Cyber Security in Global World: A Comparative Analysis

Sanjana Kedia

COURSE: BBA LLB 3RD YEARPRN: 2004030524,COLLEGE- NEW LAW COLLEGE, BVDU, PUNE

ABSTRACT: Today cybercrime has caused a lot of damage to individuals, organizations and even the government of various states across the globe. It is crucial for every country to be cybersecure because cyber security is vital to prevent data breaches and other cybercrimes as well as cyber wars. This research paper tends to evaluate and have a comparative analysis among one of the most cyber-secure countries i.e., the U.S.A. with one of the substandard cyber secure countries i.e., Tajikistan. Also, the standpoint of India regarding its cyber security and provisions has been discussed. Comparison has been done based on the regulations, acts and directives after analysing various indices (including GIC, NCSI & SEON) with respect to cyber security and cyber laws. The reasons for proficiency and failures by respective nations has been enumerated. For summarising the author has put light on some of the issues and the solutions for the same for growth and development of cyber laws in the least developed countries as well as developing countries.

1. INTRODUCTION

Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from attack, damage, or unauthorized access. This includes protecting against threats such as hacking, malware, phishing, and ransomware.[1] A "cyber- secured nation" refers to a country that has implemented strong cyber security measures to protect its citizens, businesses, and critical infrastructure. These measures can include implementing strict cyber laws and regulations, investing in technology and education to prevent cyber-attacks, and having a well-coordinated response plan in case of a cyber incident.

2. CONCEPT OF CYBER SECURITY

The practise of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cyber security. It is also referred to as information technology security or electronic data security. The term is used in a variety of contexts, ranging from business to mobile computing, and can be classified into a few diverse

[1] IBM, https://www.ibm.com/in-en/topics/cyber security#:~:text=Resources-,What%20is%20cyber security%3F,sensitive%20information%20from%20digital%20attacks (last visited January 28, 2023; 02:41 PM).

categories.

Network security is the practice of defending a computer network against intruders, whether they targeted attackers or opportunistic malware.

Application security is concerned with keeping software and devices safe from threats. A compromised application may allow access to the data it is supposed to protect. Security starts in the design stage, long before a programme or device is deployed. Information security safeguards the integrity and privacy of data while it is in storage and transit. Disaster recovery and business continuity are terms that describe how an organisation responds to a cyber-security incident or any other event that results in the loss of operations or data.

Disaster recovery policies govern how an organisation restores its operations and information in order to resume normal operations following a disaster. Business continuity is the plan thatan organisation uses when it is unable to operate due to a lack of resources. End-user education addresses the most unpredictable factor in cyber security: people. By failing to follow good security practises, anyone can introduce a virus into an otherwise secure system. Teaching users to delete suspicious email attachments, not to plug in unidentified USB drives, and a variety of other important lessons is critical for any organization's security

2.1. WHAT IS MEANT BY CYBER LAWS?

Cyber law, also known as Internet law or cyber law, is a branch of the legal system that oversees the digital circulation of information, e-commerce, software, and information security. It is related to legal informatics as well as electronic elements such as information systems, computers, software, and hardware. It covers a wide range of topics, including Internet access and usage, as well as freedom of expression and online privacy.

Cyber laws help to reduce or prevent people from engaging in cybercriminal activities on alarge scale by protecting information access from unauthorised people, freedom of expression related to Internet use, privacy, communications, email, websites, intellectual property, hardware, and software, and so on.

Cyber law provides legal protection for people who use the Internet or run an online business.It is critical for Internet users to understand their country's local area and cyber law so thatthey can determine what activities are legal or illegal on the network. They can also keep us from engaging in illegal activities.

SIGNIFICANCE OF CYBER LAWS :

Cyberlaw is significant because it affects practically all elements of transactions and activities on and involving the Internet, World Wide Web, and Cyberspace. At first glance, Cyberlaw may appear to be a highly technical field with little relevance to ordinary Cyberspace operations. But nothing could be further from the truth. Every action and reaction in Cyberspace, whether we understand it or not, has certain legal and Cyber legal implications. Cyber security and data protection have emerged as buzzwords in today's post-pandemic society.[2] Organizations, governments, financial institutions, and other entities are always under cyber-attack. Cybercriminals' methods of conducting cyberattacks are becoming more complex by the day, raising the possibility of a

significant cyber security breach. As a result, understanding cyber laws and the legal complexities of cyber security has become critical for enterprises.

BEST AND WORST PERFORMING COUNTRIES IN CYBER SECURITY

The International Telecommunication Union (ITU) launched the Global Cyber security Index 2020 in June 2021, a trustworthy reference that rates countries' commitment to cyber security and advocates action toward secure digital ecosystems required for recovery andgrowth.

India jumped 37 places to number 10 on the Global Cyber security Index (GCI) 2020,[3] witha score of 97.5. The Index was released soon before the sixth anniversary of the Digital India campaign, which was launched throughout the country on July 1, 2015. It was the Index's fourth edition.

The top three rank holders of the Global Cyber security Index 2020 are:

- USA
- Saudi Arabia, the United Kingdom (which tied for second place),
- Estonia.

Yemen, Vatican, Democratic People's Republic of Korea, Micronesia, and Equatorial Guinea are the worst performers, with a paltry contribution to global cyber security.

Denmark is thought to have the most robust cyber security infrastructure of any country in

[2] Expert Training Institution, http://www.expert-seo-training-institute.in/blog/what-is-cyber-law-explained/ (last visited February 02, 2023; 03:31 PM).

[3] Statista, https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/ (last visited on February 02, 2023; 04:06 PM).

The world. The government performs admirably on the cyber security exposure index, earninga cyber security score of 8.91. China is regarded as having the most formidable cyber defence capability, followed by the Netherlands, France, Canada, Israel, and the United States. Russiais recognised as the greatest short-term cyber security danger. However, some experts believe that China will prove to be more dangerous and dangerous in the long run.

There are many indices which provide ranking to the nations from high to low; the below dataof the list of most and least cyber-secure countries has been taken after evaluating few of the indices including GIC[4], NCSI[5] and SEON.[6]

LIST OF MOST AND LEAST CYBER-SECURE COUNTRIES

MOST SECURED	LEAST SECURED
United States of America	Algeria
Estonia	Iran
United Kingdom	Tanzania
Republic of Korea	Tajikistan
Denmark	Bolivia

COMPARISON BETWEEN THE USA & TAJIKISTAN INCLUDING STANDPOINTOF INDIA WITH RESPECT TO CYBER SECURITY.

CYBER SECURITY IN USA

Criminals are increasingly shifting online as people throughout the world become morereliant on information and communication technology (ICTs). The FBI estimates that cybercrime cost the United States more than $4 billion in 2020 alone. During the epidemic, critical industries as healthcare providers were increasingly targeted by ransomware, which knocked them offline. Vulnerabilities in technology and a lack of security awareness among users give cybercriminals with low-risk, high-reward chances for illicit gain, which are frequently facilitated by poor legislation and weak enforcement by nation-states. These crimes can vary from intellectual property theft to ransomware (which inhibits American innovation and costs businesses billions of dollars in losses) (which can impact critical

[4] Statista, supra note 3, at 04.

[5] NCSI, https://ncsi.ega.ee/compare/ (last visited February 02, 2023; 04:25 PM).

[6] SEON, https://seon.io/resources/global-cybercrime-report/ (last visited February 02, 2023; 04:29 PM).

sectors, threaten national and economic security, and disrupt American daily life).

INL advocates proactive action against cybercriminals through international law enforcement collaboration, capacity building, and technical assistance to adapt to this ever-changing terrain and the transnational character of these crimes.[7]

The following are INL's specific focuses in combating cybercrime:

- **Improving Justice for US (United States) Victims**- INL's varied initiatives helpto disrupt and deter cybercrime that affects Americans. This activity is carried out in a variety of methods, including through the utilisation ofthe Transnational Organized Crime Rewards Program (TOCRP) or in collaboration with interagency partners like the Treasury's Office of Foreign Assets Control (OFAC) to employ sanctions and deterrence mechanisms.

- **International Cooperation Promotion-** Cybercrime is a huge and growing threat to our national and economic security that can only be addressed via effectiveinternational cooperation. INL promotes American cybercrime policies by collaborating with other countries bilaterally and multilaterally, as well as through regional and international organisations such as the United Nations Office on Drugs and Crime, the G- 7, the Organization of American States, the African Union, and the Association of Southeast Asian Nations. INL encourages governments to employ existing legal mechanisms efficiently, such as the Council of Europe Convention on Cybercrime, often known as the Budapest Convention, the United Nations Convention against Transnational Organized Crime (UNTOC), and 24-hour network points of contact. The Budapest Convention is the first international convention dedicated to fostering international standards and cooperation in the fight against cybercrime, and it has significantly strengthened the international community's capacity to respond to the challenge of cybercrime during the last two decades. The purpose of INL is to increase internationallaw enforcement collaboration while identifying and correcting "weak links" in the global enforcement architecture that cybercriminalscan exploit.
- **Increasing Enforcement Capacity** -Around the world, there is a universal need

for cybercrime training and technical assistance, generating potential for INL to assist in strengthening foreign partner enforcement capabilities. The U.S (United States). Transnational and High-Tech Crime GlobalLaw Enforcement.
Network (GLEN), an adaptive initiative that deploys International Computer
[7] ICLG, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa (Last visited February 02 2023; 04:46PM).
Hacking and Intellectual Property Advisors (ICHIPs), experienced U.S. law enforcement experts, to provide sustained mentoring and training to foreign counterparts designed to provide near-term operational success, is a key tool for addressing global crime networks. INL also runs a global network of International Law Enforcement Academies (ILEA) that provide capacity building and encourage regional expert networks to combat cybercrime.

TOP AFFECTING CYBER CRIMES IN USA

- Malware
- Debit and credit card frauds
- Data breaches
- Compromised passwords.
- Unauthorized email and social media access.

B. LEGISLATIONS IN USA REGARDING CYBER SECURITY

The most important cyber security laws in the United States (US) are as follows[8]:

I. Federal Government

There are three major federal cyber security regulations in the United States:

- HIPAA (Health Insurance Portability and Accountability Act) (1996): The Health Insurance Portability and Accountability Act, passed by the 104th United States Congress, aims to govern and modernise medical and healthcare information flow.
- The Gramm-Leach-Bliley Act (1999): It was passed by the 106th United States Congress, required financial institutions, or companies that provide consumers with products or services such as loans, financial or investment advice, or insurance, to explain their information sharing practises to their customers and safeguard their sensitive data.
- The Homeland Security Act (2002): It contained the Federal Information Security Management Act (FISMA) which aims to emphasise the relevance of information security tothe United States' economic and national security objectives.

II. State Government

Notice of Security Breach Act (2003): Businesses that handled sensitive customer data (such
[8] ICLG, supra note 7, at 06.
as names, credit card numbers, social security numbers, driver's licence numbers, medical records, or financial information) were required to publicly disclose any security or data breach that occurred within their organisation. This rule provides an incentive for businesses to invest a significant amount of their budget to build a secure infrastructure to avoid potential reputational harm.
California Assembly Bill 1950 (2004): The California State Legislature approved this law in
2004 and made it a necessity for businesses to maintain a decent degree of cyber security, aswell as to extend those security measures to their business partners in order to maintainan acceptable level of cyber security.

III. Proposed regulation

Other legislation that has been offered by the US Congress in recent years to expand on cyber security regulations include:

- The Consumer Data Security and Notification Act- It supplements the Gramm-Leach-Bliley Act by mandating financial institutions to report anydata or security breaches.
- Securely Protect Yourself Against Cyber Trespass (SPY ACT)- The US House of Representatives enacted the SPY ACT in 2005, but it died in the US Senate. It primarily targeted phishing and spyware frauds.
- The Cyber security Act, 2012- It suggested anti-cybercrime legislation with the goal of improving cyber security infrastructure and protecting it from cyberattacks, which businesses would be encouraged to adopt through incentives such as tax breaks.
- National Cyber security Action Plan (CNAP)- President Obama created the plan in 2016 with the goal of raising public awareness about the growing threat of cybercrime and informing people about how to improve and control digital security.

IV. Additional Government Efforts

The United States federal government has attempted to strengthen cyber security by committing greater money to research and cooperating with the private sector to establish acceptable standards and adopt crucial cyber laws. Aside from that, the government has launched various public awareness campaigns via social media to raise public knowledge of cybercrime concerns.

C. WHY IS USA CYBER SECURITY PROFICIENT?

The United States is widely considered to be proficient in cyber security for several reasons:

Robust legal framework: The country has a strong legal framework in place to address cybercrime, including laws and regulations that provide for criminal prosecution and civil remedies for cyber-attacks.
Advanced technology: The US has access to some of the most advanced technology in the world, which allows organizations to implement robust cyber security measures such as firewalls, encryption, and threat intelligence.
Skilled workforce: The US has a large and highly skilled workforce in the field of cyber security, including both government employees and private sector professionals, who work to prevent and respond to cyber threats.
Investment in cyber security: The US government and private organizations invest heavily in improving their cyber security infrastructure, including research and development of innovative technologies, training and certification programs, and incident response capabilities.
Partnership between government and private sector: The US government and private organizations work closely together to address cyber security threats, sharing information andbest practices to ensure a comprehensive approach to security.

CYBER SECURITY IN TAJIKISTAN

Cyber security in Tajikistan is an emerging issue as the country increasingly relies on technology and the internet. While the government has taken steps to address cyber security, the country still faces challenges such as a lack of technical expertise, limited resources, and an inadequate legal framework. Cybercriminals often target Tajikistan because of its weak security infrastructure, and the country experiences a considerable number of cyber-attacks, particularly in the financial and telecommunications sectors. The government and private organizations are working to enhance their cyber security measures. However, much work still needs to be done to ensure the safety and security of Tajikistan's critical information infrastructure. Tajikistan ranks 145th in NCSI (National Cyber Security Index) and 138th in GCI (Global Cyber security Index).[9]
In Tajikistan, financial cybercrime is one of the most significant and impacting types of cybercrime. This can include activities such as online banking fraud, credit card frauds, and theft of personal financial information. Cybercriminals often target individuals and businessesin Tajikistan, taking advantage of the country's weak cyber security infrastructure. As a result, financial losses from cybercrime can have a significant impact on the economy and

[9] Statista, supra note 3, at 04.

citizens of Tajikistan. Additionally, the country also experiences cyber-attacks in its telecommunications sector, which can disrupt communications and compromise sensitive information.

A. IMPORTANT DIRECTIVES AND LEGISLATIONS OF TAJIKISTAN RELATINGTO CYBER SECURITY

The fundamental provision of Tajik legislation that provides for the right to personal data protection is contained in Article 23 of the Republic of Tajikistan's Constitution of 6 November 1994, which states that the collection, storage, use, and dissemination of an individual's personal data without their consent is prohibited.
In addition to the Law on Personal Data, the following laws govern data protection: Law No. 37 of 17 May 2004 on Certain Types of Activities ('the Law on Licensing'); Law No. 55 of 10 May 2002 on Information (only available in Tajik here) ('the Law on Information');
Criminal Code of the Republic of Tajikistan No. 574 of 21 May 1998 (only available in Tajik here) ('the Criminal Code'), which provides for criminal liability for various offences related to information stored on computer systems;
Code on Administrative Offences of the Republic of Tajikistan No. 455 of 31 December 2008 ('the Code on Administrative Offences'), which provides for administrative liabilities for failure to take measures ensuring (this publication is not available in electronic form).

B. WHY TAJIKISTAN IS WEAK IN CYBER SECURITY?

Tajikistan's cyber security is considered to be weak for several reasons:

- Lack of technical expertise: Tajikistan has a shortage of trained cyber security professionals, which makes it difficult to prevent and respond to cyberattacks.
- Inadequate legal framework: The country has limited laws and regulationsin place to address cybercrime, making it difficult to prosecute cyber criminals and protect citizens from cyber-attacks.
- Limited resources: Tajikistan has limited resources, both financial andtechnical,to invest in improving its cyber security infrastructure.
- Vulnerability to cyber-attacks: The country's weak cyber security infrastructure makes it a prime target for cyber criminals, who can easily exploitvulnerabilities to carry out cyber-attacks.
- Disruptions in the telecommunications sector: Cyber-attacks on the telecommunications sector can disrupt communications and compromise sensitive information, leading to significant consequences for both businesses and individuals.

Overall, these factors contribute to the weakness of Tajikistan's cyber security and make it vulnerable to a wide range of cyber-attacks, which can have a significant impact on the country's economy and citizens.

STANDPOINT OF INDIA IN CYBER SECURITY

India's ever-expanding digital infrastructure has increased the necessity for new, updated, and enhanced regulatory regulations to strengthen cyber security. Weekly, numerous cyber security incidents have occurred, worrying businesses, organisations, and individuals across India.
According to the IBM Security Data Breach Report 2022,[10] the average data breach cost in India for fiscal year 2022 has hit a record high of 17.5 crores (175 million) rupees, or $2.2 million, a 6.6% increase from 2021 and a shocking 25% increase from the average cost of 14 crores in 2020.
The Indian government has begun to review how it governs cyber security and cybercrime in reaction to the quickly evolving digital transformation, outmoded cyber security regulations, and a lack of clear, comprehensive data protection rules.

A. TOPMOST CYBER ATTACKS IN INDIA

- Phishing and Social Engineering
- Malware
- Spear Phishing
- Denial of Service
- Out of Date Software Ransomware

B. IMPORTANT CYBER SECURITY LAWS AND REGULATIONS IN INDIA

The following are the current cyber security laws in use in India:[11]

I. The Information Technology Act, 2000

The Information Technology Act of 2000 was India's first major cyber security law. The

[10] IBM, https://www.ibm.com/in-en/reports/data-breach (Last visited February 03, 2023; 02:22 AM)

[11] ICLG, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india (Last Visited February 03, 2023 03:30 AM).

Indian Computer Emergency Response Team (CERT-In) administers the IT Act of 2000, which was passed by the Indian Parliament to regulate Indian cyber security legislation,institute data protection rules, and govern cybercrime. It also safeguards, among other things, e-governance, e-banking, e-commerce, and the private sector.

While India lacks a unified cyber security law, it promotes cyber security standards through the IT Act and a variety of sector-specific rules. It also establishes a legal foundation for India's essential information infrastructure.

II. The Information Technology Act (Amendment) Act, 2008.

The Information Technology (Amendment) Act, 2008 was passed in October 2008 and went into force the following year as a significant update to the Information Technology Act of 2000. These revisions aided in the improvement of the original bill, which had previously failed to pave the path for future IT-related development. It was lauded as a ground breaking and long-awaited move toward a more robust cyber security framework in India. The IT Actof 2008 includes updated and revised phrases for current use, broadening the meaning of cybercrime and electronic signature validation. It also strongly encourages businesses to improve their data security processes and holds them accountable for data breaches.

III. Information Technology Rules, 2011

Another major piece of cyber security law under the IT Act is the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules).

IV. Indian SPDI Rules for Reasonable Security Practices, 2011.

The Indian SPDI Rules, 2011, identify the IS/ISO/IEC 27001 norms as international standards. As a result, Indian enterprises are not required — but strongly encouraged — to follow these standards, which can assist in meeting the "reasonable security procedures" under Indian authority. Individuals may also have the right to have their information corrected, and the rules may set restrictions on disclosure, data transfer, and security measures. They only apply to corporations, although they are not liable for the veracity of sensitive personal data (SPD).

V. National Cyber security Policy, 2013

The National Cyber Security Policy 2013 was released in 2013 by the Department of Electronics and Information Technology (DeitY) as a security framework for public and commercial businesses to better protect themselves against cyber threats.

The National Cyber Security Policy's purpose is to build and develop more dynamic policies to secure India's cyber ecosystem. Through skill development and training, the initiative seeks to establish a workforce of over 500,000 expert IT professionals over the next five years.

4. CONCLUSION AND RECOMMENDATIONS

The need for cyber security is critical in today's digital age where sensitive information and valuable assets are stored and exchanged online. The increasing reliance on technology andthe internet has made it imperative to protect against cyber threats such as hacking, data breaches, and malicious software. Cyber security helps to ensure the confidentiality, integrity, and availability of information, prevent financial losses, protect personal and sensitive information, and maintain trust and credibility in the online world. In short, cyber security is essential for individuals, organizations, and nations to secure their digital assets and preserve the safety and security of their online activities. In conclusion, the United States is widely considered to have one of the strongest cyber security infrastructures in the world. The country has a robust legal framework, advanced technology, and a highly skilled workforce to prevent and respond to cyber-attacks. The US government and private sector organizationsare continuously working to enhance their cyber security measures to stay ahead of evolving threats. Despite these efforts, no system is completely infallible, and cyber security remains a significant challenge that requires ongoing attention and resources. Moreover, it is important for Tajikistan to prioritize and invest in strengthening its cyber security capabilities in order to better protect its digital assets and ensure the safety and security of its online activities. By doing so, the country can enhance its cyber resilience and minimize the impact of potential cyber-attacks. As far as India is concerned, it has been actively working to build its cyber security posture in recent years. The Indian government has established a national cyber security strategy and a dedicated cyber security coordination centre, which are aimed at improving the country's overall cyber security posture. In addition, the Indian government has taken steps to educate the public and private sectors about cyber security risks and has implemented various cyber security laws and regulations to protect citizens and organizations from cyber threats. However, there is still room for improvement in terms of investment in technology and infrastructure, and international collaboration to tackle cyber threats.

AUTHOR'S OPINION

While ICTs offer unparalleled opportunities to advance social and economic growth, their misuse and weaknesses bring new and serious challenges. To address the issues provided by the global nature of cybercrime, national cyber security strategies must include mechanismsfor identifying, managing, and responding to cyber threats. This is especially difficult for Least Developing

Countries like Tajikistan, which lack a suitable legal and regulatory framework, as well as inadequate human capacity/expertise and financial resources. This canbe curbed by evaluating the situation by gathering information and assessing the current situation in each beneficiary country. Developing guidelines on cyber security legislation, policy, and technologies to aid in the establishment of an electronic security system.

Distribution of equipment and solutions and delivery of necessary equipment and software. Increasing capacity of training materials and curriculum on national, regional, and worldwide cyber security legislation and regulation, as well as technological aspects, shall be created.

Furthermore, for developing nations like India, the techno-diplomacy needs to get stronger, linking cyber security with cooperative federalism shall be done for recognition of cybercrime and effective implementation of directives and rules for the same, global understanding and commonality of morality and ethics shall be blended with cyber security, filling infrastructural gaps and cyber awareness campaigns are also useful to promote cyber security in developing nations.