Cybercrime and the efficacy of Cyber Laws in the 21st century: Review of the Global situation

Sairah Ghuman[1]

[1] *Sairah Ghuman, Research Trainee, 360 College Review Research, Methodology Course – I, Chandigarh, India*

Abstract

The international scenario pertaining to the increasing use of the internet as a vital medium of communication is fraught with dangers of a new and unknown variety that are manifested in myriad opportunities for taking unfair advantage of ignorant and less aware persons across the globe. The terminology for these manifestations is cyber crime as it occurs in the lesser known and relatively latent world. Cyber crime has taken on virulent forms in varying situations and has necessitated the emergence of an entirely fresh lexicon of crime perpetuation.

The fact that the cyber world comprises the entire media and communications networking of the global finances, administration and governance makes the processes of survival and sustenance of humankind all the more intricate and intertwined. The cyber criminals became aware of these crucial linkages and evolved their own miasma of taking advantage at various stages.

It is an interesting fact that along with the creation of cyber crimes there has been an equally heated race to enact laws that deal with these crimes and can prove effectively deterrent for them. The magnitude and novelty of cyber crimes is matched by the creation of laws to combat them and stem their perpetuation. Another interesting fact is that the talents of the criminals and the minds of those who work towards enacting laws law to uphold the justice system are well matched. The current paper is a review of the global scenario as regards the emergence of various forms of cyber crime and the methods adopted to curb them especially in terms of legal redressal and enactment of specialised laws,

Key words: Cyber crime, cyber laws, internet, media, communication, laws, justice, administration, governance.

Introduction

Cybersecurity dangers are both singular and worldwide, which poses serious challenges to international law, which is often grounded in ideas of territoriality and state sovereignty. Examining regulatory tactics, challenges, and opportunities for reform within existing frameworks, this essay delves into the connection between international law and cybersecurity. In order to address cybersecurity concerns, the study highlights the importance of international legislation.

Governments, corporations, and individuals alike have made cybersecurity a top priority in the digital era due to the wide range of cyber dangers, including cyberterrorism, data breaches, and cyberattacks. Cybercrimes often endanger national security, personal privacy, and the stability of financial systems. According to the World Economic Forum (2021), cyberattacks are becoming more

common and more severe, which poses a global danger to national security as well as the functioning of critical infrastructure, healthcare systems, and financial networks.

Since conventional international law was primarily developed to address issues of State sovereignty and physical borders, it has proven inadequate to address the complexities of cybersecurity. Because cyber dangers are global in scope, attempting to regulate them through legal systems is fraught with difficulty in terms of both enforcement and jurisdiction. Unfortunately, victims of cybercrime often find themselves unable to seek justice across borders due to a lack of adequate legal frameworks and resources (Kshetri, 2020). Offenders can evade prosecution due to the anonymity and global nature of the internet.

To address cybersecurity issues, however, international law remains a crucial foundation. For instance, the United Nations' resolutions on cybercrime and cybersecurity (United Nations, 2013) and the Budapest Convention on Cybercrime (Council of Europe, 2001) are examples of international agreements, conventions, and initiatives that attempt to provide answers for establishing global cybersecurity standards and cross-border cooperation. There is skepticism about the ability of international law to handle the complex and ever-changing cybersecurity dangers because of the fragmented character of these legal frameworks and their insufficient enforcement mechanisms.
The growing worries about cybersecurity have led to the emergence of several international legal frameworks.

Need for and the emergence of international legislations targeting cyber crime
According to the Council of Europe (2001), the initial significant step was the organization of the Budapest Convention on Cybercrime. The need for consistent cybercrime laws among the member states was stressed in the convention's final declaration, which also called for increased international cooperation in the fight against cybercrime. The first-ever global pact to criminalize acts involving information technology (IT), data, and content is the Convention on Cybercrime. Nations such as Russia and China have voiced concerns about national sovereignty and control over cyberspace, which has hindered the global acceptance of the Budapest Convention.

Along with the Budapest Convention, the United Nations also passed resolutions and made other attempts to address cybersecurity. The United Nations Group of Governmental Experts (GGE) on Cybersecurity has been working since 2004 to establish cyber behavior norms, with an emphasis on the importance of international cooperation and respect for sovereignty (UNIDIR, 2015). However, their efforts have been obstructed by vested interests. The "Recommendation on the Ethics of Artificial Intelligence," the first ever worldwide guideline on AI ethics, was published in November 2021 by UNESCO. All 194 member states of UNESCO are bound by it. The fundamental principle underlying the suggestion is the protection of human rights and dignity. Developing fundamental principles like justice and transparency while bearing in mind the importance of human oversight of AI systems forms its foundation.

What makes the UNESCO recommendation especially relevant are the "Policy Action Areas," which allow policymakers to implement basic principles and values in areas such as data governance, gender, ecosystems, education, research, health, and social wellbeing, among others. "Human rights and human dignity," which includes respecting, protecting, and promoting human rights, basic freedoms, and human dignity; "Living in peaceful, just, and interconnected" societies; and "Ensuring diversity and inclusiveness" in addition to "Environment and ecosystem flourishing" are the four core values that set the foundation for AI systems that work for the good of people, societies, and the environment.

These rules were needed because it was getting too hard to keep up with the growing amount and variety of hacking.

Challenges in Regulating Cybersecurity under Traditional International Law

When it came to cyberspace, traditional international law, which has been built for hundreds of years on the ideas of state sovereignty and territoriality, was severely limited. Cyberspace has no borders and is not controlled by a single group. It's hard to decide who is responsible for cybercrimes and attacks because there aren't clear geographical lines. Also, because the internet lets people remain anonymous, it is harder to find and punish criminals, especially when they work in more than one place (Kshetri, 2020).

In reality, legal systems are constantly battling to keep up with new technologies like artificial intelligence, blockchain, and quantum computing, which all create new cybersecurity risks (Zittrain, 2017). Cyber risks are always changing, so international law needs to be more adaptable and creative in order to make rules that are fair and are strictly enforced.

Research Questions

To better appreciate the difficulties and regulatory strategies in the context of cybersecurity and international law, a number of important issues must be addressed. The following research questions will direct the examination of how international law may offer a thorough framework for cybersecurity governance and effectively address the changing nature of cyber threats:

1. How well do the current international law frameworks deal with cybersecurity issues?
2. What problems do you see with using old-fashioned international law to deal with current cyber threats?
3. What changes need to be made to international law to protect both state and non-state players from cybersecurity risks?
4. How can international groups oversee and encourage countries to use cybersecurity?
5. In the face of hacking, how can international law protect national security while also protecting people's rights to privacy and freedom?

Organizations like the United Nations (UN), the European Union (EU), and the International Telecommunication Union (ITU) play a big role in making and promoting rules and guidelines for hacking. EU's Cybersecurity Act (European Union, 2019) and UN's Group of Governmental Experts (GGE) (UNIDIR, 2015) are two efforts to improve cooperation between countries in cybersecurity. While the EU's General Data Protection Regulation (GDPR) (European Union, 2016) tries to protect people's privacy online, states may also need to access encrypted data for national security reasons. Security measures like data retention rules, government surveillance, and sharing information between businesses and governments raise ethical and legal issues.

Dealing with cybercrime that crosses borders, setting rules for how states should act responsibly in cyberspace, and encouraging less developed countries to build up their cybersecurity infrastructures can all be studied using these study questions. Additionally, they look into how useful it is to create global rules for protection. Scholarly research on the subject is needed to fully understand the depth of the ongoing power struggle between people who abuse others online and people who watch them.

Literature Review

International Legal Instruments to ensure Cybersecurity

International legal tools are essential for controlling cybersecurity and combating cybercrime. According to studies by Kshetri (2020) and Weichert (2018), efficacy is limited by the lack of comprehensive enforcement mechanisms and the global adoption of robust legislative measures.

Challenges in Regulating Cybersecurity under Traditional International Law

The limitations of conventional international law in regulating cybersecurity are the subject of a substantial body of study (Zittrain, 2017). Hacking, data breaches, and cyberattacks are examples of cyberthreats that frequently take place in a decentralized, international setting, making enforcement and jurisdictional concerns more difficult. Cyberattacks may come from one nation but target organizations in another, leading to a jurisdictional dispute and complicating prosecution (Kshetri, 2020).

There are proposals for a more comprehensive approach to international cyber governance because the current international legal frameworks are not equipped to handle such novel kinds of conflict (Tikk et al., 2018). Additionally, anonymity makes it more difficult to prosecute cybercriminals, and current legal frameworks are ill-suited to deal with this issue. Cybercrime can be committed from any location, and encryption and other methods can be used to hide the identity of the perpetrator (Weichert, 2018).

Cybersecurity and State Sovereignty

The issue of state authority in cyberspace is still being debated in international law. Some countries can still run and control their own digital infrastructures without help from other countries (Zittrain, 2017). This is especially clear in countries like China and Russia, which support cyber sovereignty, the idea that each country should control its own cyberspace and internet traffic within its limits. For example, China's Great Firewall tries to keep an eye on how people use the internet and restrict access to foreign websites so that information seen as harmful to the government doesn't get around (Zittrain, 2017). People who want a more open and cooperative strategy, on the other hand, say that cyberthreats like cybercrime, cyberterrorism, and cyberespionage need international cooperation and cross-border rules to be stopped. Trying to find a balance between working together and protecting national interests has led to different national goals and different legal approaches to managing the internet (Greenleaf, 2018).

Human Rights and Cybersecurity

By giving people more control over their personal data, including the ability to access, amend, and remove it, the GDPR (European Union, 2016) aims to allay these worries. Global adoption of comparable privacy protections is still difficult, though. Cybersecurity laws that safeguard national security are absolutely necessary. The delicate balance between security and privacy is shown by state surveillance operations, such as those that Edward Snowden revealed in 2013 (Greenleaf, 2018). Governments may use national security concerns as an excuse to impose speech restrictions online, but this can result in censorship and the repression of dissent. Therefore, maintaining cybersecurity while defending freedom of speech is a difficult for international law.

International law is still a crucial framework for handling cybersecurity issues in spite of the difficulties. The Budapest Convention on Cybercrime (Council of Europe, 2001) and the United Nations' resolutions on cybercrime and cybersecurity (United Nations, 2013) are two examples of international agreements, conventions, and initiatives that aim to offer solutions for cross-border cooperation and the creation of global cybersecurity norms.

Conceptual Background

The fast development of technology, the digitization of worldwide sectors, and the increasing reliance on interconnected networks have all contributed to a dramatic shift in cybersecurity risks during the last several decades. While the "Morris Worm" experiment by Robert Tappan Morris in 1988 was mostly harmless, it caused widespread system outage and affected more than 6,000 machines online (Spafford, 1989). This incident was one of the first to bring cybercrime to the attention of the world's public. Attacks like ransomware, phishing, and Distributed Denial of Service (DDoS) became routine

thereafter, and cybercrime became a profitable enterprise for criminal organizations. Cyberspace has become more geopolitically and strategically important due to state-sponsored cyberattacks like the 2007 Estonian cyberattacks (Zetter, 2014) and the 2017 NotPetya attack in Ukraine (Kaspersky, 2017). As a result, there is a pressing need for international legal frameworks to deal with these types of cyber threats.

Rapidity of cybersecurity in becoming a global concern

A data breach occurred in 2013 at the United States Office of Personnel Management (OPM), exposing the identities of more than 21 million government employees. The intrusion, which was linked to Chinese hackers with ties to the state, caused concern on the susceptibility of government systems to hacking and the possible ramifications of cyber espionage (Friedman, 2015). In order to tackle cybercrime and other harmful actions, a worldwide strategy for cybersecurity governance is required, given the growing number of cyber incidents that across international borders. When it comes to shaping cybersecurity governance, a number of foreign players are pivotal. Among these are non-governmental organizations (NGOs), corporate companies, and governments from throughout the world.

When looking at cybersecurity legislative frameworks around the world, the General Data Protection Regulation (GDPR) enacted by the European Union stands out as one of the most all-encompassing laws. It affects how member states regulate cybersecurity. Next, there's the US strategy towards cybersecurity, which encompasses both federal and state-level legislation, as well as its impact on cybersecurity standards worldwide. A state-centric paradigm of cybersecurity regulation is exemplified by China's Great Firewall and its approach to cyber sovereignty. Similarly, international collaboration on cyber matters is jeopardized by Russia's attitude on cybersecurity law and its opposition to specific international legal frameworks. An increasing amount of research into the difficulties of harmonising international law across different political and legal systems, as well as regional variations in cybersecurity regulation, is required.

Discussion and analysis of some case findings

An analysis of specific incidents of cybercrime and state-sponsored cyberattacks brings up the following cardinal examples which have been studied chronologically:

1. **Stuxnet (2010)**: Many consider this malware assault on Iran's nuclear program to be the first instance of serious cyberwarfare. When it comes to state-sponsored cyber assaults that involve espionage or sabotage, the current international legal frameworks have their limits brought to light for the first time in the Stuxnet case.
2. **NotPetya (2017)**: After what seemed like a ransomware strike, the NotPetya malware turned out to be state-sponsored cyberwarfare. An examination of the NotPetya case shows how international law can deal with the increasing danger of cyberwarfare and the difficulties in linking cyberattacks to particular state actors. Findings from these research shed light on how international law concepts might be applied to actual cyber occurrences.

When it comes to cyberspace, questions of whether attacks could be considered acts of war and the applicability of international legal norms like jus ad bellum and jus in bello remain unanswered (Tikk et al., 2018). National security and international collaboration are both jeopardized by the absence of a well-defined legal framework to counteract state-sponsored cyberattacks.

Effectiveness of current cybersecurity regulations and policies in the United States

When it comes to protecting America's digital landscape, cybersecurity policies and regulations are paramount. The government has established a thorough framework to safeguard vital infrastructure, private information, and national security in response to the growing number and complexity of

cyber threats. These rules and policies are constantly being reviewed and examined to see how well they work.

In 2014, Congress passed the Cybersecurity Enhancement Act, which bolstered cybersecurity R&D, set standards for best practices, and improved collaboration between the public and commercial sectors. The Act highlighted the significance of working together and sharing knowledge to effectively reduce cyber risks.

A watershed moment in the federal government's attempt to unify cybersecurity was the 2018 creation of the Cybersecurity and Infrastructure Security Agency (CISA). When it comes to distributing threat intelligence, supporting critical infrastructure institutions, and coordinating cybersecurity measures, CISA is crucial. Despite the agency's best efforts, obstacles including limited resources and ever-changing threat environments continue to undermine the nation's cyber defenses.

The study highlights the significance of attorneys keeping up with the ever-changing cybersecurity legislation and its effects on domestic and international legal practices. Cyber law attorneys should research and study the intricate relationship between data protection, privacy, national security, and cybersecurity; they should also think about how new legal challenges might be handled within the context of international law.

In order to make the country's cyberspace more resilient, the US government, businesses, and universities have worked together to create a thorough cybersecurity architecture. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a cornerstone of the United States' cybersecurity policy. For better cybersecurity management, this framework lays out best practices and standards for enterprises to follow. It aims to improve cybersecurity resilience by focusing on risk management, constant monitoring, and incident response. Protecting critical infrastructure and investigating cybercrimes are important responsibilities of several government organizations, including the FBI and the Department of Homeland Security (DHS). Since its inception in 2009, the United States Cyber Command has been tasked with protecting the country from major cyber threats and guaranteeing the cyber capabilities of the military.

Protecting vital infrastructure and sensitive information from cyber dangers such as hacking, malware, and data breaches is an important responsibility of cybersecurity laws and regulations in the US. They lay down the groundwork for how businesses should safeguard their computer systems and networks. Victims of cybercrime now have legal options thanks to these laws, which also help to hold individuals and businesses responsible for cyber crimes.

The National Institute of Standards and Technology (NIST) made the Cybersecurity Framework to help businesses best handle and improve their cybersecurity risk management. A structure includes rules, standards, and the best ways to keep your information safe. It was released to the public in April 2018 and is called NIST Cybersecurity Framework 1.1.

Current legal redressal for cyber crime

For better monitoring and improvement of cybersecurity risk management processes, organizations can turn to the NIST Cybersecurity Framework (CSF), an extensive and adaptable set of standards and best practices. The National Institute of Standards and Technology (NIST) developed the framework, which offers a versatile method that firms in many sectors can employ to shore up their cybersecurity. There are primarily three parts to the framework: the Core, the Implementation Tiers, and the Framework Profile.

Core Functions:

There are five main components to the NIST CSF, and they all play an important role in any good cybersecurity program:

[a] Identify: Establishing an organizational environment, managing assets, and devising risk management strategies are all part of this function's understanding and management of cybersecurity threats.

[b] Protect: Critical infrastructure services must be reliably delivered, and the Protect function is devoted to doing just that. Data protection procedures, training and awareness initiatives, and access controls are all part of this.

[c] Detect: Constant vigilance and prompt detection of cybersecurity incidents are key features of Detect.

[d] Respond: Organizations should be prepared to respond effectively to cybersecurity incidents. In the event of an incident, the Respond function details what to do immediately to lessen its impact.

[e] Recover: In the event of a cybersecurity incident, the Recover function is responsible for creating and executing plans to recover any compromised services or systems. Efforts to recover must be prioritized, and lessons learnt must be incorporated for future improvements.

[ii] HIPAA (Health Insurance Portability and Accountability Act):
HIPAA establishes rules for keeping people's private health information safe. To protect the privacy, security, and easy access of patients' medical data, HIPAA requires all "covered entities," like insurance companies and doctor's offices, to follow specific rules and instructions.

The Health Insurance Portability and Accountability Act (HIPAA) is a major piece of U.S. legislation that enacted in 1996 to safeguard the privacy of patients' medical information. For keeping electronic protected health information (ePHI) safe, the HIPAA Security Rule provides a detailed framework. The availability, integrity, and privacy of electronic protected health information (ePHI) must be protected by healthcare providers, health plans, healthcare clearinghouses, and other covered groups through administrative, physical, and technical measures. Breaking HIPAA rules could lead to serious problems, like fines and court action. (6).

[iii] Gramm-Leach-Bliley Act (GLBA):
A law called GLBA says that financial companies must keep their customers' private financial information safe. It calls for making and following information security plans and includes steps to protect the safety and accuracy of nonpublic personal data (U.S. Department of Health & Human Services, 2003).

A seminal piece of US legislation, the Gramm-Leach-Bliley Act (GLBA) or the Financial Modernization Act of 1999 sought to strengthen financial sector information security and consumer privacy. In addition to removing some Glass-Steagall Act regulations, the Glass-Little John A. Pepper Act (GLBA) imposed additional safeguards for customers' nonpublic personal information (NPI) on banking, credit union, and securities companies. The U.S. Congress passed GLBA in 1999 with the express purpose of requiring financial institutions to take reasonable precautions to secure and protect their customers' personal information (U.S. Congress, 1999).

There are serious fines and regulatory measures that can happen if you don't follow GLBA. Financial institutions' use and disclosure of customers' personal financial information is something that the Act seeks to make more transparent and to give consumers more agency over [9].

[iv] Federal Information Security Modernization Act (FISMA)
The United States passed a landmark cybersecurity law, the Federal Information Security Modernization Act (FISMA), in 2002. It requires all government agencies to protect their data and information systems by implementing security procedures. Federal agencies' data collection, storage, and use must be protected from unauthorized access, use, or disclosure in order to fulfill its mission [10].

In order to comply with FISMA, agencies must set up thorough information security systems that include things like incident response plans, testing, regular risk assessments, and continuous control monitoring. The OMB and DHS must also receive reports from agencies regarding their legal compliance (FISMA, 2014).

[v] Cybersecurity Information Sharing Act (CISA)
The U.S. Congress passed the Cybersecurity Information Sharing Act (CISA) in 2015, which encourages private businesses to provide the government with information about cyberthreats and offers liability protections for doing so. In order to protect vital infrastructure and national security from cyberattacks, its main objective is to improve the sharing of cyber threat intelligence between the public and commercial sectors. The Department of Homeland Security (DHS) and other federal agencies can exchange cyber threat data with private enterprises thanks to CISA, which also facilitates information sharing between the government and private organizations.

CISA also provides for the creation of volunteer Information Sharing and Analysis Organizations (ISAOs). Advocates for civil rights and privacy contend that CISA may not provide adequate protections for personal data and may be used for government monitoring (Enterprise Engineering Solutions, 2023).

[v] California Consumer Privacy Act (CCPA):
Despite its primary emphasis on privacy, the CCPA mandates that businesses implement suitable security measures to safeguard consumers' personal information. The California Consumer Privacy Act (CCPA) is a landmark US privacy law that grants greater agency to individuals residing in the Golden State with respect to the personal information that businesses collect and store. Customers have the right to know what personal data organizations are collecting, selling, or revealing according to the CCPA, which was passed in 2018 and went into effect on January 1, 2020.

The CCPA has significant implications for businesses in California and the US privacy landscape at large, and it influences conversations about potential federal privacy measures (Enterprise Engineering Solutions, 2023).

[vi] DOD Cybersecurity Maturity Model Certification (CMMC):
To better safeguard Controlled Unclassified Information (CUI) inside the defense industrial base, the CMMC was introduced by the Department of Defense (DOD). For contracts with the Department of Defense (DOD), vendors and contractors must adhere to stringent cybersecurity requirements. A thorough framework developed to improve cybersecurity procedures inside the defense industrial base (DIB), the Cybersecurity Maturity Model Certification (CMMC) is administered by the United States Department of Defense (DOD). Some of the obstacles that DIB firms may face include the expense of installation and the constant requirement for updates to keep up with the ever-changing cybersecurity threat landscape (California Legislative Information, 2018).

Effectiveness of current cybersecurity regulations and policies in the United States

Protecting America's digital infrastructure relies heavily on cybersecurity rules and practices. To safeguard vital infrastructure, private information, and the nation's security, the government has set up a thorough framework in response to the growing number and complexity of cyber threats. There is a continuous effort to assess how well these policies and laws are working.

The Cybersecurity Enhancement Act of 2014 was a landmark piece of legislation that strengthened cybersecurity-related R&D, codified industry best practices, and improved public-private partnerships. In order to successfully reduce cyber risks, the Act stressed the significance of sharing information and working together.

In 2018, the United States government took a giant step toward coordinating its cybersecurity initiatives with the creation of the Cybersecurity and Infrastructure Security Agency (CISA). In order to coordinate cybersecurity initiatives, support critical infrastructure institutions, and disseminate threat intelligence, CISA is an essential component. Challenges such as resource restrictions and developing threat landscapes persist in the agency's attempts to enhance the nation's resilience against cyber threats.

Recent cyber threats

Cybercriminals have also targeted the banking industry, stealing customers' personal information and credit card details. An example of this is the data breach that happened at JPMorgan Chase in 2014. Discussions about the need for more rules and heightened scrutiny of the banking industry's cybersecurity policies ensued after the incident. Consequently, in order to strengthen the safety of payment card transactions, financial institutions have been compelled to adhere to regulatory frameworks like the PCI DSS (U.S. Department of Defense, 2020).

The UK's National Health Service (NHS) was one of many healthcare organizations hit hard by the 2017 WannaCry ransomware assault. Although the United States was not the intended target, the incident did highlight certain weaknesses in healthcare systems. To counter this, the federal government and healthcare institutions in the United States have stepped up their efforts to adhere to and even improve upon existing cybersecurity standards, such as HIPAA, in order to safeguard patient data and increase overall cybersecurity resilience (National Institute of Standards and Technology, 2018).

A prime example of the difficulties in protecting against complex cyberattacks is the SolarWinds supply chain breach that was uncovered in the latter half of 2020. By taking advantage of a reliable software vendor, the incident affected numerous private and public entities in the United States. This incident emphasizes the significance of constant monitoring and the exchange of threat intelligence, and the necessity for all-encompassing cybersecurity strategies that deal with threats throughout the supply chain [16].

The steadily rising number of data breaches since 2015 is indicative of the growing sophistication and awareness of cyber-attacks. The most number of reported data intrusions occurred in the year 2021, which stands out in the statistics. All the more need to beef up cybersecurity procedures to protect sensitive information from the widening array of threats.

Reports of fraud show both steady growth and periodic dips, according to a trend analysis of the "Fraud" dataset that spans 2010–2021. With an increase in future years, the number of registered occurrences of fraud reached 820,072 in 2010. The statistics shows that the number of reported fraud cases increased dramatically beginning in 2014 and peaking at 2,789,161 cases in 2021.

Cybercriminals have also targeted the banking industry, stealing customers' personal information and credit card details. An example of this is the data breach that happened at JPMorgan Chase in 2014. Discussions about the need for more rules and heightened scrutiny of the banking industry's cybersecurity policies ensued after the incident. Consequently, in order to strengthen the safety of payment card transactions, financial institutions have been compelled to adhere to regulatory frameworks like the PCI DSS [14].

The UK's National Health Service (NHS) was one of many healthcare organizations hit hard by the 2017 WannaCry ransomware assault. Although the United States was not the intended target, the incident did highlight certain weaknesses in healthcare systems. To counter this, the federal government and healthcare institutions in the United States have stepped up their efforts to adhere to and even improve upon existing cybersecurity standards, such as HIPAA, in order to safeguard patient data and increase overall cybersecurity resilience [15].

A prime example of the difficulties in protecting against complex cyberattacks is the SolarWinds supply chain breach that was uncovered in the latter half of 2020. By taking advantage of a reliable software vendor, the incident affected numerous private and public entities in the United States. This incident emphasizes the significance of constant monitoring and the exchange of threat intelligence, and the necessity for all-encompassing cybersecurity strategies that deal with threats throughout the supply chain [16].

The steadily rising number of data breaches since 2015 is indicative of the growing sophistication and awareness of cyber-attacks. The most number of reported data intrusions occurred in the year 2021, which stands out in the statistics. All the more need to beef up cybersecurity procedures to protect sensitive information from the widening array of threats.

You may learn a lot about potential changes in cyber-attack strategies by looking at the variations from year to year. Data breaches may occur more or less frequently in different years, which could indicate that cybercriminals' tactics or target preferences have changed. Organizations and cybersecurity experts should thoroughly analyze these trends in order to appropriately modify their security protocols.

Reports of fraud show both steady growth and periodic dips, according to a trend analysis of the "Fraud" dataset that spans 2010–2021. With an increase in future years, the number of registered occurrences of fraud reached 820,072 in 2010. The statistics shows that the number of reported fraud cases increased dramatically beginning in 2014 and peaking at 2,789,161 cases in 2021.

There is an immediate requirement for clear international legal standards for the employment of cyber operations in conflict, since cyberwarfare is a characteristic of contemporary wars. While the Tallinn Manual 2.0 (Tikk et al., 2018) provides helpful information regarding the application of international humanitarian law to cyber operations, there has to be more effort to create legally enforceable treaties regarding cyber warfare. When disputes emerge as a result of cyberattacks, these treaties would serve as a guide.

Concerns for national security must be balanced in international law. According to the current findings, cybersecurity measures should take human rights and safety into account simultaneously. To make sure that national security measures don't violate civil liberties, governments should put in place rigorous checks and balances to stop the misuse of surveillance capabilities (Greenleaf, 2018).

Limitations of Existing Legal Frameworks

Some governments feel that data privacy legislation, such as the General Data Protection Regulation (GDPR), make it harder for them to fight cybercrime, particularly when the data is stored in a foreign country.One of the key problems with international legal frameworks for cybersecurity is the question of jurisdiction. Due to the worldwide character of cybercrime, neither national laws nor international legal cooperation structures are enough to deal with the full extent of cyber threats. In spite of initiatives by groups like Interpol and the United Nations, there are still holes in the system of global cybersecurity governance due to the absence of enforceable international agreements and standardized legal frameworks.

Conclusion and Summary of Key Findings

The meeting point of cyberspace and international law has been the primary emphasis of this study. In the ever-changing world of cyber dangers, it highlights the main obstacles and ways to regulate them. Addressing cybersecurity risks within the framework of international law is complicated, as the study emphasizes numerous critical results.

A universal cybersecurity treaty is one of the most important recommendations to strengthen the role of international law in regulating cyberspace, according to the study of current legal frameworks and the problems found. Better cross-border cooperation can help reduce cybersecurity jurisdictional conflicts. To overcome these shortcomings, existing frameworks should be enhanced through the establishment of stronger international legal channels for the exchange of information, the provision of mutual legal assistance, and the prohibition and punishment of cybercrime. With the help of international agencies such as Europol and Interpol, a worldwide cybercrime task force can promote collaboration among countries.

Cybersecurity and international law practitioners and legislators should take note of these study results. More inclusive and thorough cybersecurity frameworks, with an emphasis on cross-border collaboration and harmonization, should be a top priority for policymakers. In order to combat cybercrime and cyberwarfare, among other forms of cybercrime, they should strive to establish legally enforceable international treaties.

Reference

California Legislative Information. (2018). California Consumer Privacy Act (CCPA). Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Council of Europe. (2001). *Convention on Cybercrime* (CETS No. 185). https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Cybersecurity & Infrastructure Security Agency (CISA). (2020). SolarWinds Supply Chain Attack: "Active Exploitation of SolarWinds Software." Retrieved from https://www.cisa.gov/active-exploitation-SolarWinds-software

Department of Justice. (2015). JPMorgan Chase Data Breach: "Russian National Pleads Guilty to Largest Data Breach Conspiracy Ever Charged in the United States." Retrieved from https://www.justice.gov/opa/pr/russian-national-pleads-guilty-largest-data-breach-conspiracy- ever-charged-united-states

Enterprise Engineering Solutions. (2023). Cybersecurity Laws And Regulations In US (2023). Retrieved from https://www.eescorporation.com/cybersecurity-laws-and-regulations-in-us/

European Union. (2016). *General Data Protection Regulation (GDPR)*. https://gdpr.eu/

European Union. (2019). *Cybersecurity Act*. https://europa.eu/rapid/press-release_MEMO-19-2120_en.htm

Federal Information Security Modernization Act of 2014 (FISMA 2014) retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

Friedman, U. (2015). The OPM Hack and the Dangers of Cyber Espionage. *The Atlantic*. https://www.theatlantic.com/

Greenleaf, G. (2018). *Global data privacy laws 2018: The second year of the GDPR*. *International Data Privacy Law*, 8(4), 256-274. https://doi.org/10.1093/idpl/ipy019

Jamshed, J., Naeem, S., & Ahmad, K. (2020). Analysis of Criminal Law Literature A Bibliometric Study from2010-2019. *Library Philosophy & Practice*.

Jamshed, J., Jamshaid, M. K., & Saleemi, I. (2021). Law library usage for legal information seeking among the lawstudents in public sector universities: an empirical study. *Library Philosophy and Practice (e-Journal)*.

Kaspersky. (2017). *NotPetya: The Global Cyberattack*. https://www.kaspersky.com/

Kshetri, N. (2020). *Cybersecurity and international law: An emerging area of research*. *Journal of Cybersecurityand Digital Forensics*, 8(2), 45-62. https://doi.org/10.1016/j.cybsec.2020.05.002

Langner, R. (2011). *Stuxnet: A Breakthrough?*. *The Langner Group*. https://www.langner.com/en/stuxnet.html

National Institute of Standards and Technology. (2018). National Institute of Standards and Technology (NIST) Cybersecurity Framework: "Framework for Improving Critical Infrastructure Cybersecurity." Retrieved from https://www.nist.gov/cyberframework

NATO. (2018). *Cyber Defence*. https://www.nato.int/cps/en/natolive/topics_82703.htm

NHS ransomware attack spreads worldwide Roger Collier 10.1503/cmaj.1095434

Privacy of Consumer Financial Information (Regulation S-P) retrieved from https://www.sec.gov/rules/2000/06/privacy-consumer-financial-information-regulationsp#:~:text=Under%20the%20Gramm%2DLeach%2DBliley,to%20the%20consumer%20and%20the

Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act retrieved through https://www.federalregister.gov/documents/2019/04/04/2019-06039/privacy-of-consumer-financial-information-rule-under-the-gramm-leach-bliley-act

Razi, Naseem, et al. "CHILD MARRIAGE IN PAKISTAN: A CRITICAL ANALYSIS IN THE LIGHT OFSOCIO-LEGAL AND RELIGIOUS CONTEXT." *PalArch's Journal of Archaeology of Egypt/Egyptology* 18.2(2021).

Spafford, E. H. (1989). *The Morris Worm: A Case Study in Computer Security*. *Communications of the ACM*, 32(6),70-79. https://doi.org/10.1145/67417.67419

Tikk, E., Kaska, K., & Lember, V. (2018). *The Tallinn Manual 2.0 on the International Law Applicable to CyberOperations*. Cambridge University Press. https://doi.org/10.1017/9781108567451

The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks Michael Lang https://dl.acm.org/doi/full/10.1145/3558006
U.S. Cyber Command (2024). (https://www.cybercom.mil/)

The Gramm-Leach-Bliley Act and Financial Integration retrieved from https://www.federalreservehistory.org/essays/gramm-leach-bliley-act

UNIDIR. (2015). *The United Nations Group of Governmental Experts (GGE) on Cybersecurity*. https://www.unidir.org/

United Nations. (2013). *General Assembly resolution 68/167 on creation of a global culture of cybersecurity andthe protection of critical information infrastructure*.
https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

U.S. Department of Defense. (2020). CMMC Frequently Asked Questions. Retrieved from https://www.acq.osd.mil/cmmc/faq.html

U.S. Department of Homeland Security (2024). (https://www.dhs.gov/)

U.S. Department of Health & Human Services. (2003). Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Retrieved from https://www.hhs.gov/sites/default/files/hipaa- simplification-201303.pdf

World Economic Forum. (2021). *The Global Risks Report 2021*. https://www.weforum.org/reports/the-globalrisks-report-2021

Weichert, K. (2018). *Cyber sovereignty and the governance of cyberspace*. *Journal of International Affairs*, 72(2), 111-128. https://jia.sipa.columbia.edu/

Zetter, K. (2014). *Inside the U.S. government's battle to stop the world's most sophisticated cyberattacks*. *Wired*.https://www.wired.com/

Zittrain, J. (2017). *The Future of Cybersecurity and International Law*. *Harvard Law Review*, 130(4), 900-938.https://harvardlawreview.org