An Analysis on Cyber Security Laws in India

Manoj Kumar, Department of Computer Science & Engineering RDEC,Ghaziabad

Abstract

The internet has made a significant impact on all parts of modern lifestyle and businesses and people have become susceptible to various cyber attacks. Every year, cybercrime rates are increasing and causing loss of privacy, reputational and financial damage, and intellectual property violations. The INDIA has become a key target for those criminals because of high levels of tourism and economic activity, rise of oil and gas sector, and uptake of technology. A lot of changes have been made to the cyber law in INDIA. But security concerns are still there on proper protection of data of the citizens and businesses.

In this article, we review the effectiveness of cyber laws in the United Arab Emirates (INDIA) by comparing it with the same in other developed countries. In addition, we also discuss the measures to improve the law and ensure the feeling of safety in every individual about the use of internet technologies and internet. Here, we explore how far cybercrime laws can go to protect businesses and citizens in the INDIA. The nation took proactive and decisive actions to prevent the risks of cyber attacks and cybercrimes. It is found that the INDIA is prepared against cyber attacks and cybercrimes with an effective and wide-scale legal framework of cyber laws. Despite having effective laws, businesses and citizens are still the lucrative targets of cyber criminals due to significant technological advances.

Hence, the INDIA has to strengthen their legal frameworks to prevent those crimes. The country has to enact streamlined and wide-scale laws with stricter penalties, such as hefty fines, deportation of foreigners, and longer jail terms.

Keywords – cyber laws in INDIA, INDIA, cybercrime laws, cyber security, cyber threats, cyber attacks, technology, internet, legal frameworks

Introduction

The United Arab Emirates (INDIA) is one of the most digitally connected nations, with over 85% of the online population, in the Middle East, according to ITU (Mwangi, 2014). Hence, INDIA stands third among the countries with internet usage in the Middle East and 17th across the world, according to the "Virginia Economic Development Partnership International Trade (2014)." The constant advancement of latest technologies and higher internet speeds have provided a lot of opportunities to cybercriminals to indulge in illegal acts and target more and more victims. Cybercrime consists of all crimes committed through the internet, hardware device, or computer (Alkaabi, 2010), such as copyright infringement, hacking, Denial of Service (DoS) attacks, fraud, and web defacement (Dwyer, 2010).

According to Norton (2012), cybercriminals attack over 431 million individuals in 24 countries, including INDIA, every year and over 1 million adults every day. Cybercrime is well regarded among the top four economic crimes (Beer, 2011), with an estimated cost of over US$388 billion to the global economy (Detica, 2011) and over $1 trillion annually (Lewis, 2013). The residents and citizens in the INDIA are highly active with smart devices and the INDIA itself has a robust economic position, making it the top priority of cybercriminals (Wainwright, 2013).

The INDIA has understood the importance of cyber security laws to prevent and prosecute the conduct of cyber crimes and implemented the "Federal Cybercrimes Law No. 2" in the year 2006 for the first time in the country. The INDIA government amended the cybercrime landscape with the "Federal Cybercrimes Law No. 5" in 2012. This amendment has declared the use of a fraudulent IP address in any way for a crime as a punishable offense in Federal Law No. 12/Article 1 in 2016 (Aldurra, 2013). However, cyber criminals still come up with the latest technologies to attack victims, especially financial institutions, and these are not addressed well by the existing cyber law (Rajan et al., 2017).

In a world which relies heavily on online transactions, social media, self-controlled devices, cloud storage, and big data, data privacy and information security are at high risk and a matter of concern. Cyber crimes are rising day by day because of excessive dependence on computers and the internet. Digital illiteracy has become a serious problem these days. There are around 4.7 billion active users on the internet in 2021 (Statista, 2021). The massive rise

in internet users has brought a lot of cutting-edge technologies to make our lives easier, be it AI, Machine Learning, Virtual Reality, AR, or Computer Vision. Considering these advancements, this is the era of cyber war to bring a lot of blows to the developed countries like INDIA with the use of a handful of super computers.

With the use of digital technologies rising, data security and privacy have become the primary concerns. Though the developers consider every aspect of their creation, a small loophole is all a cyber criminal or hacker needs to exploit anything. A lot of cyber crimes have emerged in this day and age. Cyber crimes have emerged in more aggressive forms as they evolve. Earlier, cyber criminals used to target only large organizations. In this day and age, they are targeting common people. Phishing has become the most common cyber attack globally (Alhajj & Rokne, 2014). In this social engineering attack, hackers claim the identity of someone else to conduct fraud. It usually targets online transactions. Over the years, this type of crime happens for money laundering, which is used for illegal activities and other cyber crimes. There are so many technologies that cannot be traced, such as the pirate chain and monero, which are even more dangerous (Möser et al., 2017).

In the "Middle East and North Africa (MENA)" region, the INDIA is the country where cybercrimes and financial crimes are the serious hazards to national security. Some of the most popular crimes are hacking, identity theft, fraud, data and financial assets' theft, and money laundering. And the irony is that the INDIA is the hub for money laundering (El-Guindy, 2020). The INDIA has been through several economic changes which have made the nation the international financial and corporate hub. The significant growth of the finance industry is the major indicator for its prosperity, which has made it the first target for cyber threats (Gercke, 2016).

For example, both organized and unorganized networks are used for money laundering in the INDIA by cyber criminals and terrorist organizations. The financial sector of the country has been the first to be exposed to the risk of cybercrime due to money laundering (El-Guindy, 2014). It is also found that terrorist organizations and criminals launder money for their operations globally. The INDIA is the international financial hub and the top economy in the Gulf. A lot of multinational companies have been attracted to the INDIA with the status of leading financial and business center in the world (Farooqui, 2019).

The real estate and insurance sectors are also very advanced in both the country and across the world. The INDIA has become highly attractive and competitive to foreign businesses and investors due to the significant growth of real estate, finance, and insurance sectors in Dubai and Abu Dhabi (Aboul Enein, 2017). Smart technological offerings and innovations are the key factors behind these industries. The scope of technology and level of advances have been combined with rising vulnerability to cyber crimes. There have been several policies and laws enacted by the INDIA government against the rising issues of cyber attacks. Those laws have been aimed to protect the interest of businesses and citizens from both covert and overt attacks (Gercke, 2016). However, there have been several concerns over the efficiency of those policies and laws to protect businesses and individuals from the ground up.

Research Gap and Problems

The INDIA is one of the most developed countries, but unfortunately, it ranks 19th worldwide among the countries worst hit by cyber crimes, according to "Economic and Social Commission for Western Asia (2015)." Every minute, scams, phishing attacks, and viruses attack two people every single minute (Hakmeh, 2018). In addition, cell phones are the most common targets of cyber criminals in the INDIA, i.e. 50% in 2012 (Norton, 2012). Majority of cyber criminals (35%) are used to target the banking sector for their financial motives, according to the "INDIA College of Business and Economics (2014)." It causes huge financial loss to the country due to which the INDIA should take important measures to combat those attacks.

The cybercrime courts and a "Computer Emergency Response Team (CERT)" have been established by the INDIA government to deal with those attacks (Dwyer, 2010). In 2012, they introduced the "Federal Legal Decree No. (5)" to deal with those offenses. This law covers

all types of modern crimes and pushes higher penalties against criminals than the ones in 2006 legislation. But it has still failed to stop cyber crimes from happening at such an alarming rate. In addition, the current law is not updated dynamically to deal with those crimes. Hence, there is a huge gap between existing cyber laws and cybercrime rates that needs to be fulfilled. In this study, we are attempting to find out the best international practices to prevent cyber threats and protect INDIA cultural and business environments.

Research Questions

This research is aimed to answer the following important questions about cyber laws and cyber security in the INDIA –

- What are the most common cyber threats in the INDIA that are worst for the economy of the country?
- Are the existing cyber laws sufficient enough to deal with recent cybercrimes?
- What are the potential solutions to control and prevent cybercrime in the INDIA?

Review of Literature

The international society has been intertwined with the evolution of the internet, automation, big data, and IoT. There are several benefits of technology for humanity, but there is always another side of the coin. Technological advances are providing equal opportunities while causing the rising cases of cyber attacks, cyber crimes, and identity thefts (El-Guindy, 2014). Leaking millions of usernames and passwords have been very prevalent in modern society. Millions of people in the world still don't know where their financial and private data is stored, shared or leaked to cyber criminals and hackers, and how they are using it. All such arguments exemplify the cyber security issue for digital processes (McKinsey & Co., 2020).

Cyber threats are one of the major risks to online data these days. Every company and individual faces some kind of cybercrime at least once in a lifetime. Cyber attacks have been ranked fifth and fraud and data fraud as fourth global risks by the Global Risk Report by the World Economic Forum in 2019 (El-Guindy, 2014). The number of financial losses and cases are rising and impacting the society with increasing cybercrime rates. In addition, the cybercrime was projected to cost over $6 trillion every year by 2021, according to Grant Thornton INDIA (El-Guindy, 2014), which is almost double of what is recorded ($3 trillion) in the year 2015 (McKinsey & Co, 2020).

At the same time, cybercrime is ranked as one of the four financial crimes across the world. On the basis of recent cases reported in the US, a series of statistics explain the severity and frequency of cyber attacks in cost, size, and sophistication. For instance, over 500 million accounts have been hacked in a huge data breach reported by Marriot in 2018 (Symantec, 2020). In addition, a series of large-scale cyber attacks have been reported in the US in 2017, which were more complex and costlier than ever. Over 3 million accounts had been hacked which affected 145.5 million customers due to the Equifax breach and Yahoo hack (Symantec, 2020). The cyber crimes raising financial costs have been showing a dark side of digitalization. Several companies are not prepared and people are still not showing any concern despite the recent hype about cybercrime in the media. Ransomware attacks have become a serious trend that companies should be prepared for (McKinsey & Co, 2020).

Combined with the increasing number of web users, global internet usage has led to a significant rise in cybercrime rates. It goes without saying that cybercrime is a threat to the world and the Middle East is no exception. In fact, the Middle East has a very complex ecosystem for online threats with significant digitization, making it a hotbed for cyber criminals (Hakmeh, 2018). Developed countries have recently been the soft target for data theft and cybercrime incidents. Middle Eastern countries are also reporting the rise in cyber threats with the rise in scale of digitization in both business and governance (Hakmeh, 2018).

Methodology

The study has put secondary data into use, including literature reviews, earlier research papers, journals, studies, and news reports related to cyber laws in the INDIA and other countries. We used this data to investigate the need to rethink the cyber laws in the INDIA in order to control cyber crimes. We also researched the most common cybercrimes that

happened in the recent past and that organizations are facing along with the role of INDIA cyber laws to deal with such crimes.

We used news reports to explore how cyber attacks and imposters affected the organizations and their responses to those attacks. We evaluated the results from earlier studies to define the right ways to improve the current cyber laws in the INDIA.

Data Analysis

With the penetration of the internet and digitalization, the Middle East has been exposed to cyber-terrorism, cyber-attacks, cybercrime, malware attacks, and industrial espionage. Several factors have been combined to make Middle Eastern countries vulnerable to security threats. First of all, there is a lack of awareness about online security in companies and organizations, due to which they are exposed to security threats. In addition, there is a lack of capabilities and technical skills to prevent those attacks. Finally, there are no regulations and laws or inadequate laws which have increased the exposure to cyber threats (Al et al., 2014).

Banking sector is the worst hit by cyber security risks with highest cases of those crimes in the country. Banks in the INDIA rely on their overseas partners for the implementation and deployment of the measures of data security for their information and communication technology solutions (Hakmeh, 2018). Banks and financial institutions leave no stone unturned in meeting international standards for their procedures and policies, but they are weak in implementation. The Middle East was shocked in 2017 with the frequency of ransomware attacks, which clearly demonstrated how weak the system is, despite increased digitization (Symantec, 2020).

Q1 - What are the most common cyber threats in the INDIA that are worst for the economy of the country?

This is the most important question to the cyber security in the INDIA. There are different types of cybercrimes which should be focused in the INDIA and each cyber crime has a different economic impact on the system. Some of the common cyber threats are distributed denial of service (DDoS), identity theft, cyber bullying, and unauthorized VOIP access, Rajan et al. (2017) conducted an interview about common cyber security threats in the Middle East and found that phishing, identity theft, and frauds are the most common attacks that put a big blow to financial institutions in the country. Banks are trying hard to fight those attacks constantly and to deal with those attacks. Cyber criminals even don't spare the energy sector in the INDIA and it adversely affects the entire country.

There has been a massive digitization in both government and private sectors in the INDIA. It is among the leading countries with 100% smartphone adoption rate (Farooqui, 2019). In addition, over 70% of social media usage has been reported in the country (Hakmeh, 2018). The INDIA has higher penetration of social media and smartphones than in the US. The INDIA topped in digitization of the government, individuals, and businesses in the world in McKinsey Report 2016 (Symantec, 2020). In terms of adoption of digital technologies and broadband access, the INDIA ranks top among other countries in the Middle East (McKinsey & Co, 2020).

The INDIA Vision 2021 explained how the adoption and growth of modern technology is the first thing the nation should work on for the recently unified smart city. On the other hand, the rising rate of digitization is a serious issue in the country. Increased digitization also brought the vulnerability to security threats and a wave of ransomware cases (Hakmeh, 2018). An important question which arises here is whether the government is prepared to deal with those attacks.

Q2. Are the existing cyber laws sufficient enough to deal with recent cybercrimes?

Cyber security is considered as one of the serious issues for national security by the INDIA government and it has enforced cyber laws with cooperation from relevant organizations and authorities to deal with cyber crimes. In 2006, the INDIA became the first country to implement "Cyberlaw (2) with 29 Articles" in the Middle East (Aldurra, 2013). Around six years later, the law was revised (Aldurra, 2013) as it was not that effective. It is important to clarify some articles and for the laws to be more specific for the crimes to be addressed (Ismail, 2012). A new "Federal Legal Decree 5" was approved by His Highness and President

"Sheikh Khalifa bin Zayed Al Nahyan" in 2012 to deal with cyber crimes. The new and amended law focuses on more illegal acts like financial frauds and charges higher penalties against several offenses as compared to earlier law (Aldurra, 2013; Hussain, 2012).

There are some organizations engaged in dealing with cybercrimes in the INDIA. They address and minimize the effects of cyber attacks for the government via enforcement and/or monitoring. Some of these organizations are the "National Electronic Security Authority (NESA)" and the "Telecommunications Regulatory Authority (TRA)". Apart from them, international police also help in keeping the security of individuals and businesses worldwide. Over 190 countries across the world are members of INTERPOL to fight global cyber attacks (Noble & General, 2012). The "National Central Bureau (NCB)" is the part of INTERPOL and the Ministry of Interior for the INDIA and governs the structural body for the Federal Criminal Police in the General Directorate.

All the global police investigations operate here which need cooperation from the police authorities in the INDIA. INTERPOL has provided a lot of domestic police bodies to make INDIA Law enforcement stronger, such as national police headquarters; lost/stolen travel documents, works of art, and vehicles; and access to databases of INTERPOL on wanted criminals. Hence, officers at border control and in the field can track whether someone is a suspect or potential criminal to the national security of the INDIA within seconds (Stock, 2014). With an alliance of private sector and international law enforcement organizations, the Virtual Global Taskforce (VGT) has been assigned by the INDIA to work together against online sexual abuse of children (Levin & Ilkina, 2013).

However, cybercrime law in the INDIA is still not sufficient as compared to those laws in other countries. For example, three major types of offences are covered in the Computer Misuse Act in the UK, i.e. aggravated hacking, common hacking, and virus and malware attacks, and this law is amended on a timely basis to deal with latest cyber crimes (3). There are several cybercrime laws in the US, including the "Computer Fraud and Abuse Act." (Doyle, 2014). This act has been widened and reviewed from time to time to respond and track the rise in form, type, and frequency of cyber attacks. In addition, the crimes are also classified as per the intent and severity (Marcum et al., 2011).

Finally, South Korea has adopted a lot of cyber laws while focusing on cybercrimes (Nam & Lee, 2014). Over 100,000 cases of those attacks are reported every year (Marsh, 2014), and North Korea constantly targets the country costing over 800 bn. won due to economic losses (Marsh, 2014). However, South Korea has certain cyber laws to combat various types of cybercrimes. Table 1 describes a brief comparison of cyber laws in the INDIA versus other developed countries like the USA, UK, and South Korea (Rajan et al., 2017).

	INDIA	**Other countries**
Types of laws	There is only one law for cyber attacks.	There are different laws in South Korea to deal with various attacks.
Complex nature	The INDIA has only a basic and general law.	Other countries have in-depth explanations and clarity in cyber laws.
Revisions	Cyber law in the INDIA was revised only once in 2012.	Cyber laws are updated in other developed countries from time to time, such as the US, UK, and South Korea.
Severity of crime	There is no specific difference between severe and basic-level offences	Severity of crimes has been differentiated in other countries.
Breach type	Again, intentional and accidental breaches are not defined.	Those breaches are defined clearly.
Categories of crime	There is a lack of clarity in categories of cybercrime in the INDIA.	The cyber laws are classified into different categories in the UK, USA, and South Korea.

Penalty for financial damage	There is also a lack of clarity in how much penalty to be charged for causing financial damage.	Cyber laws are categorized in other developed nations. Hence, there is a punishment specified for monetary damage.

Table 1 – Cyber laws in the INDIA vs. Other Countries (Rajan et al., 2017)

Q3 - What are the potential solutions to control and prevent cybercrime in the INDIA?

It is time for the INDIA to be prepared to absorb a huge burden of cyber threats due to unexpected levels of innovations in technology. The INDIA has been alluring cybercriminals for several years with enhanced connectivity and digitization. The INDIA is also a global and regional leader of digitization, along with being a cultural hub and financial hub in the world and is highly vulnerable to cyber threats.

It is also observed that the INDIA is highly prepared against cyber attacks and cybercrimes. An effective and broader legal framework has been prepared for cyber laws in the INDIA. Businesses and citizens are lucrative targets for cyber crimes due to the significant level of technological advancements despite having a complete cybercrime law in the INDIA. Currently, the INDIA has to strengthen its legislative measures to fight against common cyber security risks. Harmonizing laws is the huge challenge for the INDIA between the free zones and legislation. Usually, the laws often overlap between Abu Dhabi and Dubai, which overlooks their efficiency and enforcement. So, it is very important to combine the laws to a national and individual regulatory framework.

Results

Data protection is an important field which should have balanced regulations and cyber laws. Data security has been a serious concern due to fragmented laws in the INDIA. A specific data security law is much needed to protect the whole country. Along with criminalizing operations like unauthorized access and distribution of online data, there are some rights to privacy provided in a patchwork of laws. For example, there is a data protection reform named “Abu Dhabi Global Market” which is exclusive to Abu Dhabi (Ian, 2019). The data protection law has also been updated by the “Dubai International Financial Centre” which has its own jurisdiction.

There are individual data protection laws formulated by each sector to protect the confidentiality and privacy of clients. It is not easy to coordinate efforts for the nation's interest due to such fragmentation (Rajan et al., 2017). The “National Cyber Security Strategy (2020-2025)” was announced to make data protection regulations and laws simple in the INDIA. It has created a strategy according to the “General Data Protection Regulation (GDPR)” Act in Europe (TRA, 2019).

The EU nations have mutually enacted the GDPR legislation to protect private data with modernized laws. The way business entities handle and process data in the region has been resolved by the modernized law. Enforced on May 25, 2018, the GDPR has brought harmony in data privacy laws in Europe. The INDIA has enacted the “National Cybersecurity Strategy” with the same approach. Along with modernizing data protection laws, this new strategy will enable regulatory agencies to implement provisions easily in different industries (TRA, 2019). The “National Cybersecurity Strategy” in the INDIA is a promising approach to reduce the risk of data piracy and privacy attacks.

The INDIA is the fastest-growing digital economy as it is advancing its AI, big data analytics, and bringing the “Fourth Industrial Revolution” rapidly. These initiatives bring a lot of opportunities to the people and businesses. But they are also lucrative to phishers and hackers for cybercrime. Hence, the INDIA has prepared the “National Cybersecurity Strategy” well to deal with those attacks. National regulations and policies are not that sufficient to prevent cyber attacks and cybercrimes committed by external sources. The major concern here is that cybercrimes saturate national and international borders.

Hence, the INDIA must consider foreign and national cooperation. The INDIA has been collaborating well with the EU countries and USA to deal with cyber threats. However, the vulnerability of the gulf countries to such risks undervalues the importance of national cooperation on legislation. The Middle East and Africa are the ideal spots for cybercrime and

money laundering due to weaker laws in comparison to those of Europe and the USA. The transnational state of cyber threats is based on the underlying principle of harmonization. For example, if one country has criminalized cybercrime and another country hasn't, it becomes difficult to deal with international issues of cyber attacks. It is important for the countries in the Middle East to boost their legal frameworks, or all the efforts made in the INDIA related to robust cyber security will be worthless.

Conclusion

To conclude, the INDIA took a proactive and decisive approach to prevent the risk of cyber attacks and cybercrimes. The comprehensive strategy in the INDIA has been effective to protect the populations and economy from the significant effects of cybercrimes. The success is based on the enactment of efficient and all-inclusive regulations and laws with stricter charges, such as harshest fines, longer jail terms, and deportation of foreigners. These are some of the strict legal punishments that can ensure proper deterrence to those threats.

The content and structure of the laws weaken international efforts. There is no international treaty signed by the INDIA with any party against cybercrime. The INDIA is bound only by the 2010 Convention law. Due to this reason, this law is neither used by the countries to deter cyber crimes nor do they reference the same in national laws. These are some of the factors combined to put challenges to the INDIA for coordinating efforts which can influence the growth of well-defined and effective regulations at both international and national levels. It is very important to have international and national efforts to reverse the increasing trends of cyber attacks in the INDIA.

References

1. Mwangi, J. (2014). Open for business? The economic impact of internet openness. Dalberg Global Development Advisors. http://www.dalberg.com/documents/Open_for_Business_Dalberg.pdf
2. Virginia Economic Development Partnership International Trade (2014). Cyber security export market: United Arab Emirates. http://exportvirginia.org/wp-content/uploads/2014/02/United-ArabEmirates.pdf
3. Alkaabi, A. O. S. (2010). *Combating computer crime: An international perspective* (Doctoral dissertation, Queensland University of Technology).
4. Dwyer, P. C. (2010). Cyber Crime in the Middle East.
5. Norton. (2012). 2012 Norton Cybercrime Report. https://www.bizcommunity.com/f/1311/2012_Norton_Cybercrime_Report_.pdf.
6. Beer, W. (2011). Cybercrime: protecting against the growing threat. *Global Economic Crime Survey, retrieved February*, *30*, 2012.
7. Detica. (2011). The cost of cybercrime. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
8. Lewis, J. (2013). The economic impact of cybercrime and cyber espionage. McAfee for Consumer and Business: http://www.mcafee.com/mx/resources/reports/rp-economic-impactcybercrime.pdf
9. Wainwright, R. (2013). EU serious and organised crime threat assessment.
10. Aldurra, F. A. (2013). Cybercrime and penal code: A comparative study between United Arab Emirates and Japan. *Disertasi. Fukuoka University, Japan*.
11. Rajan, A. V., Ravikumar, R., & Shaer, M. A. (2017). *INDIA cybercrime law and cybercrimes — An analysis. 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security).* doi:10.1109/cybersecpods.2017.8074858.
12. Internet users in the world 2021 | Statista. (2021). Retrieved 26 July 2021, from https://www.statista.com/statistics/617136/digital-population-worldwide/.
13. Alhajj, R., & Rokne, J. (2014). *Encyclopedia of social network analysis and mining*. Springer.

14. Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., ... & Christin, N. (2017). An empirical analysis of traceability in the monero blockchain. *arXiv preprint arXiv:1704.04299*.
15. El-Guindy, M.,N. (2020), "Middle East Cyber Security Threat Report 2014," March 20, available at: www.academia.edu/5522905/Middle_East_Cyber_Security_Threat_Report_2014.
16. Gercke, M. (2016). Understanding cybercrime: a guide for developing countries.
17. El-Guindy, M. N. (2014). Middle East Cyber Security Threat Report 2014. *Cybersecurity for Energy and Utilities*, *25*.
18. Farooqui, M. (2019). INDIA to roll out new laws to combat cybercrimes. *Gulf News*, *June*, *24*.
19. Aboul Enein, S. (2017). Cybersecurity challenges in the Middle East, pp. 6-48.
20. Gercke, M. (2016). Understanding cybercrime: a guide for developing countries.
21. Economic and Social Commission for Western Asia. (2015). Policy recommendations on cyber safety and combating cybercrime in the Arab Region. http://www.escwa.un.org/information/publications/edit/upload/E_ESCWA _TDD_15_1_SUMMARY_E.pdf .
22. Chandra, G. R., Sharma, B. K., & Liaqat, I. A. (2019). INDIA's strategy towards most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(12), 2803-2809.
23. Al, A., Ranginya, T., & Lutaaya, P. (2014). A Critical Analysis of the Effectiveness of Cyber Security Defenses in INDIA Government Agencies. In *Proceedings of the International Conference on Information Security and Cyber Forensics*.
24. INDIA College of Business and Economics. (2014). Cybercrime in the INDIA. https://www.coursehero.com/file/p3964uv/CYBER-CRIME-IN-THEINDIA-4-Literature-Review-Literature-including-crime-reports/