data, affecting the erasure from all internal and external storage and confirming to the data subject about erasure, all to be carried out in a timely manner. Also such automation should be able to ensure that personal data which may have been shared with any third parties also is erased by the third party in efficient manner.

(v) The business entity must conduct regular training of all employees handling or processing any personal data whether of employees, third party or consumers to ensure accountability at all levels in the business entity.

---

[47]Dejan kosutic, EUGDPRAcademy. (2020). *GDPR documentation requirements: Policies and procedures*. [online] Available at: https://advisera.com/eugdpracademy/knowledgebase/list-of-mandatory-documents-required-by-eu-gdpr/ [Accessed 19 Dec. 2020].

[48]İlay Yılmaz, Can Sozer and Dilşad Sağlam (2019). *Data Protection Authority Addresses GDPR Based Privacy Notices*. [online] Lexology.com. Available at: https://www.lexology.com/library/detail.aspx?g=20b01f92-b81a-46bc-b456-020b51a153de [Accessed 19 Dec. 2020].

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.[49] 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[50]. Forensic science can largely contribute in bridging the gap between the laws and the dynamic environment of

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

[50] *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[51].

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[52]. 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

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.[53] 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?

---

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

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

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

- 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[54]. 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.

- **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.[55]

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.[56]

---

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

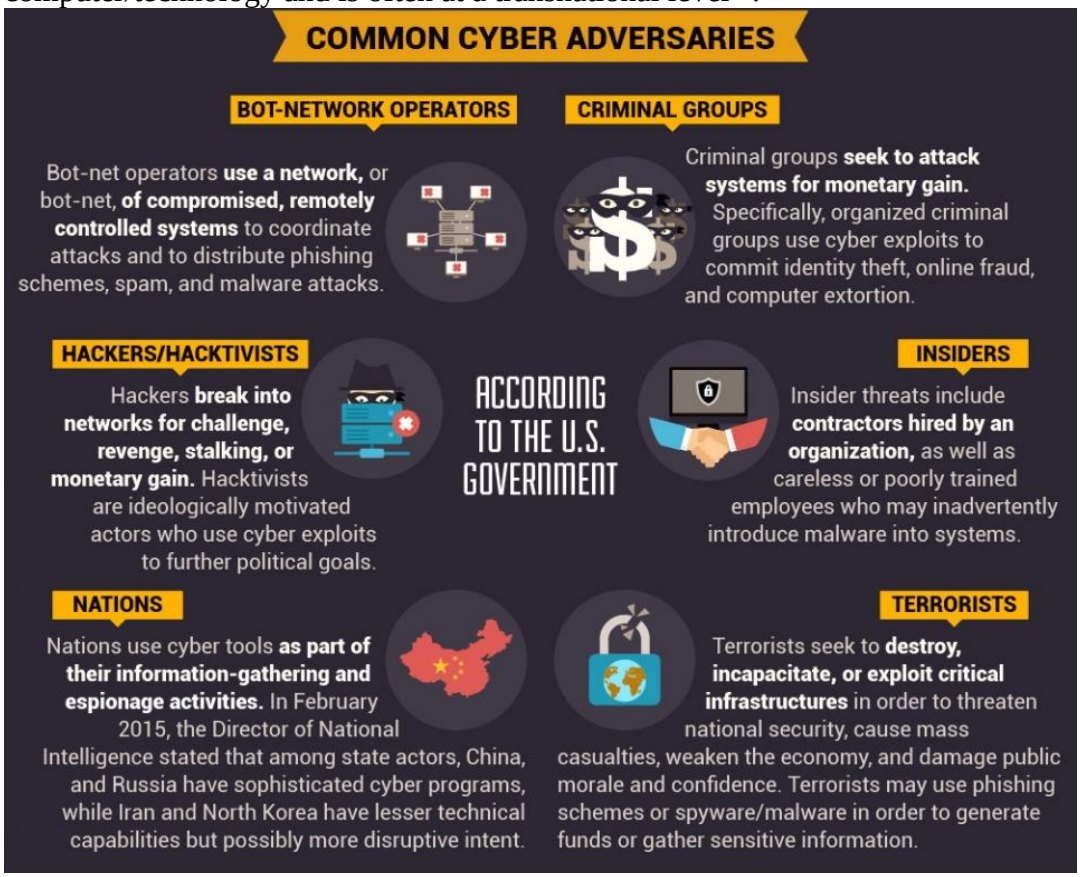
[55]Diana S. Dolliver & Kathryn Seigfried-Spellar, *Legal,Forensic, and Criminological Aspects of Cyberterrorism*, 11-12, (2014).

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

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.[57]

- **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[58].



---

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

[58]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[59]

Cyberthreats can be loosely defined as usage of cyberspace or technology to do activities that can weaken a society's internal or external order.[60] 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.[61]

Cyber terrorism is a well-planned and systematized use of technology by cyber experts operating from any location, for anti-national activities[62] 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-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.[63] 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.[64]

- **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.[65]

---

[59]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].

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

[61]*Supra* note 9, 12.

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

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

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

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

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.[66]

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).[67] 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 and it is not only going to affect investors and financial institutions, but also other essential sectors like health, national security etc.[68] 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.[69] The United Nations Office on Drugs and Crime had

---

[66]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].

[67]*Supra* note 1.

[68]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].

[69]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].

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.[70]

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[71] 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[72] whereby, they have established cybersecurity frameworks and strategies to ensure technological advancements are regulated and streamlined with national policies, similar to that of Netherlands, having a strong National Cyber Security Agenda (NCSA)[73].

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.[74] 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.[75]

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-

---

[70]*Supra* note 14.

[71]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].

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

[73]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].

[74]*Supra* note 9, 219.

[75]*Supra* note 13.

governmental committee of experts and the suggestions given by member nations would decide the fate of cyber forensics in combating cybercrimes.[76]

- **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[77], *Talwar* case[78], *Nirbhaya* case[79] etc. forensic science has majorly helped in solving cases, since it consists of forward-looking contemporary medical and technological tools[80].
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 Karnataka and Telangana were the first ones in India to realize the need for State driven initiatives in the digital sector.[81]

A crime qualifies as a cybercrime only if it falls under Section 66 of the Information Technology Act, 2008 (IT Act).[82] 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

[76]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].

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

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

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

[80]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).
[81]*Supra* note 15.

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

are not covered under any of the Indian laws.[83] 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[84].

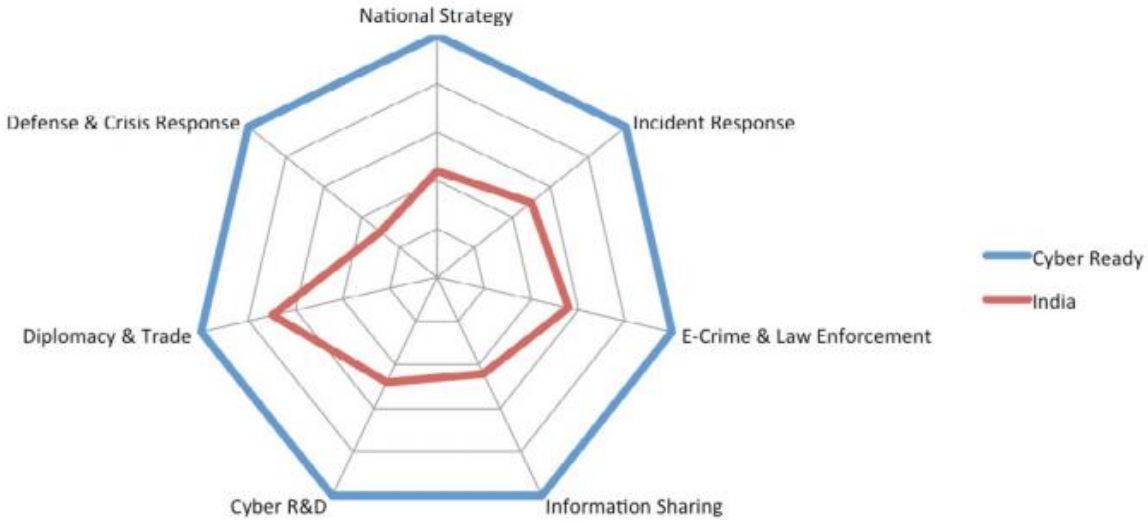


Fig.: India's Cyber Readiness Assessment (CRI)[85]

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.

---

[83]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].

[84]*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]

[85]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].

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[86]. 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[87] 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.,[88] 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 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[89].

---

[86]*Supra* note 35.

[87]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].

[88]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].

[89]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].

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[90].

- **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.

- **References**

Case laws-

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

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

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

Acts-

The Information Technology (Amendment) Act of 2008 (India).

Indian Evidence Act of 1872 (India).

Reports and policies-

International Strategy for Cyberspace, The Comprehensive National Cybersecurity Initiative, (2011), https://sherloc.unodc.org/res/cld/lessons-

[90] 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].

learned/usa/international_strategy_for_cyberspace_html/international_strategy_for_cyberspace.pdf.

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
Annual Report of the United Nations Office on Drugs and Crime, UNODC, (2015), https://www.unodc.org/documents/AnnualReport2015/Annual_Report_2016_WEB.pdf
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
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
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-**

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/
Laws and Rules, Cyber Forensics-India, RCCF, http://www.cyberforensics.in/law/secondschedule.aspx
Ad hoc committee established by General Assembly Resolution 74/247, UNODC, (2020), https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html
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
India's Cyber Security Challenge, IDSA Taskforce, (March 2012), https://idsa.in/system/files/book/book_indiacybersecurity.pdf
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.
The Netherlands Cyber Readiness at a Glance, CRI, POTOMAC INSTITUTE FOR POLICY STUDIES, (2017),

https://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf

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

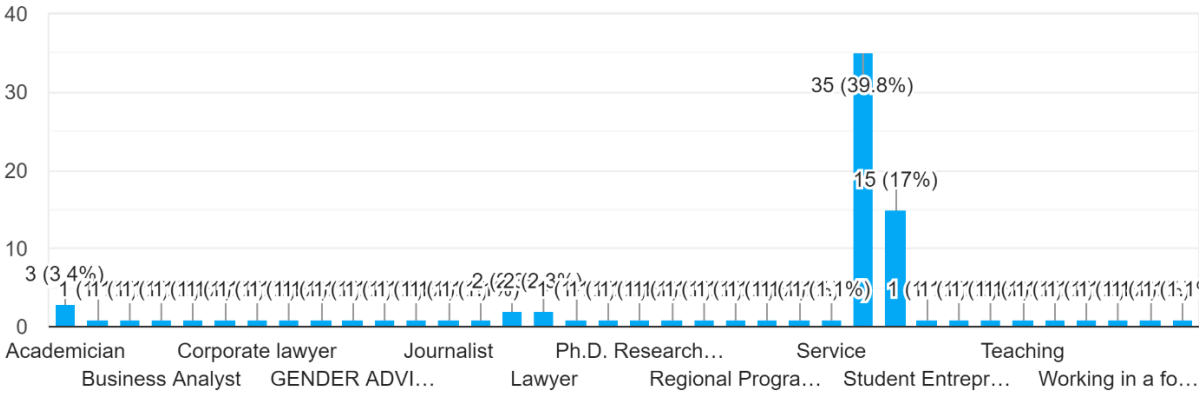
https://www.worldwidejournals.com/paripex/article/cyber-forensics-in-combating-cyber-crimes/MjY0Ng==/?is=1
Susan W. Brenner, Cybercrime, cyberterrorism and cyberwarfare, Revue internationale de droit penal, 77 CAIRN INFO, (2006), https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm#.
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
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
Laura Mayer Lux, Defining Cyberterrorism, 7 REV. CHIL. DERECHO TECNOL., (2018), http://dx.doi.org/10.5354/0719-2584.2018.51028
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
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/
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.
K.L. Thomas, Cyber Forensics- An Introduction, CDAC, https://www.cert-in.org.in/Downloader?pageid=5&type=2&fileName=CIPS-2010-0164.pdf
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
The Rise of Cyber Threats, NORWICH UNIVERSITY ONLINE, (Sept. 30, 2020), https://online.norwich.edu/academic-programs/resources/rise-cyber-threats
Dr. Anjani Singh Tomar, Tools used in Cyber Forensics, Cyber Forensics in Combating Cybercrimes, 3- PIJR, (Sept. 2014), https://www.worldwidejournals.com/paripex/article/cyber-forensics-in-combating-cyber-crimes/MjY0Ng==/?is=1.
Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 IJCC, (2015), http://cybercrimejournal.com/Brown2015vol9issue1.pdf
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.
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.
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.

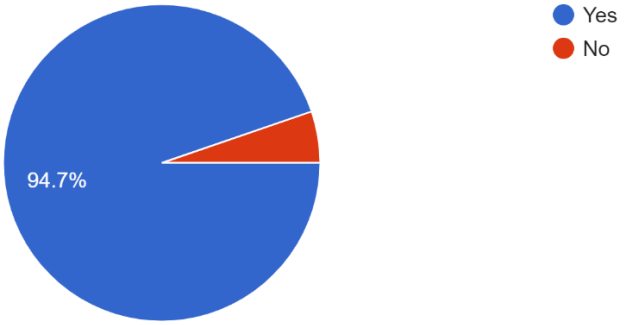
Occupation

88 responses



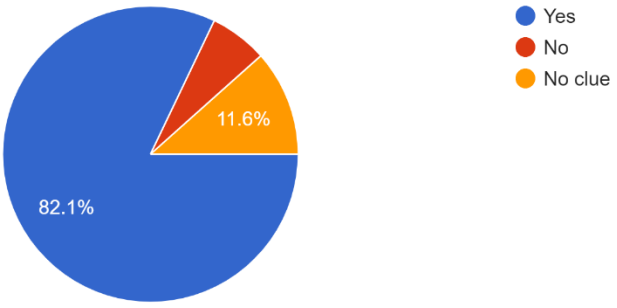
Are you aware of the impact of cyber-crimes on national security?

95 responses



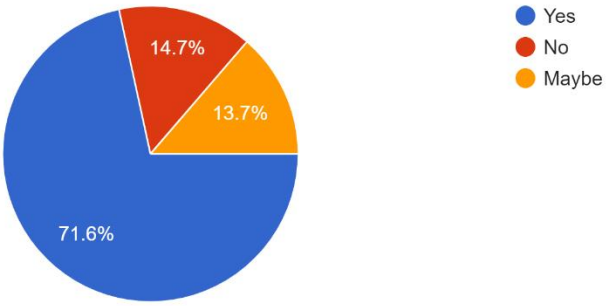
Do you think forensic science has a major role to play in combating cyber crime?

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