Law and Humanities Quarterly Reviews

Nget, M., Sam, R., Im, K., Kheuy, S., Em, D., & Yoeng, H. Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions. ***Law and Humanities Quarterly Reviews*****, 3(4), 26-41.**

ISSN 2827-9735

DOI: 10.31014/aior.1996.03.04.132

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research Law and Humanities Quarterly Reviews is a peer-reviewed International Journal of the Asian Institute of Research. The journal covers scholarly articles in the interdisciplinary fields of law and humanities, including constitutional and administrative law, criminal law, civil law, international law, linguistics, history, literature, performing art, philosophy, religion, visual arts, anthropology, culture, and ethics studies. The Law and Humanities Quarterly Reviews is an Open Access Journal that can be accessed and downloaded online for free. Thus, ensuring high visibility and increase of citations for all research articles published. The journal aims to facilitate scholarly work on recent theoretical and practical aspects of law.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Law and Humanities Quarterly Reviews
Vol.3, No.4, 2024: 26-41
ISSN 2827-9735

DOI: 10.31014/aior.1996.03.04.132

Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions

Makara Nget[1], Rany Sam[2], Kouy Im[3], Sinoeurn Kheuy[4], Dara Em[5], Hak Yoeng[6]

[1] Ministry of Interior and Royal University of Law and Economics (RUEL), Cambodia.
Email: makara.ng8181@gmail.com
[2] Graduate School, National University of Battambang (NUBB), Cambodia. Email: sam.rany@nubb.edu.kh
[3] Faculty of Arts, Humanities, and Education, National University of Battambang (NUBB), Cambodia.
Email: im.kouy@nubb.edu.kh
[4] Graduate School, National University of Battambang (NUBB), Cambodia.
Email: kheuysinoeurn2021@gmail.com
[5] Faculty of Sociology and Community Development, National University of Battambang (NUBB), Cambodia.
Email: em.dara@nubb.edu.kh
[6] Faculty of Arts, Humanities, and Education, National University of Battambang (NUBB), Cambodia.
Email: yoeng.hak@nubb.edu.kh

Correspondence: Rany Sam. Tel: +855(0)92646680, Email: sam.rany@nubb.edu.kh

Abstract
As global reliance on digital technology expands, so do the risks posed by cybercrime, which impacts individuals, institutions, and nations. This study has five main objectives: to evaluate global strategies for countering the growing cybercrime threat, compare diverse national approaches that reflect distinct legal traditions and enforcement priorities, identify and address critical challenges in combating cybercrime, assess the significant social and economic impacts of cybercrime, and highlight critical areas of focus to mitigate these threats. It also looks at the sophisticated methods that cybercriminals use and how technological advancements constantly reshape societal understanding and responses to cybercrimes. Cybercrime, once rooted in traditional crime, has evolved into a distinct and formidable threat fueled by the internet's anonymity and interconnectivity. This study advocates for a comprehensive global cybersecurity strategy that prioritizes legal reforms, encourages international cooperation, and tailors prevention strategies to the changing cyber landscape. It also addresses disparities in national cybersecurity preparedness, emphasizing the critical need for enhanced security measures and proactive strategies to mitigate cybercrime's widespread economic, social, and national security consequences.

Keywords: Cybercrime, Global, National, Dimensions, Challenges, Impacts, Solutions

1. Introduction

1.1. Definition of Cybercrime

The use of cybercrime is growing uncontrollably, and digital technology is advancing at an irreversible rate. We offer definitions of cybercrime that consider several scenarios. Cybercrime involves illegal activities via the internet and devices, which are often associated with hackers. Hacking is a general term for cybercrime, not just

hacking itself (Coll, 2022). Additionally, it is defined as the use of computers to perform socially unacceptable acts; the majority of cybercrime in the modern day involves the transfer of physical crimes into virtual spaces. (Richards, 2011). Hence, cybercrime encompasses a range of illicit activities conducted through devices and the internet, which are often linked to hackers. It represents the migration of traditional criminal activities into the digital realm, where illegal operations are conducted via computers and online platforms. Hacking serves as a prominent example of cybercrime, encompassing various socially unacceptable acts facilitated through computer technology. The landscape of cybercrime is always changing along with technology; thus, attempts to prevent and lessen its negative effects on society must be continuous.

Cybercrime, a significant issue in the digital age, can have severe consequences for nations and globally. states should be aware of this and take precautions. Cybercrime is increasing globally, highlighting the need for improved legal systems, national policies and response strategies to safeguard national security and social and economic systems. Owing to an increase in cybercrimes globally, research has emphasized the growing significance of cybersecurity and the need for improved national and international planning and response strategies to safeguard social and economic systems (Batrachenko, et al., 2024). With respect to government data, financial theft, and espionage, cybercrime is on the rise worldwide. Governments need to work together, establish prevention plans, and conduct investigations via digital forensic methods. (Sara, 2016). Social cohesiveness, economic stability, and national security are all impacted by cybercrime, which is an increasing concern in the digital era. Preemptive response strategies, robust policies, and enhanced legal frameworks are needed. Resilient social and economic networks depend on effective cybersecurity and digital forensic measures.

In conclusion, the emergence of digital technology has coincided with a notable rise in cybercrime, which is characterized by illicit actions carried out using electronic devices that are linked to the internet and that pose a general threat to public safety. The stability of contemporary society, the economy, and national security are all seriously threatened by cybercrime utilizing computers and other internet-connected gadgets. Recent studies have highlighted the need for national regulations, strong legal frameworks and strategies for enforcing response as cybercrime spreads around the world. Effective cybersecurity measures and the use of digital forensics are essential in the fight against cyber threats targeting wealth, finance, government action and sensitive data worldwide. We need to take comprehensive measures to protect the integrity of our growing digital industry and society.

1.2. Traditional Crime and the New Cybercrime

As digital technology has advanced, a new phrase called "cybercrime" has surfaced. There are crimes that fall outside of the usual categories. The methods employed in these two categories of crimes are diametrically opposed. Consequently, the various aspects of these two crimes are contrasted in this paper. Traditional crimes are committed by bodily offenders. Criminals use their experience and knowledge to commit crimes, and emerging crimes demand knowledge (Kumar, 2021). The microcontext of crime involves a person's presence, spatial possibilities, control, surveillance, and vulnerability, all of which have been used historically to explain criminal behavior (Rothe & Friedrichs, 2017). Understanding different kinds of criminal offenses is more structured by the categories shown in Table 1.2.1. The table facilitates recognition of the many types and consequences of these crimes by grouping them into several categories. Crimes directed at individuals or property include theft or other forms of physical injury, whereas crimes concentrate on the development of criminal intent. Criminal activity in legal contexts is widely represented by statutory and financial crimes, which include financial deception and regulatory infractions. Traditional crimes involve direct physical actions, whereas emerging crimes require specialized knowledge and skills. The microcontext approach examines individual and environmental factors influencing criminal behavior, such as location, control, surveillance, and vulnerability. Crimes are classified into crimes against persons and property, inchoate crimes, statutory offenses, and financial and other crimes. Table 1.2.1 helps organize and clarify these types of offenses, facilitating a clearer understanding of their nature, consequences, and context. This structured understanding aids in recognizing diverse forms of criminal behavior and the specific legal and societal responses needed. Recognizing these categories is crucial for academic study and practical applications in criminal justice.

Table 1.2.1: Criminal Offense Types

Categories	***Offenses***
Crimes Committed Against Individuals	Arson, Child Abuse, Domestic Abuse, Homicide, Assault and Battery, Kidnapping, Rape, and Statutory Rape
Crimes Involving Property	Robbery, Vandalism, Theft, and Fraud
Inchoate Crime	Conspiracy, attempt, aiding, and abetting
Lawful Offenses	Financial/White Collar Crimes, Drug-Related Crimes, Traffic Offenses, and Crimes Associated with Alcohol
Financial and Additional Offenses	Cybercrime, tax evasion, embezzlement, money laundering, fraud, and blackmail

The word "cybercrime," which was coined in the latter half of the 20th century, describes a traditional crime with a fresh look that is constantly evolving in response to new developments in technology (Newman, 2009). Cybercrime is the term for crimes committed using technology and the internet by the same offenders as traditional crimes. Hackers can be members of criminal gangs, disillusion teenagers, and enraged employees, activists, and state foes. Their techniques for obtaining information and carrying out attacks are comparable to those of physical crimes; the distinction is in the application of technology (PGI, 2018). Despite the use of technology and the internet, cybercrime essentially does not differ from traditional crime in terms of players and their goals. In essence, it is a contemporary version of classic crime, committed by comparable criminal characters employing cutting-edge technology techniques. Rather than a fundamental shift in criminal behavior or intent, the evolution of cybercrime is primarily a reflection of changes in the instruments employed. Understanding the types of cybercrime is a reflection of the level of danger it poses to institutions, individuals, and businesses, as well as its relentless evolutionary process as technology advances daily. Recognizing its type is important in arranging legal framework amendments in accordance with the digilization context, as shown in Table 2.1.2. Cybercrime, though it uses modern technology and the internet, fundamentally mirrors traditional crime in terms of its underlying motives and the individuals involved. While tools and methods have evolved, the essence of cybercrime remains consistent with classical criminal behavior. The motivations behind cybercrimes are often the same as those behind physical crimes, regardless of the hacker's identity: state rivals, activists, angry employees, professional thieves, or others. The primary distinction lies in the technological means used, not in the nature of the crime itself. Technology advancements are contributing to the sophistication of cybercrime, which is commensurate with the continuous expansion of criminal tactics. Understanding the different forms and characteristics of cybercrime is crucial for assessing the risks that it poses to businesses, organisations, and people. As shown in Table 2.1.2, this understanding is crucial for modifying legal frameworks to meet the difficulties brought about by digitalization. Therefore, even though crime has taken on a different face, the underlying ideas that motivate criminal activity have not been altered.

In contrast to cybercrime, which involves virtual interactions and digital proofs, traditional crimes require direct physical actions and tangible evidence, such as theft, violence, and property damage. Similar criminal profiles and motivations underlie both kinds of crimes; thieves are frequently driven by a desire for vengeance, money, or personal fulfillment. In contrast, cybercrime employs technologically enabled digital techniques such as malware, phishing, and hacking. While traditional crimes have changed over time due to modifications to physical security systems and tactics used by law enforcement, cybercrime has continued to adapt due to advancements in technology. Conventional crimes have well-established legal frameworks that can be modified to accommodate emerging practices. Legislative frameworks are changing to keep up with technology advancements, and cybercrime is becoming more widely acknowledged as a separate category requiring specialized legal and technological knowledge. To effectively build legal responses and modify frameworks to address both classic and emergent criminal concerns, comprehending the similarities and differences between cybercrimes and traditional crimes is imperative.

In conclusion, a comparison of traditional and cybercrimes reveals that criminal behavior is both constant and evolving. Conventional crimes, such as stealing, violence, and property destruction, are defined by overt physical acts and concrete proof, and they are carried out by people driven by greed, retaliation, or self-gratification. These crimes have evolved with changes in physical security and law enforcement techniques, but their core nature remains consistent. In contrast, cybercrime represents a contemporary adaptation of traditional criminal behavior, leveraging modern technology and the internet. Although the methods—such as hacking, phishing, and malware—are digital, the underlying motives and criminal profiles are similar to those involved in traditional crimes. Cybercriminals, whether professional thieves, criminal organizations, or state adversaries, commit crimes for reasons comparable to those of their traditional counterparts, with the primary difference lying in the technological tools and techniques used. The evolution of cybercrime reflects the rapid advancement of technology, necessitating specialized knowledge and sophisticated methods. This ongoing development poses unique challenges to legal frameworks, which must adapt to address the specific nature of cybercrime effectively. Even though they are well established, traditional legal solutions must change to meet the complexity of cybercrime, as demonstrated by the modifications needed for digital environments. To effectively construct legal remedies and ensure that both classic and emergent criminal dangers are fully addressed, comprehending the parallels and differences between cybercrimes and traditional crimes is imperative. The structured classification of crimes, as displayed in Tables 1.2.1 and 2.1.2, facilitates this understanding by making it simpler to recognize and address various categories of criminal activities. Legal frameworks must be modified to reflect the changing nature of crime, both traditional and cyber, to maintain the integrity of justice and security protocols in a world that is changing constantly.

1.3. Research Questions

The article focuses on comprehending the extent of cybercrime at the global and national levels, the various issues these crimes provide, their effects on various sectors of society, and viable tactics and solutions for tackling them, which are encompassed by the study question.

- How can the global community effectively address and mitigate the growing threat of cybercrime?
- How do different countries' legislative frameworks and enforcement strategies address and adapt to the evolving threat of cybercrime, and what are the distinctive features of their approaches?
- What are the key challenges in combating cybercrime, and how can it be improved to address these issues effectively?
- What are the impacts of cybercrime on society and businesses, and what comprehensive strategies are needed to address and combat these impacts effectively?
- What are the key categories of activities necessary for effectively combating cybercrime?

1.4. Research Objectives

To answer the research questions above, this research highlights five objectives:

- To evaluate global strategies to effectively address the growing threat of cybercrime, the global community must adopt a coordinated and multifaceted approach.
- To compare national approaches between different countries that have developed various legislative frameworks and enforcement strategies to combat cybercrime, reflecting their unique legal traditions and national priorities.
- To identify and address challenges in combating cybercrime.
- To evaluate the significant impacts of cybercrime on society, comprehensive strategies that incorporate both preventive and responsive measures are needed.
- To identify and describe the essential areas of focus and activities required to address and mitigate the threats posed by cybercrime.

1.5. Research Methodology

This research employs a desk-based methodology to examine the impact of cybercrime across different geographical regions, alongside a comparative analysis to assess various nations' legal frameworks and response strategies. Through this approach, the study reveals shared challenges, distinct differences, and specialized tactics

these regions use to combat cybercrime effectively. Additionally, this analysis highlights critical issues and identifies potential solutions to enhance the global response to cybercrime.

1.6. Literature Review

Cybercrime has become a major worldwide concern in an era characterized by rapid technical innovation. The significance of understanding cybercrime—defined broadly as illegal activities facilitated through the use of the internet—has escalated as countless social, economic, and national security systems have become increasingly interconnected and reliant on digital infrastructure. This literature review synthesizes findings from recent studies exploring the multifaceted nature of cybercrime, its traditional crime roots, and the responses required in both global and national contexts.

The definitions of cybercrime provided by scholars such as Coll (2022) and Richards (2011) underscore the phenomenon's breadth, encompassing various actors and motivations that reflect the shifting boundaries of criminality in the digital age. Batrachenko and colleagues (2024) highlight the increasing prevalence of cybercrime, necessitating stronger legal frameworks and policy responses tailored to protect social and economic structures at the national and international levels. Governments are increasingly aware of the implications of cyber threats, as cybercriminal activities target sensitive data, financial assets, and infrastructure, thereby jeopardizing economic stability and national security (Sara, 2016). The need for collaborative and multifaceted response strategies is further emphasized by the literature, which advocates for enhanced cybersecurity measures, robust legal systems, and improved international cooperation.

Traditional crimes have historically involved direct physical interaction and impacts, whereas cybercrime leverages technology to perpetrate similar motives, such as theft, revenge, or satisfaction (Kumar, 2021; PGI, 2018). Research highlights that successful analyses of cybercrime must address both the continuity and transformation of criminal behavior, emphasizing that despite the change in tools, the fundamental motivations of criminals remain largely unchanged (Newman, 2009). The literature illustrates those cybercriminals, whether state-sponsored actors or malicious individuals, often employ methods that mirror those of traditional crime, albeit through a digital interface (Indonet, 2024). The literature reveals distinct approaches to combatting cybercrime shared by various national entities, highlighting the evolving legislative framework of key nations, including the United States, the EU, China, Japan, and Australia. These frameworks illustrate a trend toward specialized legislation and enforcement mechanisms to address the unique challenges posed by cyber threats (CISA, 2024; GDPR, 2016; Markopoulou et al., 2019). In particular, the U.S. demonstrates a comprehensive strategy involving various legislative acts, such as the DMCA and CFAA, alongside multiagency collaborations focusing on strategic enforcement of cybercrime laws (Chabinsky, 2010). The European Union’s rigorous legal framework emphasizes data protection and international collaboration to enhance collective resilience against cyber threats (Seger, 2011).

Combating cybercrime poses several unique challenges because of its complex and adaptive nature. The literature highlights significant hurdles, including anonymity and jurisdictional issues, which hinder the effective tracking and reporting of cybercriminal activity (Marisol Cruz Cain, 2023). Furthermore, differing legal frameworks and international cooperation inconsistencies impede a unified front against cybercriminal organizations, emphasizing a pressing need for continual adaptation and collaboration (Europol, 2019; Cassim, 2010). The consequences of cybercrime are profound, extending beyond monetary losses to encompass psychological, social, and organizational dimensions. Studies by the Center for Strategic and International Studies (CSIS) indicate that cybercrime costs nearly one percent of global GDP annually, further illustrating the growing need for advanced protective measures and strategic investments in cybersecurity (Lewis, 2018; Tariq, 2018; Tieng et al., 2024).

The literature presents a compelling narrative on the significant challenges posed by cybercrime in both global and national arenas, underscoring the necessity of comprehensive, adaptive, and collaborative approaches to cybersecurity. Understanding the evolution of cybercrime—its overlap with traditional crime motivations—can inform legislative and enforcement strategies tailored to the contemporary digital landscape. Future research should seek to bridge existing gaps, offering insight into effective collaboration frameworks that enhance the

global response to this pressing threat and ensure continued protection for individuals, organizations, and nations alike.

2. Research Findings

2.1. How can the global community effectively address and mitigate the growing threat of cybercrime?

The threat of cybercrime is growing and becoming more widespread because of daily digital technology advancements, which have been used as the means in relationships among trade, politics, and the economy. These elements result from our growing dependence on digital technology. Although technology has evolved into a vital instrument for expediting tasks, cutting expenses, time, and complex procedures, it is also a weapon capable of destroying economic growth. Billionaire Warren Buffet noted that cybercrime is more of a threat to the economy and instability than nuclear weapons are (Chin, 2023). Significant geographical differences in cybercrime costs in relation to GDP are highlighted in Table 2.1.1. Cybercrime affects a larger percentage of GDP in industrialized nations such as North America, Europe, and Central Asia, whereas less developed regions are comparatively less affected. Nonetheless, as digital economies expand worldwide, the equitable consequences of cybercrime continue to be a crucial concern for every area. Effectively combating cybercrime necessitates specialized approaches that consider the distinct digital infrastructures and economic environments of every location.

Table 2.1.1: Geographic Dispersion of Cybercrime in 2017

Area (World Bank)	GDP by Region (USD, trillions)	Cost of Cybercrime (USD, trillions)	Loss from Cybercrime (% GDP)
Americas North	20.2	140 to 175	0.69 to 0.87%
Central Asia and Europe	20.3	160 to 180	0.79 to 0.89%
The Pacific and East Asia	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
The Caribbean and Latin America	5.3	15 to 30	0.28 to 0.57%
The African Sub-Saharan	1.5	1 to 3	0.07 to 0.20%
MENA region	3.1	2 to 5	0.06 to 0.16%
Global	$75.8	$445 to $608	0.59 to 0.80%

Source: (Lewis, 2018)

The international economy is seriously at risk due to the growing menace of cybercrime, which is being fed by rapid improvements in digital technology. While technology fosters creativity and increases output, it also presents risks that could compromise financial stability. Cybercrime has the potential to pose greater economic risk than nuclear threats. Compared with less developed countries, industrialized regions experience greater GDP loss as a percentage of cybercrime. Effective cybercrime response necessitates customized approaches that consider the distinct technological and economic environments of each country, given the ongoing growth of the digital economy.

The typology of cybercrime shown in Table 2.1.2 emphasizes how varied and intricate cybercrime is. Every category, which includes offenses against people and property as well as deception, market-based, and political offenses, illustrates a distinct facet of the illicit use of technology. A multimodal approach linking international cooperation, legal frameworks, and technical innovations is needed to combat these cyber offenses. Staying up to date with initial cyberthreats is imperative to safeguard individuals, organizations, and entire countries against the ever-destructive effects of cybercrime as digital technologies progress.

Table 2.1.2: Cybercrime typology

Crimes against devices	Crimes against persons	Crimes of deception and coercion	Market-based crimes and crimes against property	Political offences
Hacking	Hate speech	Fraud	Illegal markets online	Hacktivism
	Harassment	Extortion	Intellectual property infringement	Cyberwarfare
	Sex crimes			Cyberterrorism
				Controlling cyberspace as political deviancy

Source: (Lavorgna, 2020) Cybercrimes: Critical issues in a global context

One category of online criminal conduct is cybercrime, which can range from small-term mischief to more serious financial crimes. Cybercrimes are more common due to several factors, such as weak security systems, a lack of security awareness, technological advancements, internet anonymity, the exploitation of human weaknesses, lax punishment, reliance on technology, user identities, location, financial motivation, and the ever-changing digital environment. To reduce the likelihood of cybercrimes and create effective security procedures, it is imperative to become aware of these components (Indonet. 2024). Cybercrime is a complex offense involving personal, property, deception, market-based activities, and political offenses. Addressing this topic requires a comprehensive approach involving technological advancements, robust regulatory frameworks, and international collaboration, while understanding the underlying factors is crucial for protection.

The surge of cyberthreats has had a major effect on international institutions and governmental organizations. The consequences of global and business-critical risks and threats are emphasized in the 2020 UN Joint Inspection Unit examination of the country's cybersecurity rules (Flores Callejas, et al., 2021). The UN Joint Inspection Unit highlights the necessity of strong cybersecurity frameworks and plans and stresses the importance of tackling global and business-critical cyber threats. The acknowledgment of the possible repercussions of cyberattacks is seen in the change from putting national security measures into place to considering the wider effects of cyberthreats on international governance and collaboration. Cyberattack reports indicate that the popularity of targeting international governments and institutions has increased (Sentinel One, 2022). Studies have shown a marked rise in cyberattacks directed at foreign governments and organizations. The increasing focus on high-profile targets with significant influence and vital infrastructure by cybercriminals and state-sponsored actors is indicative of a strategic shift that is driving this expanding trend. There are a variety of reasons behind these attacks, including destabilization, disruption, and financial or political gain. The number of cyber threats is growing, impacting governmental organizations and international institutions. The UN Joint Inspection Unit emphasizes the need for enhanced cybersecurity measures. Collaboration, information sharing, and defensive capabilities are crucial for maintaining global governance and institutional operations.

Advances in digital technology have led to an increasing menace of cybercrime, which presents a serious risk to international trade, politics, economies, and stability. Technology increases efficiency and output, but it also introduces risks that could negatively affect economic expansion. Cybercrime now represents a greater economic threat, particularly affecting industrialized nations more than less developed regions do. As digital economies continue to expand, addressing cybercrime requires tailored approaches that consider regional technological and economic contexts. The diverse nature of cybercrime, spanning offenses against individuals, property, and political structures, underscores the need for a comprehensive and adaptive response. This encompasses technological progress, strong regulatory environments, and global cooperation. The complications of cybercrime and the factors that cause it to increase the effectiveness of security solutions are determined. To protect institutional and governmental truthfulness from the threat of cyberattacks, it is critical to increase cybersecurity safeguards and

foster international cooperation. This is demonstrated by the increasing weight given to well-known international targets.

2.2. How do different countries' legislative frameworks and enforcement strategies address and adapt to the evolving threat of cybercrime, and what are the distinctive features of their approaches?

The ways in which countries respond to cyber threats are changing in tandem with the digital realm. Owing to the serious threat cybercrime poses to international security, privacy, and economic stability, several legislative frameworks and enforcement strategies have been developed by various nations. The national approaches to fighting cybercrime from the US, the EU, China, Japan, and Australia are compared and examined in this paper, with an emphasis on the legal systems and methods of enforcement. The United States has implemented a diverse legislative framework that consists of a network of specialized authorities in addition to federal legislation to combat cybercrime. The important pieces of legislation are the Digital Millennium Copyright Act (DMCA), which provides internet service providers with safe harbor protection against digital copyright infringement (Congress, 1998), and the Computer Fraud and Abuse Act (CFAA), which aims to counteract the growing ubiquity of cybercrimes (Goldman, 2012). The Cybersecurity Information Sharing Act (CISA) encourages government and business sector sharing of threat intelligence (Beyer, 2015). Numerous important organizations oversee enforcement. Financial cybercrime, including credit card fraud and financial crimes enabled by cybercrime, is the primary focus of the United States. While the Federal Bureau of Investigation (FBI) conducts high-profile investigations into major cyber threats (Chabinsky, 2010) and the Infrastructure Security Agency (CISA) promotes worldwide cooperation with international partners to address cybersecurity threats (CISA, 2024), while federal laws are enforced, the Department of Justice (DOJ) seeks appropriate punishment for those guilty and ensures that justice is administered impartially and fairly (Livingston, 1999). The US has a comprehensive approach to combating cybercrime, combining legislative frameworks such as the DMCA and CFAA with specialized enforcement agencies. Important laws that address unauthorized access and digital copyright infringement are the DMCA and the CFAA. Different authorities carry out enforcement, which is indicative of the dynamic nature of cyber threats.

The European Union’s approach to cybercrime is guided by a robust legal framework focused on data protection and network security. The General Data Protection Regulation (GDPR), which is the cornerstone of EU data privacy, guarantees confidentiality and adherence to legal requirements for the handling and acquisition of personal data (GDPR, 2016). The first piece of legislation at the EU level to secure network and information systems is the Network and Information Systems (NIS) Directive, which addresses the risk of interruptions to IT services and key infrastructures, which are vital to the operation of the Union and Internal Market (Markopoulou, et al., 2019). The Budapest Convention further promotes international cooperation through its global framework for combating cybercrime to criminalize computer-related crimes, providing investigative tools and safeguards to protect human rights and prevent law enforcement abuse, with the Council of Europe developing additional practices (Seger, 2011). The European Cyber Crime Centre (EC3), which was founded to fight cybercrime in the EU, supports enforcement throughout the EU. It generated analytical products for the deep web and dark net, particularly items related to bitcoin and the underground economy (Vendius, 2015). The European Union Agency for Cybersecurity (ENISA) provides operational cybersecurity advice and recommendations (Negreiro, 2019). Additionally, each member state has its own national cybersecurity agencies responsible for implementing EU directives and enforcing cybersecurity laws. The European Union's comprehensive approach to combating cybercrime integrates a robust legal framework with dedicated institutions to safeguard data privacy and network security. Central to this framework are the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) Directive, which establish stringent guidelines for data handling and protection of critical infrastructure. The Budapest Convention further enhances international collaboration and establishes a global standard for addressing cybercrime. Important responsibilities in providing operational and strategic support are played by the European Union Agency for Cybersecurity (ENISA) and the European Cyber Crime Centre (EC3). When taken as a whole, these steps guarantee a coordinated and efficient response from national agencies throughout member states to the constantly changing risks posed by cybercrime.

China's legal framework for addressing cyber threats is characterized by stringent national regulations and a focus on state control. The Cybersecurity Law aims to ensure adequate security for the country's "informatization" policy (Creemers, 2023). The People's Republic of China's Data Security Law, which addresses procedures, responsibilities, and liabilities at the levels of both state administration and data handlers, is the cornerstone legislation in China's data security domain (Chen & Sun, 2021). The country's data protection law was reformed, leading to the creation of China's new Personal Information Protection Law, which has the main goal of protecting the privacy and personal information of Chinese citizens (Torrisi, 2023). Enforcement is handled primarily by the Cyberspace Administration of China (CAC), which governs the Chinese digital realm, sets rules, and enforces regulations while supporting the Party Central Cybersecurity and Information Commission (CCIC)'s work and holding authority over specialized technical bodies (Portrait, 2023). The Public Security Bureau (PSB) enforces criminal background checks for websites and mobile applications hosted in China. The "Measures for the Administration of internet Information Services" that the Chinese State Council published in 2000 serve as the reference law (What is Public Security Bureau filing and why is it required?, 2023). The SIIO oversees internet communication policies, legal systems, online content management, business approvals, government plans, news website promotion, government publicity, website investigations, telecom service provider management, and local information office guidance (Michelle Chan, 2011; Sam et al., 2015). China's legal framework for cybersecurity and data protection is characterized by a robust and centralized regulatory approach intended to enhance state control and safeguard national interests. The nation's efforts to safeguard its digital infrastructure and manage data security, with a focus on the protection of private and personal information, are driven primarily by the Cybersecurity Law and the Data Security Law. China's evolving attitudes toward privacy are reflected in the Personal Information Protection Law, a significant form of data protection legislation. A number of important organizations oversee enforcement, such as the Public Security Bureau (PSB) and the Cyberspace Administration of China (CAC), which ensure that digital operations follow strict regulations and supervise compliance. Measures for the Administration of internet Information and other historical rules serve as the foundation for the framework.

Japan's national approach to cybercrime is proactive and involves robust legislative frameworks, coordinated enforcement, and a strong emphasis on prevention and resilience. Cybercrimes in Japan are punishable by the Penal Code and Unauthorized Computer Access Law, along with the most defined laws in the Cybercrime Convention. However, certain Convention's provisions—such as communication eavesdropping and unlawful access to computer systems—are not addressed by current legislation (Natsui, 2003). The private sector's practices for processing and protecting personal data are governed by the Act on the Protection of Personal Information (APPI) (Iwase, 2019). The Japanese Act on the Regulation of Transmission of Specified Electronic Mail aims to combat spam emails, introduced in 2002, with an opt-out system, strengthened penalties in 2005, and targeted overseas spam (Kawase, 2024). National and municipal governments' roles and strategies for improving cybersecurity are delineated in the Basic Act on Cybersecurity (BAC). Critical infrastructure operators must voluntarily improve cybersecurity and cooperate with governments according to a cybersecurity strategy released by the Japanese government (Hiromi Hayashi, 2023). The Cybersecurity Strategy of 2018 was announced by the Japanese government and aimed to promote a sustainable cybersecurity ecosystem for sustainable development, with a focus on mission assurance, risk management, and participation (Europe, 2024). Japan's cybercrime enforcement is overseen by several institutions.

The National Police Agency (NPA) is a national organization that is tasked with developing police policies; carrying out operations; managing issues, including criminal justice, education, training, and communications; and organizing police administration (NPA, n.d.). According to the Act on Personal Information Protection, the Personal Information Protection Commission (PPC), an independent body in Japan, protects people's rights and interests and ensures that personal information is used appropriately (PIPC, n.d.). The secretariat of the Cybersecurity Strategy Headquarters is the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which works with the public and business sectors to create a safe, open, and equitable cyberspace (NISC, 2024). The first Computer Security Incident Response Team (CSIRT) in Japan, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), works with the Asia Pacific Computer Emergency Response Team (APCERT) to coordinate incident coordination and manage damage-causing incidents (JPCERT/CC, 2023). Japan's cybercrime strategy is a comprehensive approach that combines legislative measures, coordinated enforcement, and cybersecurity resilience. The country's legal framework includes the Penal Code, Unauthorized

Computer Access Law, and Cybercrime Convention regulations. However, there are still holes in the coverage, especially in regard to communication interception and illegal access to computer systems. As they address cybersecurity risk, specific privacy laws and regulatory email regulations need to be updated on a regular basis to respond to the limitless evolution of cybercrime. The Basic Act on Cybersecurity and the Cybersecurity Strategy emphasize collaboration and a collaborative approach to enhance national cybersecurity. The Cybersecurity Strategy of 2018 emphasized sustainable cybersecurity practices and international collaboration. Despite these challenges, Japan's commitment to updating its legal framework and international cooperation is crucial for maintaining and advancing its cybersecurity posture in the digital world.

Australia takes a balanced legal framework and proactive enforcement stance in regard to fighting cybercrime. The 2001 Cybercrime Act amended the Criminal Code Act of 1995 to include the following new offenses (Chan, et al., 2003). With the help of the Privacy Act of 1988, people now have more control over their personal data. They can seek access, prohibit unsolicited marketing, understand its use and dissemination, amend inaccurate information, and register complaints (Government, n.d.). Enforcement is conducted by several government agencies, including the Australian Cyber Security Centre (ACSC), which is a Commonwealth government agency that monitors global cyber threats, issues alerts Australians, and develops solutions. It provides advice to individuals, businesses, and critical infrastructure owners on cybersecurity incidents (Reuters, 2024). The Australian Federal Police (AFP) is the main law enforcement body that helps other law enforcement agencies while upholding Commonwealth criminal legislation, fighting organized crime, and safeguarding Commonwealth interests (Government, 2024). The Privacy Act of 1988, the Freedom of Information Act of 1982, and the Australian Information Commissioner Act of 2010 assign three primary duties to the Office of the Australian Information Commissioner (OAIC): privacy, freedom of information, and government information policy (Government, 2023). Australia's approach to cybercrime is a balanced legal framework with a proactive enforcement strategy. The Cybercrime Act of 2001 and the Privacy Act of 1988 are key legislative updates that address cyber threats and protect individual rights. The Australian Cyber Security Centre (ACSC) monitors global cyber threats, whereas the Australian Federal Police (AFP) enforces Commonwealth laws and tackles organized crime. The federal information policy, freedom of information, and privacy departments are overseen by the Office of the Australian Information Commissioner (OAIC). This integrated strategy addresses immediate cyber threats while fostering a culture of cybersecurity resilience and individual privacy. As cyber threats evolve, Australia's approach will need to adapt to ensure the effectiveness of both legal frameworks and enforcement mechanisms in safeguarding the nation's digital landscape.

In conclusion, the global response to cyber dangers is represented in various legislative frameworks and enforcement strategies that are tailored to the unique needs and objectives of each nation. The United States employs a multipronged strategy to combat various aspects of cybercrime, combining federal legislation such as the DMCA and CFAA with specialized authorities. The European Union prioritizes network security and data protection through regulations such as the GDPR and the NIS Directive, with assistance from groups such as the EC3 and ENISA. China's cyber defense posture is greatly impacted by its strict national regulations and state control policies, which include laws such as the Data Security Law and Cybersecurity Law. Japan combines these components with proactive laws such as the Penal Code and APPI, coordinated enforcement, and an emphasis on resilience. Australia has taken a balanced stance, incorporating both legislative changes and effective enforcement by organisations such as the AFP and ACSC. Each region's strategy highlights the need to adapt to evolving cyber hazards while balancing legal, regulatory, and enforcement actions to protect digital environments and maintain privacy.

2.3. What are the key challenges in combating cybercrime, and how can it be improved to address these issues effectively?

Cybercriminals use cutting-edge technology and crafty tactics. This is a factor that makes it challenging for experts to combat cybercrime. Common problems in fighting cybercrime, such as location loss, data loss, problems with the legal system, barriers to international cooperation, and public–private partnerships, call for more investigations and comparisons (European, 2019). Cybercrime is a crime involving cybercriminals targeting computers or networks, causing damage, or stealing information. It is difficult to track due to anonymity and international

spread. Fear of identity theft and reputational damage hinders reporting. Internal limitations hinder a comprehensive understanding of cybercrime (Marisol Cruz Cain, 2023). Therefore, specialists attempting to counter these threats face considerable obstacles in light of the growing environment of cybercrime, which is typified by the use of sophisticated strategies and cutting-edge technology. The difficulties in international cooperation and public–private partnerships, as well as problems with location loss, data loss, and the shortcomings of the legal system, add to the complexity. To solve these issues and develop better solutions, further research and comparisons are needed. Tracking and reporting are made more difficult by the anonymity and global reach of cybercriminal operations, which deters people from coming forward for fear of identity theft and reputational damage. A comprehensive and collaborative strategy that overcomes internal barriers and fosters international collaboration is needed to effectively address cybercrime.

The main problem with the suppression of cybercrime, which requires high skills and abilities, is the need to respond to more options. However, cybercrime poses a serious risk to the security of the country, as it targets private, state, and international organizations. The internet is the primary target, and combating it requires coordinated international efforts. The European Cyber Crime Center (EC3), a key player, collaborates with internet companies and operates online payment systems to protect users and destroy criminal organizations (Nuredini, 2014). On the other hand, with strong law enforcement agencies, it is not enough to fight complex cybercrime; it requires strengthening the legal framework by amending inconsistent laws to keep pace with the evolution of cybercrime. South African common law, including the Electronic Communications and Transactions Act (ECT), has been ineffective in addressing cybercrime. The Act's section 15 for electronic information admission is commendable, but its criminal sanctions are insufficient. Courts are cautious in handling cybercrime cases, and the banking sector is vulnerable. The Council of Europe's Convention on Cybercrime is recommended to prevent international cybercrime (Cassim, 2010). The fight against cybercrime is fraught with challenges that demand a high level of skill and an adaptive legal framework. Despite the efforts of entities such as the European Cyber Crime Center (EC3), which works with internet companies and online payment systems to thwart criminal activities, cybercrime remains a substantial threat to national security, affecting private, state, and international organizations. The primary battleground is the internet, necessitating coordinated international efforts to effectively counter these threats. However, even with strong law enforcement agencies, combating sophisticated cybercrime requires more than just robust enforcement; it necessitates a well-evolved legal framework. Current laws, such as South Africa's Electronic Communications and Transactions Act (ECT), fall short of addressing the complexities of cybercrime, particularly regarding inadequate criminal sanctions and cautious judicial handling. To enhance the effectiveness of legal responses, it is crucial to amend inconsistent laws and consider ratifying international agreements such as the Convention on Cybercrime of the Council of Europe. These steps are vital for developing a comprehensive and effective approach to combating international cybercrime and safeguarding against its evolving threats.

In conclusion, combat against cybercrime is becoming more complex because of the use of modern technology and modern strategies with the use of more sophisticated tools by cybercriminals. In addition, the fight against complex crime faces a number of challenges, including loss of location and data, gaps in the legal framework, and barriers to international cooperation and public–private partnerships. These factors hinder an effective response and emphasize the need for more thorough research and comparative analysis related to this type of crime. In particular, cybercrime poses a significant threat to national security and targets many organizations, including private, public, and international institutions. The main battle is the internet, where international coordination efforts are important. While specialized international organizations play a key role in addressing these threats, the current legal framework is insufficient to address the evolution of cybercrime. The limitations of this law, especially in criminal penalties and judicial prudence, highlight the need for legal reform and international cooperation. To effectively fight cybercrime, a comprehensive strategy to overcome internal obstacles and promote global cooperation is needed. Strengthening the legal framework, amending inconsistent laws, and ratifying international agreements. By addressing these issues, we can better prevent and combat the multifaceted and growing threat of cybercrime.

2.4. What are the impacts of cybercrime on society and businesses, and what comprehensive strategies are needed to address and combat these impacts effectively?

Cyberattacks cause serious societal problems, including identity theft and online scams, have a negative psychological impact on the people who are affected, and have a substantial financial impact on businesses and financial institutions. According to a survey by the Center for Strategic and International Studies (CSIS), cybercrime costs the world economy up to one percent each year. The increase in cybercrime is ascribed to the adoption of new technology by cybercriminals as well as the ease with which they may use black markets and digital currency (Lewis, 2018). Additionally, cybercrimes pose a serious danger to financial institutions since they are expanding quickly and resulting in both direct and indirect losses. Organizations need to concentrate on security measures such as strengthening internal security, performing cybersecurity assessments, providing training, and carrying out cybersecurity audits to safeguard themselves (Tariq, 2018). Cybercrime, a silent, dangerous threat, costs organizations an average annualized $5.9 million, with varying costs ranging from $1.5--36.5 million (Das, & Nayak, 2013). The study noted that crime is an omnipresent social phenomenon that affects all societies, regardless of civilization. It is a basic human instinct and a social concern because of the potential disturbance it causes. Victims may forfeit priceless things such as property, money, safety, and serenity—values that are crucial to fulfilling many desires. The study revealed that the newest type of social interaction in society is cyber communication. Emails, texts, and online social networking sites allow consumers a rapid and efficient means of communicating with individuals worldwide.

In particular, teenagers use computers or other personal electronics to spend hours every day online. Meanwhile, cybercrime costs have increased significantly in online business, with global spending on information security reaching $2.1 trillion by the end of 2019, emphasizing the need for stronger security measures to fend off possible cyberattacks (Ibrahim, 2019). The pervasive threat of cyberattacks underscores a critical challenge for businesses, financial institutions, and individuals alike. The economic burden, estimated at nearly one percent of global GDP annually, coupled with significant social issues such as identity theft and online scams, reveals the far-reaching impact of cybercrime. Financial institutions face escalating risks, necessitating rigorous security measures, including enhanced internal protocols, regular cybersecurity assessments, and comprehensive training. The substantial financial losses, alongside broader social implications, highlight the urgent need for advanced and proactive defenses. As cyber communication becomes increasingly integral to modern life, the surge in global spending on information security has emphasized the necessity of fortifying our digital infrastructure to mitigate these evolving threats. The growing sophistication of cyber threats necessitates a concerted effort to safeguard against their potentially devastating effects on both the economy and society.

Cyberattacks, which cost the world's economy more than 1% annually, represent a serious risk to individuals, businesses, and financial institutions. The rapid advance of cybercrime technology and the ease of exploitation in the black market and fundamental currency are the main reasons for this cost growth. Shares are high, especially for financial institutions, as direct and indirect losses are increasing frequently. To address these issues, organizations need to implement strict security measures, such as strengthening internal controls, conducting regular cybersecurity assessments and setting funds for in-depth training and audits. Cybercrime has more than just monetary damage. It includes important social issues such as identity theft and cyber fraud, which have a profound psychological impact on people and communities. Significant losses such as personal safety, financial security, and peace of mind are often inflicted by victims. These effects illustrate how cybercrime affects society as a whole and is exacerbated by the increasing use of cyber technology. Cybercrime affects many users, especially teenagers, who spend much of their time online, as email, text messages and social media are becoming more important for daily communication. The rising cost of cybercrime, which has reached an average annual loss, underscores the urgent need for better security measures. The need for businesses to invest in strong protection against cyber threats is illustrated by the rising global cost of information security. This investment is important in ensuring the social and emotional well-being of the general population in addition to their financial wealth.
In conclusion, a multifaceted strategy is needed to combat the threat of cyberattacks, including bolstering digital infrastructure, putting in place cutting-edge security measures, promoting a strong legislative framework, and cultivating a cybersecurity-aware culture. Organizations, businesses and individuals need to be watchful and

proactive to mitigate the potentially devastating impacts of cyber threats on society and the economy as they continue to evolve.

2.5. What are the key categories of activities necessary for effectively combating cybercrime?

The study resulted in Table 2.5.1 four fundamental categories of activities necessary for effectively combating cybercrime. Each category represents a distinct area of focus, reflecting a comprehensive strategy to address the multifaceted nature of cyber threats.

a) Cooperation and Communication

This category highlights the importance of collaborative efforts and communication channels in the fight against cybercrime. It includes actions taken between various entities, such as governments, international organizations, and the private sector. Key activities involve establishing bilateral and multilateral agreements between states to coordinate efforts across borders. Additionally, establishing reporting channels and promoting international cooperation are essential for exchanging data and resources, which improves our ability as a group to identify, stop, and neutralize cyberthreats.

b) Policy and Strategy

The development of a structured and logical strategy to combat cybercrime requires policies and approaches. The creation and execution of international and national regulations aimed at countering and averting cyberthreats fall under this category. Effective policies outline the goals, priorities, and actions needed at various levels to combat cybercrime. National policies might include guidelines for cybersecurity practices and responses, whereas international strategies could involve agreements on cooperative measures and joint initiatives to address global cyber threats.

c) Legal

Legal action is a vital means of determining, prosecuting, and prosecuting cybercrime. These rules involve the development and implementation of laws, regulations, and frameworks that focus specifically on combating cyber threats. Effective laws and regulations establish clear standards, define cybercrime activities, provide a basis for legal action against perpetrators, and provide mechanisms for dealing with and judging cybercrime cases.

d) Training and Technical Assistance

Training and technical support are necessary to provide people and organisations with the necessary abilities and knowledge to effectively combat cybercrime. They also help create a technical grasp of cybersecurity infrastructure, management, and sustainable technology. Through this training, people become more aware of cyberthreats and acquire the skills and knowledge necessary to stop and handle cyberincidents with the aid of technical support.

Therefore, Table 2.5.1 outlines a comprehensive strategy for combating cybercrime, emphasizing the necessity of cooperative endeavors, well-defined protocols, legal structures, ongoing training, and technical assistance. To provide a coordinated and successful response to the changing problems of the digital era, each category is essential to the construction of a strong defense system against cyber threats.

Table 2.5.1: Four Types of Cybercrime Prevention Activities

Categories	Activities
Cooperation and Communication	International coordination, bilateral and multilateral agreements between governments, reporting channels, and other measures are examples of actions made by entities to prevent cybercrime.

Policy and strategy	Policies and tactics at the national and international levels are required to combat cybercrime.
Legal	Legislation, regulations, and frameworks are examples of legal actions intended to prevent cybercrime.
Technical support and instruction	To combat cybercrime, one needs technical expertise (i.e., knowledge of infrastructure, security controls, and sustainable technologies), cybersecurity training, and cybercrime awareness.

Source: (To, 2023). Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime.

3. Conclusion and recommendations

Cyberbullying is becoming more serious and difficult to solve. It has a global and diverse impact on institutions, individuals, businesses, and governments. Studies have shown that as technology continues to evolve, criminals use more sophisticated tactics. These factors prompt the government to pay more attention to addressing current and future challenges. The rapid development of cybercrime, which is rooted in traditional crime, reflects the need for policy-making, building a strong legal framework, and strengthening institutions' capacity to effectively combat crime. This new type of crime. The rapid transformation of traditional crime has adapted to exploit the growing technological vulnerabilities in the anonymity and interconnectedness of the modern internet landscape. The results highlight the need for an all-encompassing global strategy for cybersecurity that includes international collaboration, legal changes, and flexible tactics. The diverse responses from various nations illustrate both progress and disparities in addressing this pervasive issue, indicating that while considerable strides have been made, much remains to be done. The wide-ranging impacts of cybercrime—including economic losses, social insecurity, and national stability—further emphasize the urgency for enhanced protective measures and proactive strategies to mitigate risks.

Drawing from the findings of my research, researchers offer the following recommendations:

1) Enhance Legal Frameworks

The government should perform extraordinarily in modernizing the legal framework to address cyber threats more effectively and in a timely manner in the context of rapid change. In this context, the government should create new laws and amend existing laws to keep pace with the evolution of cyber-illegal activities. Nations should consider ratifying international treaties or agreements in line with international standards.

2) Strengthening international collaboration

Given that cybercrime occurs across borders, international cooperation is crucial. To fight cybercrime and offer a coordinated response to cyberthreats, partnerships and exchanges across nations must be formed.

3) Enhance Cybersecurity Education and Awareness

Governments should advance policies to raise awareness of cyber risk to individuals, organizations, and businesses to be able to protect themselves from cyber threats.

4) Leveraging Technology and Innovation

Governments and the private sector should work together to invest in cybersecurity technologies to develop new tools for advanced solutions, including learning machines and artificial intelligence (AI), to anticipate, identify, and respond to cyber threats more successfully.

5) Foster public–private partnerships

Enhancing cybersecurity resilience necessitates public–private cooperation. Governments should collaborate closely with professionals in the business sector to exchange resources, knowledge, and best practices. They should also establish structures that promote cooperation and improve their countries' overall cybersecurity posture.

6) Optimization of Incident Response Mechanisms

Nations should establish and refine incident response protocols and frameworks that enable rapid and efficient handling of cyber incidents.

7) Regular assessments of cybersecurity postures

To determine their efficacy and spot weaknesses, organizations should systematically inspect and analyze their cybersecurity methods. Cybersecurity safeguards must be steadily experienced and updated to settle ahead of evolving threats.

Author Contributions: The authors contributed to the overall preparation, conception, or design of the work or the acquisition, analysis, or interpretation of the data; drafted the work; and substantively revised it.

Funding: This research received no external funding.

Conflicts of interest: The authors declare no conflicts of interest.

Data availability statement: The data used in this research are from public records and, therefore, can be found publicly.

Acknowledgments: The authors extend their heartfelt gratitude to everyone who helped, supported, and guided them in the successful completion of this manuscript. The authors would also like to express sincere appreciation to the lecturers and professors at the Royal University of Law and Economics and the National University of Battambang, for their encouragement and motivation toward professional development and academic publication.

References

Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. *Multidisciplinary Science Journal*, 6, 2024ss0212. https://doi.org/10.31893/multiscience.2024ss0212

Beyer, J. (2015). *The Cybersecurity Information Sharing Act (CISA)*. Jackson School of International Studies. https://jsis.washington.edu/news/the-cybersecurity-information-sharing-act-cisa/

Cassim, F. (2010). Addressing the challenges posed by cybercrime: a South African perspective. *J. Int'l Com. L. & Tech.*, 5, 118. https://international.vlex.com/vid/addressing-posed-cybercrime-perspective-217828625

Chin, K. (2023). The Impact of Cybercrime on the Economy. https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy

Chin, K. (2023). The Impact of Cybercrime on the Economy. https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy

Coll, L. (2022, October 28). What Is Cybercrime? U.S. News & World Report: https://www.usnews.com/360-reviews/privacy/what-is-cybercrime

Europol (202). Common challenges: the equilibrium between security and new technologies https://www.europol.europa.eu/operations-services-and-innovation/digital-challenges

Indonet. (2024). Factors Causing Cyber Crime to Easily Occur. https://indonet.co.id/factors-causing-cyber-crimes-to-easily-occur/

PGI. (2018). What is the difference between cyber-crime and traditional crime? https://www.pgitl.com/insights/what-is-the-difference-between-cyber-crime-and-traditional-crime.

Sam, R., Sieng, E., and Khim, L. (2015). Introduction to Cambodian Legal and Juridical System, *International Law Review*, 7 (1), 331-359, https://kiss.kstudy.com/Detail/Ar?key=3326909

Sara, S. (2016). Cybercrime in the digital age. https://www.slideshare.net/slideshow/cyber-crime-in-the-digital-age/66366993

Tieng, M., Hour, R., Yoeng, H., Vam, P., & Sam, R. (2024). Legal Challenges of Intellectual Property in Southeast Asia: Key Issues and Implications for Cambodia. *Law and Humanities Quarterly Reviews*, 3(2), 27-36. https://doi.org/10.31014/aior.1996.03.02.117

To, J. (2023). Global Cybercrime, https://www.gao.gov/products/gao-23-104768

Vendius, T. T. (2015). Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene. *European Journal of Policing Studies,* 3(2), 151-161. https://researchprofiles.ku.dk/en/publications/europols-cybercrime-centre-ec3-its-agreements-with-third-parties-