social sciences

Article

A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan

Syed Asad Abbas Bokhari

The Center of Security Convergence & eGovernance, Inha University, Incheon 22212, Republic of Korea;
asad.bokhari@inha.edu

Abstract: The phenomenon of law implementation has received limited attention, despite the clear evidence that it is influenced by various factors prevalent in the country, and these factors can have an impact on and obstruct the effective implementation of legislation. The primary objective of this study was to analyze the critical factors that impact the implementation of cybersecurity laws in developing nations, such as Pakistan. The prevalence of corruption, a major hindrance to the implementation of cybersecurity laws and regulations, emerged as the most influential factor in Pakistan. Additionally, factors such as discrimination, illicit conduct, expertise, ambiguity, and public confidence significantly influenced the implementation of cybersecurity laws in Pakistan. A survey was conducted among managers from banking and IT firms to collect data samples on the factors that could potentially impact the implementation of the law. The findings from a sample of 172 respondents revealed that corruption, discrimination, illicit conduct, and ambiguity appeared to have a significant negative influence on cybersecurity law implementation, whereas expertise and public confidence emerged to have a significant positive influence on the implementation of cybersecurity laws in Pakistan. This study suggests that the government of Pakistan should consider various measures such as providing training, improving capacity building, fostering institutional cooperation, strengthening legislative conviction, and promoting global collaborations to enhance the implementation of cybersecurity.

Keywords: cybersecurity law and regulations; implementation; corruption; Pakistan

check for updates

Citation: Bokhari, Syed Asad Abbas. 2023. A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social Sciences* 12: 629. https://doi.org/10.3390/socsci12110629

Academic Editor: Pedro Miguel Alves Ribeiro Correia

Received: 31 August 2023
Revised: 7 November 2023
Accepted: 8 November 2023
Published: 10 November 2023

1. Introduction

The governments and the crucial infrastructure institutions providing important services to nations are continuously under threat today (Bronk and Conklin 2022; Firdous 2018; Slipachuk et al. 2019). Organized hacker organizations, individual hackers, and groups are all targeting these institutions with modern cyberattacks. The frequency, magnitude, and intensity of cyberattacks have boosted over the past decade persistently (Buzdugan and Capatana 2022; Cabaj et al. 2018; Kure et al. 2022). Whenever any nation's security is attacked, the government reacts by enacting legislation to safeguard their assets, shield their citizens, and avoid such assaults from happening in the future. The nations regulate and implement different laws in their jurisdiction appropriate to cybersecurity, incorporating the laws applicable to the monitoring, detecting, preventing, mitigating, and managing such attack threats (Abdullahi et al. 2022; Bokhari and Myeong 2023). Such laws include, for instance, information security laws, intellectual property laws, cybersecurity laws, data protection and e-privacy laws, and confidentiality laws, among others (Kosseff 2017).

Cybersecurity law establishes socio-legal sanctions for cybercrime; categorizes morals of adequate conduct for information and communication technology (ICT) users, guards ICT operators overall, and alleviates and/or avoids harm to data, systems, people, infrastructure, and services in specific; empowers the investigation and trial of criminalities committed online; protects human rights; and facilitates collaboration (UNODC 2013). Cybersecurity law establishes guidelines of standards and comportment of behavior to utilize the computers, Internet, associated digital technologies, the activities of government, public, and private institutions; rules of criminal process and evidence, along with other criminal justice questions in cyberspace; and guidelines to condense risk and/or alleviate the destruction instigated to individuals, institutions, and infrastructure in the occurrence of a cybercrime. Consequently, cybercrime law incorporates substantial, procedural, and preemptive law (Kosseff 2017).

Cybersecurity law contains statutes that ban forms of cybercrime and penalize noncompliance with these statutes. Cybercrime encompasses both real-world (offline), traditional crimes (e.g., fraud, money laundering, organized crime, forgery, and theft) committed in cyberspace as “hybrid” or “cyber-enabled” crimes and “new” or “cyber-dependent” offenses made promising directly by the “Internet” and by “Internet-enabled digital technologies” (Chizanga et al. 2022; Kosseff 2017; Marcacci 2022). As a result of these factors, numerous nations have enacted legislation aimed explicitly at combating cybercrime. To combat cybercrime, the United States, the United Kingdom, Germany, Japan, and China, for example, have revised pertinent portions of their penal codes. Countries have also leveraged existing statutes meant for offline (real-world) crime to pursue specific cybercrimes and cybercriminals (Lim and Taeihagh 2018). In Pakistan, for instance, the existing civil law (Prevention of electric crime act 2016) and Pakistan Penal Code, 1860 (Act, LV of 1860) are utilized to punish real-world crimes such as blackmailing, fraud, identity theft committed via the Internet and digital technologies (Firdous 2018; Ministry of Information Technology & Telecommunication 2021).

In today’s world, having cybersecurity rules and regulations is essential, but putting such laws into action is critical and unavoidable. Policy implementation has been a little-researched process, despite the fact that it has become clearer that the legislative preparation, policy approval, and application procedures may influence and delay potential legislative implementation. Although influencing factors to implement public laws are discussed in previous studies (Awan et al. 2019; Janssen et al. 2020), cybersecurity laws implementation is widely neglected. We tried to explain in this study the pertinent factors that may influence the implementation of cybersecurity laws in different countries positively or negatively. The past presence in the state of mechanisms for interagency planning to implement legislative policies appeared to be the most relevant factor in different nations. Numerous researchers previously depicted the importance of cybersecurity law (Tarter 2017; Veale and Brown 2020) and implementation of cybersecurity law (Azmi 2020; Sattar et al. 2018), and a few have described the important factors that can influence the implantation of cybersecurity laws in different countries (Goel 2020). Our study will explain different elements and factors that influence the implementation of a law positively or negatively in developing economies.

The structure of the study is as follows. Section 2 examines the literature on cybersecurity law, implementation, and influencing factors to lay the groundwork for our theoretical and experimental framework. Section 3 describes the research design, which includes the methods of data collection and analytical measures. Section 4 summarizes the study’s findings. Section 5 provides the discussions, and Section 6 suggests the study’s implications. Finally, Section 7 contains the conclusions.

2. Literature Review

2.1. Technical Cybersecurity

Cybersecurity comprises the dimensions of human, material, and technical elements. An examination of the various components of cybersecurity is mostly crucial in order to resolve problems or develop security strategies. Technical cybersecurity is a separate field that employs a diverse set of capabilities, competence, and knowledge to ensure the safety of individuals, businesses, and their confidential information. This facet of cybersecurity entails employing state-of-the-art technologies and methodologies to evaluate security risks and deficiencies, as well as to counteract attacks. This is achieved through diverse methodologies and the collaboration of a variety of experts. Technical cybersecurity employs ethical espionage as a technique to secure us which is commonly known as penetration testing (Munaiah et al. 2019). Ethical hacking entails the engagement of a penetration tester by a corporation or institution to conduct authorized hacking activities on their networks. By portraying an authentic cyberattack, penetration testers can identify vulnerabilities and weaknesses in security that a hacker might possibly leverage, enabling proactive measures to be implemented in order to eliminate such incidents from occurring in the future (Hawamleh et al. 2020).

Technical cybersecurity positions entail the responsibility of devising strategies and creating security technologies to preserve networks and structures (Ma 2021). They have the ability to formulate strategies to preempt attacks and develop countermeasures in the incident of an attack. Technical professionals must possess knowledge and awareness of the dynamic threat landscape, including emerging weaknesses and malware. Technical cybersecurity experts will analyze the virus's manifestation and design software to defend against or counteract its efficient attack. Comprehending and combating malware is a crucial responsibility in the field of technical cybersecurity (Mohanta and Saldanha 2020). Ultimately, individuals employed in the field of technical cybersecurity are responsible for creating cryptographic systems in order to protect crucial and classified information. Consequently, if networks are compromised and data are pilfered, the confidential information will remain undisclosed according to its encrypted condition. These groups also evaluate encryptions to decrypt them if appropriate.

In essence, technical cybersecurity entails leveraging technology to not only help in the situation of cyberattacks but also to safeguard from and preemptively thwart such attacks. Gaining a comprehensive comprehension of both material and human cybersecurity may highlight the distinct nature of such organizations, while also acknowledging their frequent collaboration in resolving problems.

2.2. Cybersecurity Law

When consulting experts, the prevailing definition of cybersecurity is typically aligned with the official definition provided by the US federal government, which states that it is the proficient protection of computers against unauthorized access or criminal exploitation, as well as the implementation of policies to guarantee the anonymity, credibility, and accessibility of information (Kosseff 2017). The definition provided is insufficient. What constitutes "unauthorized" access, what constitutes "criminal" use, from whom should information be kept "confidential", and who has the authority to determine the integrity and availability of information? Essentially, who has the right to manage which computer? Given our recognition of the significance of cybersecurity law, we have the opportunity to expand cybersecurity avoiding excessive rationalization. Cybersecurity is achieved when the individuals who have the legal authority to control computers and information are the ones who actually possess that control. Cybersecurity issues emerge when there is a mismatch between those who have the ability to control and those who are legally authorized to do so (Goldfoot 2018). A comprehensive awareness of cybersecurity relies on a collective agreement regarding the laws, rules, and policies that establish ownership, authorization, and control. Those rules are legally cybersecurity laws (Appazov 2014).

Cybersecurity is the cumulative application of strategies, security precautions, threat management techniques, training, methodologies, assurance, and competence that may be utilized to protect an information system, an organization, and any associated assets (Möller and Haas 2019). The capacity of an organization to detect and successfully respond to cybersecurity invasions and intrusions, data theft and intellectual property, phishing assaults, and malicious attacks from both inside and outside the network is referred to as cybersecurity readiness (Tran 2016). According to (Richmond 2017), companies should be concerned about whether they are appropriately equipped to identify assaults, immediately notice a breach, efficiently repair, and accurately quantify the harm. Cybersecurity preparedness demonstrates an organization's attitudes, policies, and processes toward risk management, establishing effective cybersecurity controls, teaching staff about cyber hazards, and recognizing and responding to attacks.

To comprehend "cybersecurity law", for legislators, courts, regulators, and commentators to offer solutions to these ongoing threats, a clear definition is required. We present here some definition elements based on our history of dealing with tragedies such as the threats and attacks on various companies and institutions in various countries. This section determines a broad definition of "cybersecurity law." Kosseff (2017) formed the definition by following five questions what, where and whom, how, when, and why to secure? Taking these factors into account, he created a broad and flexible definition that outlines the basic criteria and applicability of cybersecurity law. He did not intend to imply that cybersecurity law should be restricted to a specific set of prerogatives of policy by providing this definition. Instead, it identifies the areas which should be considered as we advance and improve cybersecurity legislation. "Cybersecurity law promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, to protect individual rights and privacy, economic interests, and national security" (Kosseff 2017, p. 1010).

This interpretation of "cybersecurity law" incorporates our modern concept of cybersecurity and identifies the most advanced threats that nations face today. Furthermore, this is just one sample studied on our current national cybersecurity threats, and it makes no substantive policy recommendations for improving cybersecurity. It somewhat characterizes priority sectors of cybersecurity law that are underserved by legislative requirements in various countries. As legislators and courts confront cybersecurity law, it is becoming particularly crucial that they use a prevalent categorization and have a comprehensive understanding of all areas that their legislations, regulations, and judicial rulings should encompass.

Because the government's cybersecurity laws are lenient, people are not precluded from committing crimes. The strict laws are required to instill fear in the minds of prospective criminals so that they know that they will face repercussions if they commit the crime (Gallagher et al. 2015). It is critical to instill fear in the public's mind about any crime, particularly cybercrime, which can be accomplished by enacting harsh punishments. Criminal sanctions do not imply that a person will be appropriately punished for any minor offense, but rather that the conviction must be severe enough that the perpetrator will not intend to commit an offense again, and any prospective offender will be scared by recognizing the repercussions. When punishing an offender, there should always be equilibrium so that it is neither too severe that he must endure beyond what he did, nor too light that he would not worry about having committed it again (Gallagher et al. 2015). Strictly implementing cybersecurity laws can have the effect of discouraging potential offenders, preventing serial offenders, and creating harmony in a community with reduced cyberattacks.

2.3. Implementation of Cybersecurity Law

The law procedure requires an effective implementation framework. Superior implementation is required because no matter how stringent the laws that have been passed by the parliaments, they are useless unless they are implemented properly. The asserted or recommended laws will be of no use unless they are effectively implemented. Police, prison authorities, investigators, and other key players are required for better implementation. The law enforcers are the ones who are tasked with ensuring the public's safety. They are the ones who show up at a criminal investigation and are given the authority to apprehend the perpetrators and bring them before the prosecution. As a result, the security forces must function efficiently to apprehend the attacker as quickly as possible to provide justice to the defendant. Better implementation of cybersecurity policies may grant security and law enforcement agencies more power, instill fear in the community, particularly offenders, and aid in the proper functionality of the judicial process.

The combined effect of stricter legislation and improved implementation is critical. Stringent laws combined with better implementation would produce the desired outcome since neither draconian law nor better implementation could function alone to eliminate offenses from society. The lengthy court procedures in which the defendant seeking retribution for oneself must wait for years cause the victim to lose faith and the suspected to flee. The public is skeptical of such a delayed and tedious process because they understand that if they bring any case to the court, they will not find justice on time. The source of such skepticism is lax legislation and poor implementation. Whenever the prosecutors work efficiently, the judges can reach a decision more quickly, and stringent laws discourage the public from perpetrating future crimes. Both would thus help to prevent crime in the country and develop peace and stability.

Security forces may take a variety of interventions to deliver justice to the people, together with stricter laws and strict enforcement. For instance, a defined time limit can be suggested for discharging cases so that the complainant does not have to struggle more to obtain justice, a fixed punishment can be asserted for the offenses rather than the upper and lower limits provisions, the sanctions can be given according to the seriousness of the offense so that people would not commit those offenses, cases including cybercrimes or any severe cases can allude straightforwardly to the Special Courts for prosecution, and bail should never be granted to severe criminals. Figure 1 displays a step-by-step flowchart of the cybersecurity lawmaking and implementation process in Pakistan.

2.4. Factors Influencing Implementation of Cybersecurity Law

Most of the nation-states have laws and regulations regarding cybersecurity in existence since 2014, with fewer added later on (Burr 2015). For a variety of reasons, effective legislation and regulatory implementation remain a major challenge. Among these is the fact that cybersecurity laws and regulations must pass through several institutions, both public, semi-public, and private. All these institutions have overlapping processes that impede their effective implementation. Because of these overlaps, the country's administration's complicated pyramidal structure, and a lack of cooperation across agencies, the execution of current rules is difficult to observe and deploy in its completeness. Nevertheless, the information sector's rules are the responsibility of numerous authorities, the primary role of which is to "guarantee that the cybersecurity process must be carried out rigorously in compliance with all applicable by-laws." They are generally (but not exclusively) under the supervision of the Ministry of Information Technology. Nonetheless, numerous other ministries, such as the Ministry of Interior and the Ministry of Science, have major powers in the formulation and execution of different policies and instruments in the information technology industry at large (Tene et al. 2017).

It should be noted that collaboration across all ministries in the security process is quite weak. This may be evident at the legislative, administrative, and policy implementation levels, which eventually leads to inadequate execution and implementation of existing laws and regulations (L. J. Bikoko et al. 2019). This position raises additional worries regarding the nature of policy development in the country and in cybersecurity specifically. In this latter sector, it has been seen that cybersecurity breaches and, as a result, the collapse of cybercrime have approached an astonishing rate in recent years (Rasool 2015). These results, as well as policy structures among several ministerial departments, may have contributed to the shortcomings.

Law enforcement is vital in states, thus more demographic knowledge is essential to have a detailed understanding of the elements that might affect law enforcement regionally (Clark 2002). In the past, the state of mechanisms for law implementation development plans appeared to be the most important element in a country. Prior history of federal programs, resource availability, state wealth, or geographic location did not appear to have a substantial impact on policy formation, but there are some indicators that other elements may become relevant in the following stage of legislation implementation, policy acceptance (Harbin et al. 1992). It indicates that several variables such as inadequate resources (Burns et al. 2004), corruption (Polinsky and Shavell 2001), insufficient knowledge, ambiguity about law enforcement (Chopard and Obidzinski 2021), a willingness on the part (Bolger and Walters 2019), and low confidence (Hall 2012) are influencing progress in the application of cybersecurity regulations. These elements are detailed more below.

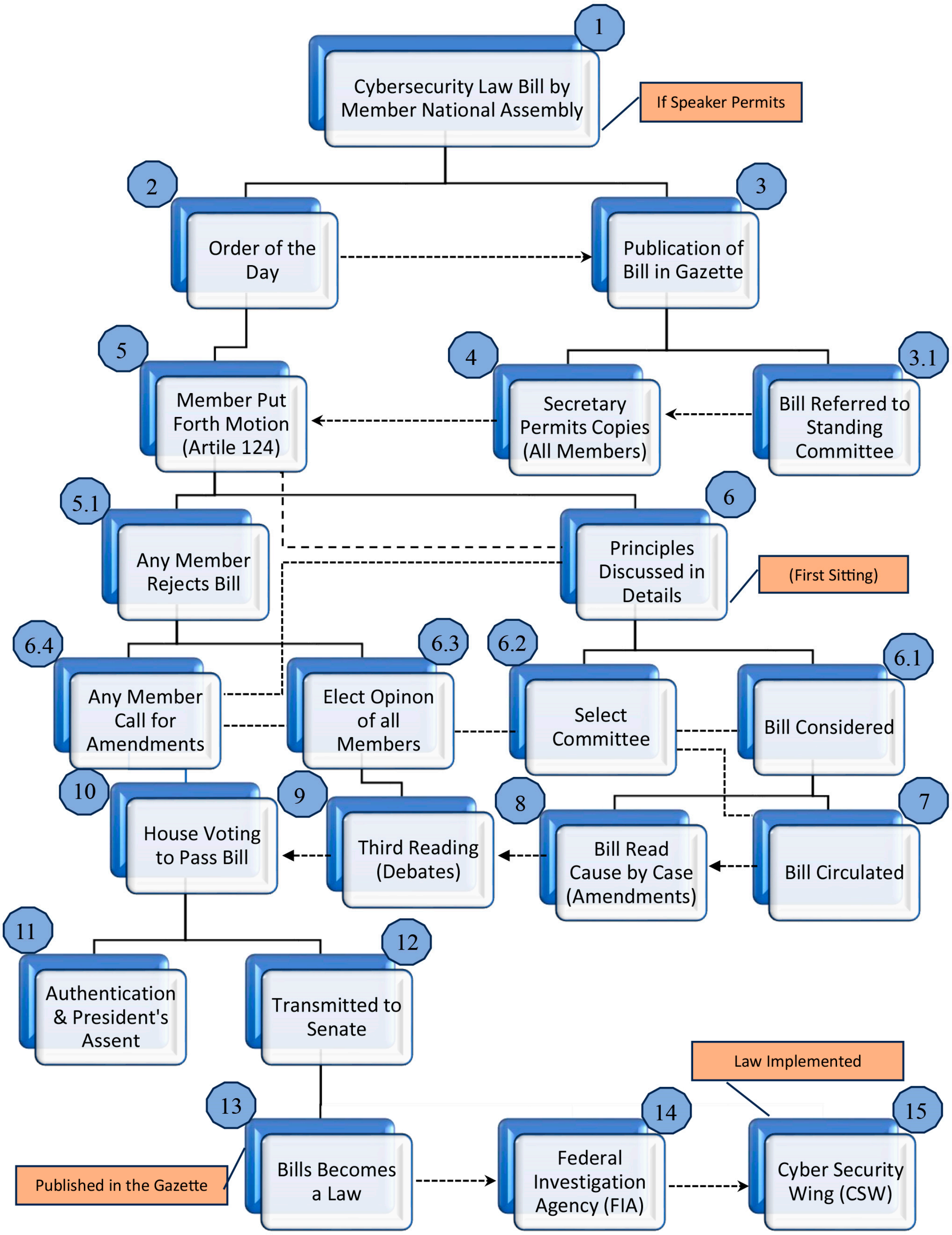
1
Cybersecurity Law Bill by Member National Assembly
If Speaker Permits
2
Order of the Day
3
Publication of Bill in Gazette
5
Member Put Forth Motion (Artile 124)
4
Secretary Permits Copies (All Members)
3.1
Bill Referred to Standing Committee
5.1
Any Member Rejects Bill
6
Principles Discussed in Details
(First Sitting)
6.4
Any Member Call for Amendments
6.3
Elect Opinon of all Members
6.2
Select Committee
6.1
Bill Considered
10
House Voting to Pass Bill
9
Third Reading (Debates)
8
Bill Read Cause by Case (Amendments)
7
Bill Circulated
11
Authentication & President's Assent
12
Transmitted to Senate
Law Implemented
13
Published in the Gazette
Bills Becomes a Law
14
Federal Investigation Agency (FIA)
15
Cyber Security Wing (CSW)

Figure 1. Procedural Flowchart of Cybersecurity Law Implementation.

2.4.1. Corruption and Law Implementation

Law enforcement agencies oversee and implement laws designed to protect those who engage in cybercrime, Internet fraud, and cyberattacks. Corruption makes law enforcement a far less reliable weapon for minimizing and avoiding cybersecurity damages (Kolstad and Søreide 2009; Parker 2019; Robbins 2000). Contributing to the difficulty is the reality that cybercrime is a minor issue for law enforcement agencies in many nations, specifically if they are under-resourced and confront a variety of other challenges to the legal system. Such crimes may even be seen as having no victims (Williams 2019). Corruption is defined as the misuse of delegated power for personal benefit. Bribery and extortion, granting benefits in return for campaign donations, favoritism, and embezzlement, are all forms of corruption.

Corrupt behaviors frequently intersect with cybercrime, and corruption is frequently used as a "door opener" for cybercrime. Bribes or gratuities to support the international or domestic usage of unlawful or unauthorized hacking, ransomware and malware distribution, and denial of service; bribery for a favorable decision or other judicial process manipulation; employing illicit ways to launder the revenues of cybercrime and associated corruption are some instances of cybercrime-related corruption (Williams 2019). Because of the prevalence and influence of corruption, efforts to decrease cybercrime through law enforcement may have unintended or unexpected consequences. This notion is illustrated by two basic approaches in which corruption may weaken law enforcement.

Throughout several historical decades, traditional states engaged in battles against different challenges in order to protect their freedom, territorial boundaries, socioeconomic equilibrium, sustained functioning, and development. In most present-day nations, owing to their elevated levels of development, societies are experiencing novel types of challenges due to the digitalization and swift development of cyber technology consisting of cyberthreats. Therefore, modern nations are obligated to propose efficient governmental policies to combat the aforementioned issues and protect information, preservation of national sovereignty, security, and continued survival in a transformed digital environment. Corruption poses a significant threat to virtual reality, as evidenced by previous studies (Holovkin et al. 2021; Richards and Eboibi 2021). Currently, the progress of the information state relies on the policies made by those in the government, in addition to its socioeconomic and technological aspects. If a country's government involves corruption in the decision-making process across various disciplines, this indicates that corruption poses a significant risk to cybersecurity (Abbas et al. 2021). Its significance is highly substantial because of the global development in informatization and the overall shift from conventional to digital paradigms. As corruption becomes more prevalent, the cybersecurity infrastructures of certain countries and the global world become increasingly susceptible to cyberattacks (Bechara and Schuch 2021; Hauser 2019; Lallie et al. 2021; Suwana and Sardini 2022). We argue that when a country's government is involved in corrupt practices in policy-making processes, it is highly vulnerable to implement those laws. Based on the above discussions, we developed our first hypothesis as follows:

Hypothesis 1. *The higher the perceived corruption in the society, the lower the likelihood of implementation of cybersecurity law.*

A. Discriminatory or Selective Ground-Level Implementation

Corruption can steer implementation toward less powerful entities and relatively low criminal activity. Lower-level offenses, such as traffic infractions or hunting, are not only relatively simple to detect, but they also present possibilities for law enforcement agents to extort bribes due to their superior position of power and influence in the scenario. When bribes are passed up the bureaucratic chain, this generates attractive benefits inside the administration to spend law enforcement resources on initiatives that maximize bribe collection potential. Where there are fewer options for remuneration, there is less motivation to pursue illicit actions. This also means that illicit actors who can afford to pay can avoid arrest or conviction (Williams 2019). In Pakistan, for instance, corruption is contributing to the demise of Pakistan's forest management system and highlighting the weaknesses of traditional anti-corruption reform efforts. The "crime and punishment method" and the "holistic approach" are the most frequently referenced reform strategies in the fight against corruption. The "crime and punishment" strategy necessitates strong enforcement mechanisms, which Pakistan lacks (Chêne 2008; Pellegrini 2011).

Adolescent communities that hold a disadvantageous position in the network of communication and social structures, particularly those who experience multimodal discrimination, are vulnerable to cyberbullying and cyberthreats and often experience negative psychological outcomes. Cyberbullying on the basis of discrimination is a pervasive worldwide social issue (Hong et al. 2018; Peguero and Hong 2020). Cyberbullying can emerge regardless of whether adolescent individuals possess discriminatory characteristics or personalities, although those with such qualities can be more susceptible. Previous studies discovered that discrimination-based cyber harassment tends to include a higher number of attackers, frequent instances, and prolonged periods compared to non-discriminated harassment (Jones et al. 2023; Navarro-Rodríguez et al. 2023). Recently, there has been a growing interest among academics in both conventional bullying and cyberbullying. Due to the absence of cybersecurity laws and of temporal and spatial constraints, cyberbullying can impact more extreme trauma on its victims compared to conventional bullying (Bauman and Yoon 2014). Although discrimination and cyberbullying both arise from a social status asymmetry, it is the government that ensures equality and justice through the implementation of adequate policies in relation to cybersecurity. Additionally, it is worth noting that cyberbullying is primarily prevalent in teenagers (Earnshaw et al. 2018), and the governments neglect this segment of society while making policies. Weinstein et al. highlighted that teenagers may encounter deleterious effects of different kinds when investigating the correlation between perceived discrimination and both offline bullying and cyberbullying (Weinstein et al. 2021). We argue that in cases of significant discrimination among various segments of society, the government of a country is incapable of implementing stringent policies that apply uniformly to all segments. Based on the aforementioned discussion, we proposed our subsequent hypothesis as follows:

Hypothesis 2. *The higher the discrimination in the society, the lower the likelihood of implementation of cybersecurity law.*

B. Involved in the Eradication of Illicit Conduct

Prosecution, juries, and law enforcement personnel can all be influenced by politics or be motivated by corrupt motives. Corruption can lead to less repression of criminal acts, such as during case preparation. In Honduras, for example, state involvement was accused of the destruction of evidence in a lawsuit involving some of the country's top timber corporations (Goncalves et al. 2012). Despite the inability to gather and present important proof that might be attributed to a lack of capacity or inadequate resources, corruption and political meddling are frequently prevalent. Bribe payments to judges, on the other hand, have been shown to influence charge and penalty levels (Williams 2019). Rendering to another research, personnel in Kenya's Forest Service (KFS) have allocated forest areas for forestry and farming in return for unlawful bribes. Attempts to expel forest inhabitants in Kenya's highlands have been regarded as a kind of rent capture and as part of wider historical methods of forced integration. Evacuations also eliminate key witnesses to criminal activity (Cavanagh 2017).

Hypothesis 3. *The higher the illicit conduct of government and law enforcement agencies, the lower the likelihood of implementation of cybersecurity laws.*

2.4.2. Expertise and Law Enforcement

Cybercrime is one of our world's most serious dangers, with far-reaching ramifications for national security, economic strength, and public safety. Investigating a wide range of cybercrimes and cyberthreats perpetrated by cybercriminals, hackers, extremists, and state actors is a problem for the state, regional, local, and territorial law enforcement agencies. To face this problem, cybersecurity law enforcement executives must guarantee that competent agency workers receive cybercrime training to gain skills in preventing cyberattacks or identifying perpetrators for prosecution in the case of such assaults.

With the advancement of technology and the global availability of the Internet, new forms of cybercrime are emerging daily. As per Mike Hulett, the director of operations of the UK's National Cyber Crime Unit, cyber was engaged in almost half of all registered crimes in the UK in 2017. Furthermore, around 68% of significant UK organizations have been the target of cybersecurity breaches or assaults. Law enforcement is having a difficult time keeping up with the surge in cybercriminals' numbers and the innovation of their techniques. Previous research suggests that the methodologies and processes employed by law enforcement in traditional investigations do not always apply in the cyber environment (Brenner 2010; Williams 2008). Consequently, to neutralize these technologically complex crimes, a new process must be adopted, as well as a new set of expertise and skills. This is critical because cybercriminals are typically technologically savvy and are always changing and developing innovative tools to stay one step ahead of law enforcement agencies (Koziarski and Lee 2020; Nurse 2018).

Technological expertise and skills are problems associated with the staff's cyber competencies. In comparison to developed countries, developing countries have a shortage of trained technical experts working on cybercrime investigations. The majority are highly skilled investigators who have previously worked on street crime but are now transitioning to the cyber field due to the growth in cybercrime. Investigators are well versed in obtaining intelligence and investigative techniques, but they may not be as well versed in cyberspace. As a result, there are still unanswered questions about employee expertise and training in emerging countries. Due to the worldwide increase in cybercrime, this is unlikely to be a problem that exclusively affects this geographic area. Further training and expertise for the appropriate staff, as well as the development of technologies that are better suited to supporting user skills and activities, are all possibilities that could be pursued in the future. The ideal situation would be to provide easy-to-use procedures and technologies that would shorten the acquisition time for new cybercrime investigators (Nouh et al. 2019).

Hypothesis 4. *The higher the expertise of law enforcement agencies, the higher the likelihood of implementation of cybersecurity law.*

2.4.3. Ambiguity and Law Enforcement

Individuals are expected to accurately appraise the likelihood of being penalized if they commit an offense under the civil law enforcement framework (Becker 1968). Nonetheless, in real-life scenarios, prospective criminals usually have only a hazy understanding of their chances of being found and perhaps punished. They have beliefs about the likelihood of discovery and may be optimistic or pessimistic. For example, in the context of corporate taxation, taxpayers tend to exaggerate the likelihood of being subjected to an examination by the tax authorities (Slemrod 2019).

Individuals' decisions on whether to respect the law will be influenced by how they assess their chances of being caught. The likelihood of identification and indictment is uncertain, even though potential perpetrators are fully aware of the severity of the penalty. The fundamental reason for this idea is that punishments are frequently stated in sentencing guidelines or criminal legislation, but information concerning the likelihood of discovery cannot be provided. Furthermore, ambiguity about the severity of punishments raises concerns about the concept of equal treatment under the law (General Assembly 2014). Assume Mr. X and Mr. Y perform the same offense under the same conditions. If Mr. X receives a 5-year sentence and Mr. Y receives a 3-year term, the disparity appears to be highly harsh (Chopard and Obidzinski 2021).

Numerous theorists, based on the predicted general law enforcement framework (Polinsky and Shavell 2007), suggest that potential offenders are aware of their chances of identification and prosecution. The purpose here is looking at how uncertainty about this probability affects the standard conclusions about the optimal punishment and the resources that benevolent public law enforcement should expend in investigation and conviction. (Snow 2011) defines ambiguity as "uncertainty regarding probability caused by the omission of crucial and potentially available information." There are various possible models of decision when there is uncertainty. In the context of cybersecurity law enforcement, two social welfare factors (populist and paternalist) are examined and determine the best implementation approach in each situation. The major distinction between the two techniques is whether the law enforcement should consider the disparity between the objective and perceived probability of a fine. Indeed, when people are pessimistic, this disparity may result in a perception bias cost (optimistic). A paternalistic state law enforcer does not consider the difference between the predicted and genuine penalty, but a populist law enforcer does (Williams 2019).

The findings suggest that the level of pessimism of potential criminals be considered when designing deterrent strategies. Consequently, attitudes can have a significant impact on deterrence policy suggestions. Assume that people are pessimistic and overestimate their possibilities of being caught and convicted (Chopard and Obidzinski 2021). It is argued that ideal penalties be reduced for two reasons: penalties may be viewed as expensive transfers if society considers mental anguish, and the perceived likelihood of detection is greater than the factual probability. In terms of the best way to invest in an investigation, the outcomes vary depending on the goal role of the law enforcement. When the law enforcer is populist, it is demonstrated that raising the likelihood and lowering the quantity of the fine may be socially acceptable provided the marginal cost of detection is sufficiently low (Williams 2019). In such a circumstance, the fine is not always the maximum. Furthermore, under certain situations, it is feasible that the resources involved in identification are smaller than in the absence of ambiguity. Despite the weight of the beliefs, the objective likelihood of detection looks to be a less effective deterrent strategy in this situation.

Hypothesis 5. *The lower the ambiguity in cybersecurity law, the higher the likelihood of its implementation.*

2.4.4. Public Confidence and Law Enforcement

In a modern democracy, the study of public confidence regarding law implementation is considered significant since the security forces are thought to exemplify the moral integrity and legitimacy of the state (Vaughn et al. 2001). Citizens' impressions of law enforcement services could act as an indicator of a government's performance in serving public needs and interests in this regard. Additionally, the public's overall attitude toward the authorities (i.e., confidence in the law enforcement, contentment with the authorities, and faith in the system) can influence the prosecutor's social control role through its impact on citizen support and collaboration (Holmes and Goodman 2010; Karakus et al. 2011). Public confidence in law authorities and the effectiveness of law enforcement agencies has been shown to boost citizens' readiness to exercise opportunities to avoid cyberattacks and cybercrimes in society (Gross et al. 2017).

Even though research conducted over the last three decades has revealed that the public at large has favorable perceptions toward the law enforcement agencies (Karakus et al. 2011), differences in citizens' attitudes have been discovered depending on the set of parameters (gender, age, socioeconomic level, civil status), neighborhood quality of life (disorder, fear of crime, neighborhood satisfaction), and interactions with the security forces (Schafer et al. 2003). Nevertheless, it is crucial to highlight that most of the past studies have been conducted in the United States and other English-speaking/developed countries (Benedict et al. 2000), and little is known about public perceptions regarding security services in developing countries (Akhtar et al. 2012; Jackson et al. 2014). The validity of current models and related outcomes clarifying variability in the public's view of law implementation across different ethnicities and contextual factors is thus called into question, as current understanding may be constricted or even subjective because of the near-unique emphasis on the United States and other developed countries. According to the scarce study undertaken in developing nations, for example, the public sees law enforcement less favorably than the populace of wealthy countries. These unfavorable sentiments against the law enforcement agencies can lead to mutual ill will, a lack of respect, chaos, and ineffective law enforcement functioning (Benedict et al. 2000).

Hypothesis 6. *The higher the public confidence in law enforcement agencies, the higher the likelihood of implementation of the law.*

3. Research Methods

3.1. Research Design and Sampling

The data were collected from a survey questionnaire administered on a quasi-random basis to managerial-level personnel employed in various banks and IT companies, applying a correlational approach (all Pakistan-based, private-sector firms in the service rather than the production sector). To safeguard employee privacy, questionnaires were answered and submitted directly to the authors via email and an online questionnaire. Study participants were informed that the study was engaged with how various factors influence the implementation of cybersecurity laws in different countries, specifically in the context of Pakistan's developing economy. The reason behind selecting two sectors, such as banks and IT corporations, was that these sectors are the most vulnerable to cyberthreats and would prefer cybersecurity laws to be implemented.

A total of 1020 questionnaires were delivered, with questionnaire responses acquired from 172 male and female personnel, ages ranging from 22 to 60 years. This corresponds to 16.7%, which is a satisfactory percentage considering the commonly minimal response rates acquired from questionnaire surveys (Baruch and Holtom 2008). The sample included 108 men (63%) and 64 women (37%). Participants functioned in a wide range of departments. This classification is divided into multiple groups, each with a variety of jobs, starting from developers and professionals in the first group to higher-level managers. Table 1 summarizes the individuals' characteristic categories to which the sample belonged.

Table 1. Demographics Characteristics.

Description		N	%
Age			
	22 to 35 years	112	65
	36 to 50 years	55	32
	51 to 60 years	05	03
Gender			
	Male	108	63
	Female	64	37
Sector			
	Banking firms	106	62
	IT firms	66	38
Position			
	Low-level managers/Supervisors	102	59
	Middle-level managers/Operations managers	52	30
	Full managers/Branch managers	18	11

3.2. Variable Assessment

3.2.1. Corruption

Corruption was measured in this study using five scales: bribery at the government official level, anti-corruption department authority, corruption risk assessment by the government, anti-corruption training programs, and anti-corruption audit programs in public departments (Bokhari 2022).

3.2.2. Discrimination

The variable discrimination is defined in this study as the unfair or deceptive exploitation of groups and individuals depending on attributes such as ethnicity, race, religion, or sexual preference. This variable was adapted from Clark et al. (Clark et al. 2004), using five scales such as being regarded with less decency, receiving terrible services, having been intimidated or humiliated, being handled with disrespect and deception, and being convicted with injustice.

3.2.3. Illicit Conduct

Illicit behaviors are deemed insensitive or socially unacceptable; activities might not always be unlawful but, nevertheless, violate societal values and norms. Illicit conduct in this study is adapted using five items such as lack of awareness of legal requirements, lack of intelligence in a specific profession, numerous breaches of law, promoting any fraudulent activity or crime, and use of brutal or barbaric behavior (Tremblay 2018).

3.2.4. Expertise

Expertise is commonly described as an exceptional, elite, or extraordinarily high degree of competency in a specific function or subject. To measure this variable, we utilized five components such as the extent of decision-making capability, level of anger management, institutional loyalty, cognition of responsibility, and intensity of analytical thinking, which were adapted from (Ohanian 1990).

3.2.5. Ambiguity

When the connotation, expression, or statement is unclear, ambiguity emerges, and there might be more than one interpretation. Ambiguity in this study is defined as the perception of criminals usually having only a vague understanding of their chances of being observed and perhaps punished by law enforcement institutions. This variable was constructed using five elements adapted from (Calford and DeAngelo 2022). Those elements were uncertain protective remedies against illegal activities, anxiety whenever anything unprecedented occurs, managing a fragmented endeavor, continuing going forward in a hazardous or confusing scenario, and making decisions in the context of uncertainty.

3.2.6. Public Confidence

Maintaining public confidence is fundamental for every law to be capable of protecting the community. Because the general population is a significant source of information, public confidence and collaboration are frequently essential to law enforcement. Public confidence in the state legislative assembly, confidence in the country's constitution, faith in the state's law enforcement agencies, trust in the country's politicians, and confidence in the country's judicial system were the components adapted (Hooghe and Kern 2015) to measure the public confidence construct.

3.2.7. Implementation of Cybersecurity Law

Five elements were applied to measure the implementation of cybersecurity law, and they were adapted from (Rafiq 2019), such as the availability of cybersecurity rules and regulations, the audience's role in implantation, the development of effective legislation, safeguarding them in place of the nation, and synthesizing before stratification.

3.3. Research Analysis

To examine our hypotheses and interpret the outcomes, we employed IBM SPSS 23. The hypothesized research framework for this study is given in Figure 2, where corruption, discrimination, illicit conduct, and ambiguity are negatively impacting whether expertise and public confidence are positively influencing the independent variables on implementation of cybersecurity law, the dependent variable. We will resume interpreting the results of our hypotheses investigation in the following section. The measuring model's reliability and validity were examined initially. Following that, the hypotheses were examined by applying linear regression and robust standard errors. Figure 3 presents a comprehensive roadmap to test the hypotheses developed in this study.

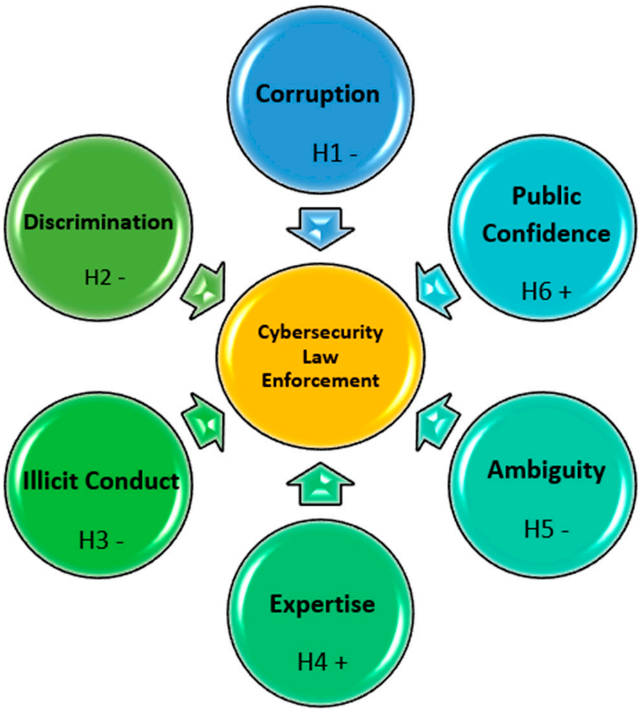

Figure 2. Research Framework.

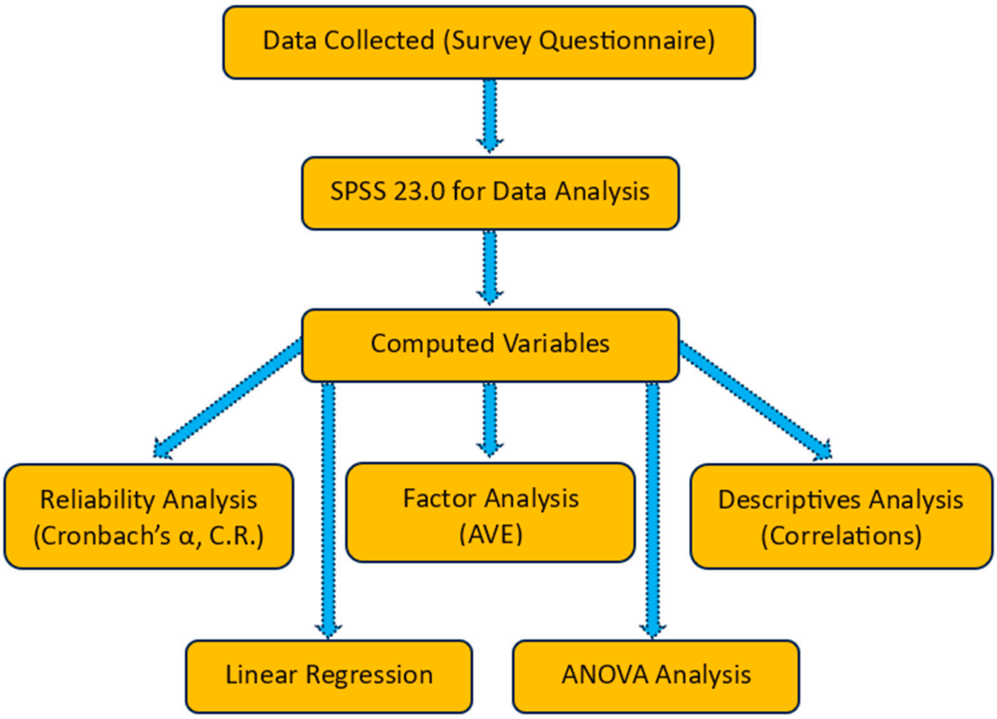
Data Collected (Survey Questionnaire)
SPSS 23.0 for Data Analysis
Computed Variables
Reliability Analysis (Cronbach's α, C.R.)
Factor Analysis (AVE)
Descriptives Analysis (Correlations)
Linear Regression
ANOVA Analysis

Figure 3. Roadmap to Test Hypotheses.

4. Findings

4.1. Reliability and Validity Findings

Table 2 shows how the reliability analysis and discriminant validity of the instrument's models were evaluated before putting them to the examination. Composite reliability (CR) is an indicator of internal consistency. The composite reliability test results demonstrate that all elements have ratings larger than the widely accepted criteria of 0.7 (Abdillah and Hartono 2015). CR, Cronbach's alpha, and AVE were all examined in the convergent reliability analysis. To start, all the substances exhibit statistical significance in Cronbach's alpha. This result indicated that all elements linked to their components confirm the hypothesized association between the indicators and the substances. Secondly, the average variance extracted (AVE) values in all research models exceeded the 0.50 cut-off threshold (Abdillah and Hartono 2015). Therefore, it indicated that the provided indicators may be used using all of the convergent validity factors.

Table 2. Construct Reliability with Cronbach's Alpha, Composite Reliability, and AVE.

	N	Cronbach's Alpha	CR	AVE
		Overall Cronbach's Alpha = 0.979		
Corruption	5	0.817	0.882	0.600
Ambiguity	5	0.894	0.927	0.719
Discrimination	5	0.915	0.939	0.757
Illicit Conduct	5	0.968	0.976	0.890
Public Confidence	5	0.842	0.888	0.615
Expertise	5	0.741	0.921	0.795
Cyber Law Implementation	5	0.823	0.894	0.764

The discriminant validity experiment was conducted to investigate how widely the variables differ. To show construct validity, the AVE of the component should be greater than the variation explained by that item and all other items in the model (Abdillah and Hartono 2015). This condition was generated by all components in this investigation; especially, the diagonal entries (AVEs) in Table 2 are larger than the corresponding components. In sum, the modeling analyses exhibited promising support for the validity and reliability of the effective implementation of the constructs.

4.2. Hypotheses Testing

Table 3 shows the values of mean, standard deviations, and correlation matrix for cybersecurity law implementation, corruption, discrimination, illicit conduct, expertise, ambiguity, and public confidence. The matrix demonstrated a strong correlation between the independent variables (corruption, discrimination, illicit conduct, expertise, ambiguity, and public confidence) and the dependent variable (i.e., cybersecurity law implementation). These observations indicate and validate the researchers' concerns for the interconnection of cybersecurity law implementation, corruption, discrimination, illicit conduct, expertise, ambiguity, and public confidence. All correlation coefficients are in the indicated patterns, implying that assumptions such as cybersecurity law implementation being connected to corruption (r = −0.449, $p < 0.01$), discrimination (r = −0.626, $p < 0.01$), illicit conduct (r = −0.573, $p < 0.01$), expertise (r = 0.712, $p < 0.01$), ambiguity (r = −0.668, $p < 0.01$), and public confidence (r = 0.624, $p < 0.01$) should be examined further (Bokhari and Myeong 2022).

Table 4 presents the empirical outcomes of a univariate analysis of variance performed with ANOVA. The one-way ANOVA should be used when there are three or more groups and only one independent variable and one dependent variable. Because there are six independent variables in this study, the univariate analysis of variance is incorporated into a two-way ANOVA. In this method, the interactivity of the endogenous variables, including the overall influences of the factors, should be studied. Because of the complexities, prior scholars suggested avoiding using beyond three attributes. Table 4 illustrates the F-model value, which is 355.738, and the *p*-value is less than 0.01, indicating that our argument is correct and that the relationships are substantial.

Table 3. Statistical Descriptive, Mean, Standard Deviation, and Pearson Correlations.

	N	M	SD	Gen	Age	Pos	CLI	COR	PC	EXP	DIS	IC
Gen	172	1.343	0.476	1								
Age	172	2.256	0.438	0.054	1							
Pos	172	3.401	0.492	0.258 **	0.472 **	1						
CLI	172	3.68	0.501	0.052	0.038 *	0.034 *	1					
COR	172	3.787	0.645	−0.075	−0.076	−0.021	−0.449 **	1				
PC	172	3.809	0.778	0.029 *	0.045 *	0.034 *	0.624 **	0.887 **	1			
EXP	172	4.053	0.826	0.060	0.035 *	0.007 **	0.712 **	0.879 **	0.959 **	1		
DIS	172	0.901	1.009	0.027 *	−0.054	−0.14 *	−0.626 **	0.846 **	0.957 **	0.977 **	1	
IC	172	3.958	0.673	0.052	0.035 *	0.006 **	−0.573 **	0.908 **	0.920 **	0.923 **	0.890 **	1
AMB	172	3.857	0.667	−0.030 *	−0.074	0.042 *	−0.668 **	0.881 **	0.906 **	0.925 **	0.933 **	0.869 **

**. Correlation is significant at the 0.01 level (2-tailed). *. Correlation is significant at the 0.05 level (2-tailed). Note: M = Mean; SD = Standard Deviation; Gen = Gender; Pos = Position; CLI = Cybersecurity Implementation; COR = Corruption; PC = Public Confidence; Exp = Expertise; DIS = Disinformation; IC = Illicit Conduct; AMB = Ambiguity.

Table 4. ANOVA Test.

ANOVA ^{a}						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1994.493	9	221.610	355.738	0.000 ^{b}
	Residual	100.920	162	0.623		
	Total	2095.413	171			

^{a} Dependent Variable: CL_Implem. ^{b} Predictors: (Constant), Ambiguity, Gen, Age, Pos, Ill_Conduct, Corruption, P_Conf, Expertise, Discrimination.

The outcomes in Table 5 reveal that corruption had a highly negative direct influence on cybersecurity law implementation, with a path coefficient (β = −7.361; t-value = −27.429; $p \leq 0.000$). This result indicated that hypothesis 1 is highly substantiated. Hypothesis 2 indicated a substantial negative relationship between discrimination and cybersecurity law implementation, as postulated, with a path coefficient (β = −10.434; t-value = −29.575; $p \leq 0.000$). Hypothesis 3 substantiated the predicted causal link between illicit conduct and with a path coefficient (β = −0.974; t-value = −3.331; $p \leq 0.000$). Hypothesis 4 suggested that expertise has a positive influence on cybersecurity law implementation, and outcomes revealed a substantial positive relationship between these two constructs with a path coefficient (β = 14.019; t-value = 33.164; $p \leq 0.000$), demonstrating that H4 is substantiated. Hypothesis 5 anticipated a strong inverse relationship between ambiguity and cybersecurity law implementation. The outcomes substantially supported our prediction, with a path coefficient (β = −6.725; t-value = 23.041; $p \leq 0.000$) confirming support for H5. Finally, Hypothesis 6 anticipated a substantial relationship between public confidence and cybersecurity law implementation. The result substantially supports our prediction, with a path coefficient (β = 2.428; t-value = 7.293; $p \leq 0.000$) confirming H6. The research framework analyzed the square multiple correlation (R2) coefficients for latent variables to examine the variance of the latent constructs. The structural model correlations (R2) findings in Table 5 indicate that the proposed model reflected statistically substantial variance for the outcome variable (Tewamba et al. 2019).

Table 5. Hypothesis Testing using Linear Regression for Independent and Dependent Variables.

Coefficients					
Model	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
	B	**Std. Error**	**Beta**		
(Constant)	−7.198	0.705		−10.214	0.000
Gen	−0.086	0.133	−0.012	−0.643	0.521
Age	−0.029	0.159	−0.004	−0.184	0.854
Position	0.111	0.146	0.016	0.763	0.447
Corruption	−7.361 **	0.268	−1.357	−27.429	0.000
Public Confidence	2.428 **	0.333	0.540	7.293	0.000
Expertise	14.019 **	0.423	3.307	33.164	0.000
Discrimination	−10.434 **	0.353	−3.007	−29.575	0.000
Illicit Conduct	−0.947 **	0.284	−0.182	−3.331	0.001
Ambiguity	−6.725 **	0.292	1.282	23.041	0.000

Model Summary			
R	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
0.976	0.952	0.949	0.7893

Dependent Variable: Cybersecurity Law Implementation. **. Correlation is significant at the 0.01 level (2-tailed).

5. Discussion

There are significant serious cyber hazards to Pakistan's state sovereignty, and without the security of certain challenges, comprehensive cybersecurity is unlikely to be attained. Several securitized initiatives were launched by government entities during the last decades; however, most were unsuccessful. The inappropriate media narrative of cybersecurity policies, the scarcity of appropriate authorities, broad-scope security discussions, conventional security mindset, and public exclusion are the key obstacles to effective cybersecurity implementation in Pakistan. The digital media network and authoritative cybersecurity perspectives might contribute to achieving intersubjective consensus amongst essential players. The unification of such an interpretive consensus with the discourse actions could alleviate difficulties concerning the public's involvement. Moreover, identifying the significant associations, stagnating players, and elements in the armed services, economical, geopolitical, and social dimensions that construct the security risk matrices working in the cyber world is crucial. Rather than the rigorous and conventional laws of the existing security cultures, cybersecurity threats must be addressed with an advanced and efficient series of standards (Rafiq 2019).

The primary goal of this research was to identify the critical factors that may influence the implementation of cybersecurity laws in developing economies such as Pakistan. This study found a substantial negative association between corruption and cybersecurity law implementation ($r = -0.449$, $p \leq 0.01$), discrimination and cybersecurity law implementation ($r = -0.626$, $p \leq 0.01$), illicit conduct and cybersecurity law implementation ($r = -0.573$, $p \leq 0.01$), and ambiguity and cybersecurity law implementation ($r = -0.668$, $p \leq 0.01$). Furthermore, the statistical results demonstrated a significant positive relationship between expertise and cybersecurity legislation implementation ($r = 0.712$, $p \leq 0.01$) and public confidence and cybersecurity law implementation ($r = 0.624$, $p \leq 0.01$). As a result, all hypotheses 1 through 6 were significantly supported.

These findings suggested that ambiguity in law and regulations, the illegal actions of attackers who understand they could be sheltered by bribing officials, discrimination in the society, and corruption in government institutions are among the most significant factors that could have a deleterious influence on the implementation of cybersecurity laws in Pakistan. For cybersecurity laws in Pakistan to have a stronger impact, the government must attempt to clarify existing laws, reduce institutional corruption, and eliminate discrimination. However, the implementation of cybersecurity laws in developing economies is hampered by problems regarding the staff's technological expertise and cyber competencies.

The public's trust in the security forces is also deemed crucial to the success of cybersecurity law enforcement because of the high esteem in which they are held as symbols of the state's moral rectitude and legal authority. While the public shows faith in the state's security forces, Pakistan's new cybersecurity law may be implemented overwhelmingly. The findings of this study are generalizable to other countries, particularly those in Asia, because of the similarities between them in terms of corruption, staff expertise, public confidence, and discrimination.

6. Implications

This study may have the following implications for the government to adopt to strengthen cybersecurity implementation in Pakistan:

Training, capacity building, and institutional cooperation: The findings of this study suggest that apprenticeships and workshops for improving cybersecurity competencies ought to be coordinated with the National Center for Cyber Security to strengthen the technological skills of personnel. Personnel orientation on the relevance of cybersecurity should be conducted to enhance knowledge of precautionary measures for preventing cybercrime. Pakistan's law enforcement agencies have collaborated with several highly experienced entities in the information technology sector, such as FIA and NADRA, to strengthen HR professionals' capacity to cope with cybersecurity and hazards. Furthermore, undoubtedly civil–military collaboration in cybersecurity is essential, and it is essential to guarantee that the civil–military institutions set their rivalry aside. Assuming that governmental prejudices are eliminated, essential cybersecurity synergies might be achieved (Anwar and Yamin 2021).

Legislative conviction: The outcomes of this study suggested that corruption, illicit conduct of attackers, and ambiguity in laws impact law implementation adversely. While a cybercrime is committed, there must be a legislative conviction from the courts. Emergence in the field of cybersecurity refers to the availability of a cybersecurity memorandum that can be used as a standard against which all actions taken in the name of information security can be measured. The implementation of cybersecurity programs and strategies should be aligned with the government's national initiative to promote internal cybersecurity ecology. The national strategies involve both operational and regulatory measures, such as organizational operating standards, institutions managing cybersecurity, HR capacity building, and endeavors to strengthen global collaboration. Furthermore, the anti-corruption department should take strong measures to prohibit unethical conduct that can jeopardize the implementation of cybersecurity laws and increase cyber hazards.

Global collaborations: Globalization with states and international institutions is also crucial to confronting cybercrimes. Pakistan has collaborated with China to counter cybercrime for not only political and regional stability but also many other interests. Considering those ambitions, Pakistan and China's determination to develop cooperation through the "China Pakistan Economic Corridor" (CPEC) suggests that it is fulfilling the strategic milestone of establishing a foundation in cybercrime deterrence and economic expansion (Chang and Khan 2019). Table 6 provides the comparison of results with efficacy to prove the efficiency of the proposed method of this study.

Table 6. Comparison to Prove the Efficiency of the Proposed Method.

	Effect	Efficacy	Method
COR → CSLI	Negative	Control Corruption	Accountability
DISC → CSLI	Negative	Equality for Human Rights	Judicial System
ICON → CSLI	Negative	Improve Transparency	Legislative Conviction
EXP → CSLI	Positive	Further IT Expertise	Capacity Building
AMBG → CSLI	Negative	Clear Laws Interpretation	Justice System
PUCO → CSLI	Positive	Strengthen Confidence	Institutional Cooperation

7. Conclusions

Pakistan already has several cybersecurity regulations in place; nonetheless, the composition of those rules is generic. Therefore, cybersecurity implementation has indeed been ineffective. The government needs to make them comprehensive and continually disseminate them among all stakeholders to make them effective. Additionally, to prevent future cyberattacks, law enforcement agencies must take cybersecurity implementation more effectively and seriously. Countries in the region, such as China and India, have already implemented appropriate cybersecurity measures in response to possible threats. In contrast, Pakistan still does not have a specialized institution other than the federal investigation agency (FIA) with complete jurisdiction to monitor and cope with cyberattacks. Moreover, in the emergence of a separate agency, the government must designate one of its bodies or institutions as a leading force. This demonstrates that cybersecurity implementation is decentralized and that the government's participation in cybersecurity is negligible. People desire to breach guidelines, infringe laws and rules, or take possession of cybersecurity as well as tangible systems to acquire monetary or nonmonetary gains. Consequently, the government must work together to accurately predict cyberthreats and attacks to keep Pakistani cybersecurity from becoming a victim of unscrupulous individuals.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The author declares no conflict of interest.

References

Abbas, Hafiz Syed Mohsin, Zahid Hussain Qaisar, Xiaodong Xu, and Chunxia Sun. 2021. Nexus of E-government, cybersecurity and corruption on public service (PSS) sustainability in Asian economies using fixed-effect and random forest algorithm. *Online Information Review* 46: 754–70. [CrossRef]

Abdillah, Willy, and Jogiyanto Hartono. 2015. Partial Least Square (PLS): Alternatif structural equation modeling (SEM) dalam penelitian bisnis. *Yogyakarta: Penerbit Andi* 22: 103–50.

Abdullahi, Mujaheed, Yahia Baashar, Hitham Alhussian, Ayed Alwadain, Norshakirah Aziz, Luiz Fernando Capretz, and Said Jadid Abdulkadir. 2022. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics* 11: 198. [CrossRef]

Akhtar, Aisha, Sadaf Rafiq, Ali Asif, Arshia Saeed, and Muhammad Kashif. 2012. Public perceptions of police service quality: Empirical evidence from Pakistan. *International Journal of Police Science & Management* 14: 97–106.

Anwar, Syeda Sundus, and Tughral Yamin. 2021. Civil Military Cooperation (CIMIC) in Cyber Security Domain: Analyzing Pakistan's Prospects. *Global Strategic & Security Studies Review* VI: 68–81. [CrossRef]

Appazov, Artur. 2014. Legal Aspects of Cybersecurity. University of Copenhagen, pp. 38–42. Available online: https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf (accessed on 14 April 2023).

Awan, Jawad Hussain, Shahzad Memon, and Fateh Muhammad Burfat. 2019. Role of Cyber Law and Mitigation Strategies in Perspective of Pakistan to Cope Cyber Threats. *International Journal of Cyber Warfare and Terrorism (IJCWT)* 9: 29–38. [CrossRef]

Azmi, Rama Halim Nur. 2020. Indonesian Cyber Law Formulation in The Development Of National Laws In 4.0 Era. *Lex Scientia Law Review* 4: 46–58.

Baruch, Yehuda, and Brooks C Holtom. 2008. Survey response rate levels and trends in organizational research. *Human Relations* 61: 1139–60. [CrossRef]

Bauman, Sheri, and Jina Yoon. 2014. *This Issue: Theories of Bullying and Cyberbullying*. London: Taylor & Francis, pp. 253–56.

Bechara, Fabio Ramazzini, and Samara Bueno Schuch. 2021. Cybersecurity and global regulatory challenges. *Journal of Financial Crime* 28: 359–74. [CrossRef]

Becker, Gary S. 1968. Crime and punishment: An economic approach. In *The Economic Dimensions of Crime*. Berlin/Heidelberg: Springer, pp. 13–68.

Benedict, Wm Reed, Ben Brown, and Douglas J. Bower. 2000. Perceptions of the police and fear of crime in a rural setting: Utility of a geographically focused survey for police services, planning, and assessment. *Criminal Justice Policy Review* 11: 275–98. [CrossRef]

Bokhari, Syed Asad Abbas. 2022. An Empirical Examination of the Impact of Initial Capital, Prior Experience, and R&D on SMEs' Survival and Economic Performance: Moderating Role of Innovation Culture. *Journal of Small Business Strategy* 32: 112–25.

Bokhari, Syed Asad Abbas, and Seunghwan Myeong. 2022. Use of artificial intelligence in smart cities for smart decision-making: A social innovation perspective. *Sustainability* 14: 620. [CrossRef]

Bokhari, Syed Asad Abbas, and Seunghwan Myeong. 2023. The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective. *IEEE Access* 11: 69783–97. [CrossRef]

Bolger, P. Colin, and Glenn D. Walters. 2019. The relationship between police procedural justice, police legitimacy, and people's willingness to cooperate with law enforcement: A meta-analysis. *Journal of Criminal Justice* 60: 93–99. [CrossRef]

Brenner, Susan W. 2010. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: ABC-CLIO.

Bronk, Chris, and Wm Arthur Conklin. 2022. Who's in charge and how does it work? US cybersecurity of critical infrastructure. *Journal of Cyber Policy* 7: 155–74. [CrossRef]

Burns, Ronald G., Keith H. Whitworth, and Carol Y. Thompson. 2004. Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice* 32: 477–93. [CrossRef]

Burr, R. 2015. To Improve Cybersecurity in the United States through Enhanced Sharing of Information about Cybersecurity Threats, and for Other Purposes. Paper presented at the 114th United States Congress, Washington, DC, USA, July 6.

Buzdugan, Aurelian, and Gheorghe Capatana. 2022. Cyber security maturity model for critical infrastructures. In *Education, Research and Business Technologies: Proceedings of 20th International Conference on Informatics in Economy (IE 2021)*. Hanover: Springer Nature.

Cabaj, Krzysztof, Luca Caviglione, Wojciech Mazurczyk, Steffen Wendzel, Alan Woodward, and Sebastian Zander. 2018. The new threats of information hiding: The road ahead. *IT Professional* 20: 31–39. [CrossRef]

Calford, Evan M., and Gregory DeAngelo. 2022. Ambiguity and enforcement. *Experimental Economics* 26: 1–35. [CrossRef]

Cavanagh, Connor Joseph. 2017. Mapping the state's Janus face: Green economy and the 'green resource curse' in Kenya's highland forests. In *Corruption, Natural Resources and Development*. Cheltenham: Edward Elgar Publishing.

Chang, Yen-Chiang, and Mehran Idris Khan. 2019. China–Pakistan economic corridor and maritime security collaboration: A growing bilateral interests. *Maritime Business Review* 4: 217–35. [CrossRef]

Chêne, Marie. 2008. Overview of corruption in Pakistan. *Transparency International*, 1–13. Available online: https://www.u4.no/publications/overview-of-corruption-in-pakistan (accessed on 7 November 2023).

Chizanga, Merrilyn, J. Agola, and Anthony Rodrigues. 2022. Factors Affecting Cyber Security Awareness in Combating Cyber Crime in Kenyan Public Universities. *International Research Journal of Innovations in Engineering and Technology* 6: 54–57. [CrossRef]

Chopard, Bertrand, and Marie Obidzinski. 2021. Public law enforcement under ambiguity. *International Review of Law and Economics* 66: 105977. [CrossRef]

Clark, Gordon. 2002. *The Geography of Law*. London: Routledge.

Clark, Rodney, Apollonia P. Coleman, and Jeremy D. Novak. 2004. Brief report: Initial psychometric properties of the everyday discrimination scale in black adolescents. *Journal of Adolescence* 27: 363–68. [CrossRef] [PubMed]

Earnshaw, Valerie A., Sari L. Reisner, David D. Menino, V. Paul Poteat, Laura M. Bogart, Tia N. Barnes, and Mark A. Schuster. 2018. Stigma-based bullying interventions: A systematic review. *Developmental Review* 48: 178–200. [CrossRef] [PubMed]

Firdous, Ms Afeera. 2018. Formulation of Pakistan's Cyber Security Policy. *CISS Insight Journal* 6: 70–94.

Gallagher, Mary, John Giles, Albert Park, and Meiyan Wang. 2015. China's 2008 Labor Contract Law: Implementation and implications for China's workers. *Human Relations* 68: 197–235. [CrossRef]

General Assembly. 2014. Universal Declaration of Human Rights, 1948, Article 15. Available online: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf (accessed on 12 April 2023).

Goel, Sanjay. 2020. National cyber security strategy and the emergence of strong digital borders. *Connections* 19: 73–86. [CrossRef]

Goldfoot, Josh A. 2018. The Pen-Trap Statute and the Internet. *Virginia Journal of Criminal Law* 6: 1.

Goncalves, Marilyne Pereira, Melissa Panjer, Theodore S. Greenberg, and William B Magrath. 2012. *Justice for Forests: Improving Criminal Justice Efforts to Combat Illegal Logging*. Washington, DC: World Bank Publications.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. 2017. Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity* 3: 49–58. [CrossRef]

Hall, Nathan. 2012. Policing hate crime in London and New York City: Some reflections on the factors influencing effective law enforcement, service provision and public trust and confidence. *International Review of Victimology* 18: 73–87. [CrossRef]

Harbin, Gloria, James J. Gallagher, Timothy Lillie, and Jane Eckland. 1992. Factors influencing state progress in the implementation of Public Law 99-457, Part H. *Policy Sciences* 25: 103–15. [CrossRef]

Hauser, Christian. 2019. Fighting against corruption: Does anti-corruption training make any difference? *Journal of Business Ethics* 159: 281–99. [CrossRef]

Hawamleh, A., Almuhannad Sulaiman M. Alorfi, Jassim Ahmad Al-Gasawneh, and Ghada Al-Rawashdeh. 2020. Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology* 63: 7894–99.

Holmes, Erin J., and Doug Goodman. 2010. African-American and White Perception of Police Services: The Impact of Diversity on Citizens' Attitudes toward Police Services. *Journal of Public Management & Social Policy* 16: 3–18.

Holovkin, Bohdan M., Oleksii V. Tavolzhanskyi, and Oleksandr V. Lysodyed. 2021. Corruption as a cybersecurity threat in conditions of the new world's order. *Linguistics and Culture Review* 5: 499–512. [CrossRef]

Hong, Jun Sung, Anthony A. Peguero, and Dorothy L. Espelage. 2018. Experiences in bullying and/or peer victimization of vulnerable, marginalized, and oppressed children and adolescents: An introduction to the special issue. *American Journal of Orthopsychiatry* 88: 399. [CrossRef]

Hooghe, Marc, and Anna Kern. 2015. Party membership and closeness and the development of trust in political institutions: An analysis of the European Social Survey, 2002–2010. *Party Politics* 21: 944–56. [CrossRef]

Jackson, Jonathan, Muhammad Asif, Ben Bradford, and Muhammad Zakria Zakar. 2014. Corruption and police legitimacy in Lahore, Pakistan. *British Journal of Criminology* 54: 1067–88. [CrossRef]

Janssen, Marijn, Vishanth Weerakkody, Elvira Ismagilova, Uthayasankar Sivarajah, and Zahir Irani. 2020. A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. *International Journal of Information Management* 50: 302–9. [CrossRef]

Jones, Lisa M., Anna Segura Montagut, Kimberly J. Mitchell, Heather A. Turner, Sherry Hamby, and Carlos A. Cuevas. 2023. Youth bias-based victimization: Comparing online only, in-person only, and mixed online/in-person incidents. *International Journal of Bullying Prevention*, 1–13. [CrossRef]

Karakus, Onder, Edmund F. McGarrell, and Oguzhan Basibuyuk. 2011. Public satisfaction with law enforcement in Turkey. *Policing: An International Journal of Police Strategies & Management* 34: 304–25.

Kolstad, Ivar, and Tina Søreide. 2009. Corruption in natural resource management: Implications for policy makers. *Resources Policy* 34: 214–26. [CrossRef]

Kosseff, Jeff. 2017. Defining cybersecurity law. *Iowa Law Review* 103: 985.

Koziarski, Jacek, and Jin Ree Lee. 2020. Connecting evidence-based policing and cybercrime. *Policing: An International Journal* 43: 198–211. [CrossRef]

Kure, Halima Ibrahim, Shareeful Islam, and Haralambos Mouratidis. 2022. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications* 34: 15241–71. [CrossRef]

L. J. Bikoko, Théodore Gautier, Jean Claude Tchamba, and Felix Ndubisi Okonta. 2019. A comprehensive review of failure and collapse of buildings/structures. *International Journal of Civil Engineering and Technology* 10: 187–98.

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security* 105: 102248.

Lim, Hazel Si Min, and Araz Taeihagh. 2018. Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. *Energies* 11: 1062. [CrossRef]

Ma, Chen. 2021. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports* 7: 7999–8012. [CrossRef]

Marcacci, Antonio. 2022. *Transnational Securities Regulation: How It Works, Who Shapes It*. Berlin/Heidelberg: Springer Nature, vol. 3.

Ministry of Information Technology & Telecommunication. 2021. *National CYBER Security Policy 2021*; Islamabad: Government of Pakistan. Available online: https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf (accessed on 26 May 2023).

Mohanta, Abhijit, and Anoop Saldanha. 2020. *Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware*. Berlin/Heidelberg: Springer.

Möller, Dietmar P. F., and Roland E. Haas. 2019. *Guide to Automotive Connectivity and Cybersecurity*. Berlin/Heidelberg: Springer.

Munaiah, Nuthan, Akond Rahman, Justin Pelletier, Laurie Williams, and Andrew Meneely. 2019. Characterizing attacker behavior in a cybersecurity penetration testing competition. Paper presented at the 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Recife, Brazil, September 19–20.

Navarro-Rodríguez, Christián Denisse, Jose A. Vera Noriega, and Sheri Bauman. 2023. Bias-Based Cyberaggression in Northwestern Mexican Adolescents: Associations With Moral Disengagement. *The Journal of Early Adolescence* 43: 110–35. [CrossRef]

Nouh, Mariam, Jason R. C. Nurse, Helena Webb, and Michael Goldsmith. 2019. Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement. *arXiv* arXiv:1902.06961.

Nurse, Jason R. C. 2018. Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv* arXiv:1811.06624.

Ohanian, Roobina. 1990. Construction and validation of a scale to measure celebrity endorsers' perceived expertise, trustworthiness, and attractiveness. *Journal of Advertising* 19: 39–52. [CrossRef]

Parker, Dominic. 2019. Corruption, Natural Resources and Development: From Resource Curse to Political Ecology. *The Energy Journal* 40: 250–53.

Peguero, Anthony A., and Jun Sung Hong. 2020. *School Bullying: Youth Vulnerability, Marginalization, and Victimization*. Berlin/Heidelberg: Springer.

Pellegrini, Lorenzo. 2011. The rule of the jungle in Pakistan: A case study on corruption and forest management in Swat. In *Corruption, Development and the Environment*. Berlin/Heidelberg: Springer, pp. 121–47.

Polinsky, A. Mitchell, and Steven Shavell. 2001. Corruption and optimal law enforcement. *Journal of public Economics* 81: 1–24. [CrossRef]

Polinsky, A. Mitchell, and Steven Shavell. 2007. The theory of public enforcement of law. *Handbook of Law and Economics* 1: 403–54.

Rafiq, Aamna. 2019. Challenges of securitising cyberspace in Pakistan. *Strategic Studies* 39: 90–101. [CrossRef]

Rasool, Sadia. 2015. Cyber security threat in Pakistan: Causes, Challenges and Way forward. *International Scientific Online Journal* 12: 21–32.

Richards, Newman U., and Felix E. Eboibi. 2021. African governments and the influence of corruption on the proliferation of cybercrime in Africa: Wherein lies the rule of law? *International Review of Law, Computers & Technology* 35: 131–61.

Richmond, Christina. 2017. *Cybersecurity Readiness: How "At Risk" Is Your Organization*. Framingham: International Data Corporation (IDC), pp. 1–17.

Robbins, Paul. 2000. The rotten institution: Corruption in natural resource management. *Political Geography* 19: 423–43. [CrossRef]

Sattar, Zunaira, Shazia Riaz, and Ahmad U. Mian. 2018. Challenges of Cybercrimes to Implementation of Legal Framework. Paper presented at the 2018 14th International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, November 21–22.

Schafer, Joseph A., Beth M. Huebner, and Timothy S. Bynum. 2003. Citizen perceptions of police services: Race, neighborhood context, and community policing. *Police Quarterly* 6: 440–68. [CrossRef]

Slemrod, Joel. 2019. Tax compliance and enforcement. *Journal of Economic Literature* 57: 904–54. [CrossRef]

Slipachuk, Lada, Serhii Toliupa, and Volodymyr Nakonechnyi. 2019. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. Paper presented at the 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, July 2–6.

Snow, Arthur. 2011. Ambiguity aversion and the propensities for self-insurance and self-protection. *Journal of Risk and Uncertainty* 42: 27–43. [CrossRef]

Suwana, Fiona, and Nur Hidayat Sardini. 2022. Cyber Terror, the Academic Anti-corruption Movement and Indonesian Democratic Regression. *Contemporary Southeast Asia* 44: 31–55.

Tarter, Alex. 2017. Importance of cyber security. In *Community Policing-A European Perspective*. Berlin/Heidelberg: Springer, pp. 213–30.

Tene, Claude Bernard, Siddig Omer, and Blaise Mempouo. 2017. Towards a coherent implementation of safe building laws and regulations in Cameroon: Law, gowernance and institutional imperatives. *Journal of Sustainable Development Law and Policy* 8: 87–109. [CrossRef]

Tewamba, Harold Nguegang, Jean Robert Kala Kamdjoug, Georges Bell Bitjoka, Samuel Fosso Wamba, and Nicolas Nkondock Mi Bahanag. 2019. Effects of information security management systems on firm performance. *American Journal of Operations Management and Information Systems* 4: 99–108. [CrossRef]

Tran, Jasper L. 2016. Navigating the Cybersecurity Act of 2015. *Chapman Law Review* 19: 483.

Tremblay, Paul R. 2018. At Your Service: Lawyer Discretion to Assist Clients in Unlawful Conduct. *Florida Law Review* 70: 251.

UNODC (United Nations Office on Drugs and Crime). 2013. Comprehensive Study on Cybercrime. Available online: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf (accessed on 28 June 2023).

Vaughn, Michael S., Tab W. Cooper, and Rolando V. del Carmen. 2001. Assessing legal liabilities in law enforcement: Police chiefs' views. *Crime & Delinquency* 47: 3–27.

Veale, Michael, and Ian Brown. 2020. Cybersecurity. *Internet Policy Review* 9: 1–22. [CrossRef]

Weinstein, Mariani, Michaeline R. Jensen, and Brendesha M. Tynes. 2021. Victimized in many ways: Online and offline bullying/harassment and perceived racial discrimination in diverse racial–ethnic minority adolescents. *Cultural Diversity and Ethnic Minority Psychology* 27: 397. [CrossRef] [PubMed]

Williams, David Aled. 2019. *Understanding Effects of Corruption on Law Enforcement and Environmental Crime*. Bergen: U4 Anti-Corruption Resource Centre.

Williams, Lynne Yarbro. 2008. Catch me if you can: A taxonomically structured approach to cybercrime. *Forum on Public Policy: A Journal of the Oxford Round Table*. Available online: https://go.gale.com/ps/i.do?p=AONE&u=googlescholar&id=GALE\T1\textbar{}A197721378&v=2.1&it=r&sid=googleScholar&asid=c64b8028 (accessed on 6 May 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.