IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 March 2023, accepted 10 April 2023, date of publication 19 April 2023, date of current version 26 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3268529

RESEARCH ARTICLE

Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of the Cyber Threat Landscape and Readiness

EHTISHAM UL HAQUE[1], WASEEM ABBASI[2], SATHISHKUMAR MURUGESAN[3], (Member, IEEE), MUHAMMAD SHAHID ANWAR[4], FAHEEM KHAN[5], AND YOUNGMOON LEE[6], (Member, IEEE)

[1]Department of Computer Science, Muslim Youth University, Islamabad 44000, Pakistan
[2]Department of Computer Science and IT, Superior University, Sargodha 40100, Pakistan
[3]Department of Mechanical Engineering, National Cheng Kung University, Tainan 70101, Taiwan
[4]Department of AI and Software, Gachon University, Seongnam-si 13120, South Korea
[5]Department of Computer Engineering, Gachon Universityg, Seongnam-si 13120, Republic of Korea
[6]Department of Robotics, Hanyang University, Ansan 15588, South Korea

Corresponding authors: Muhammad Shahid Anwar (shahidanwar786@gachon.ac.kr) and Youngmoon Lee (youngmoonlee@hanyang.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) grant 2022R1G1A1003531, 2022R1A4A3018824 and Institute of Information and Communications Technology Planning and Evaluation (IITP) grant IITP-2022-2020-0-01741, RS-2022-00155885 funded by the Korea Government Ministry of Science and ICT (MSIT).

ABSTRACT Rapid growth in technological criminal activities has drawn worldwide attention to cyber forensics. The objective of a cyber forensics is to provide situation awareness in terms of identification and preservation of digital evidence, extraction of information, and analysis of extracted information to facilitate time-critical decision making. However, Cyber Forensic Investigations (CFIs) still lack significant structure to provide reliable insight into major cyberattack patterns. Data from the Global Cyber Security Index (GCI) show that Pakistan lags far behind in technological and organizational initiatives, posing a threat to its national security. This article focuses on state coordinated CFI infrastructure to mitigate the occurrence of cybercrime challenges. Moreover, a conceptual model is established to address the infrastructure of CFI using policy approach, legal, technical, organizational, capacity building, and cooperative venture. This conceptual model is structured in pillars to simplify the CFI infrastructure. The goal of the study is to provide an empirical foundation for policymakers to develop a comprehensive framework for CFI in the country, and to offer insights and recommendations for improving the infrastructure to better combat cybercrime in Pakistan.

INDEX TERMS Cyber forensics, cyber forensic investigation, cyber landscape, cybersecurity, digital evidence, digital forensics, e-crime, incident response.

I. INTRODUCTION

It is expected that the reliance on technology-based services will grow exponentially in the future, which has already been observed to a great extent in the recent past [1]. Open-source platforms such as Dropbox, OneDrive, Google Drive, iCloud, etc. have become popular among individuals for storing valuable data due to their accessibility and digital security features [2]. However, it is important to acknowledge the potential risks associated with these platforms, such as data breaches and exposure to cyber-attacks. Despite the benefits they offer in terms of data viability and protection, open-source platforms also pose a threat of unauthorized access to the stored data and the possibility of hacking incidents [3]. This highlights the need for a careful consideration of the trade-offs between the advantages and risks of using these platforms for data storage. In their efforts to prevent data leakage and raise awareness about cyber-attacks and crimes,

The associate editor coordinating the review of this manuscript and approving it for publication was Roberto Nardone.

Law Enforcement Agencies (LEAs) are playing a vital role. The field of cyber forensics is also contributing to these efforts, as cybercrime investigators aim to gather digital evidence from a variety of physical and digital devices, such as computer network devices, personal digital assistants, cell phones, drones, robots, and closed-circuit TV systems [4]. The goal of these investigations is to collect and analyze digital evidence in order to aid in the prevention of cybercrimes and the identification of perpetrators [5].

The advancement in anti-forensic techniques has posed a challenge to the effectiveness of current forensic investigations [6]. Several technical flaws in current forensic approaches are vulnerable to anti-forensic tools that can nullify detection. Anti-forensic tactics are being employed to manipulate and hinder cyber forensics. Cyber forensics is a process that encompasses various stages of investigation, including identification, preparation, collection, examination, analysis, interpretation, documentation, and presentation of digital evidence [7]. However, the use of anti-forensic techniques complicates the process and calls for the need for improved forensic methods that can effectively counter these tactics. These procedures are adopted with legal firm adherence to establish a criminal case that will withstand the test of legal scrutiny and can be proven in court.

Globally, with increased usage of the digital media platform for data storage, cybercrime are also growing rapidly [4]. To combat cybercrime, security organizations devised different mechanisms to overcome numerous obstacles worldwide. Many studies have been conducted recently to systematize and define the phases involved in the cybercrime investigation process [4], [8]. The field of CFI is diverse and contains complex tasks, activities, processes, and subdomains [8]. A huge surge in cybercrime and cyberattacks are reported in 2022, due to advancements in anti-forensic techniques [1]. The only thing required for an offender is a computer and an internet connection. The free accessibility of software and tools for this purpose makes the cracker more suitable to exploit. To cater for this scenario, researchers in this domain used different tactics and tools for prohibited access and subterfuges of digital content to increase its vulnerability against cyber-attacks.

The National Institute of Standards and Technology (NIST) [9] has played a crucial role in addressing the issue of internet misuse by creating a framework and standards for organizations to prevent cyberattacks and audit their security infrastructure. These frameworks and standards are updated every three years to stay current with the latest threats and security measures. Despite the efforts of organizations and NIST, data theft remains a significant threat in the digital age, as it grows exponentially and becomes more difficult to prevent. A successful cyberattack requires the collaboration of multiple threat actors, who have access to basic attack tools that make it easier for them to gain access to a system's assets. These initial attacks can then be used as a stepping stone for more sophisticated hybrid strikes. Therefore, it is crucial for organizations to implement policies, procedures, guidelines, baselines, and best approaches to restrict internet misuse and prevent data theft. Adopting NIST's framework and standards can provide a solid foundation for organizations to strengthen their cybersecurity measures and prevent cyberattacks.

The paper is focused on in-depth analysis of the current state of the cyber crime investigation infrastructure in Pakistan. The paper seeks to understand the cyber threat landscape in the country and assess the readiness of the infrastructure in place to handle such threats. The research will cover various aspects of the cyber crime investigation infrastructure, including the legal framework, available resources, and challenges faced by the relevant agencies. However, the limits of the work are confined to the analysis of the cyber crime investigation infrastructure of Pakistan. The paper does not delve into other aspects of the broader cyber security landscape in the country, such as national-level strategies and policies for cyber security, or broader socio-economic factors that may influence the cyber threat landscape. The analysis is limited to a single country and may not be generalizable to other regions. The work is based on the available data and literature and is subject to the limitations of the sources used. The current body of research on the infrastructure for Cyber Forensic Investigation (CFI) is limited. A relatively few studies have previously undertaken an analysis of this infrastructure [3], [5], [10], [11], [12], [13]. The key contributions of this paper are outlined as follows:

- The paper will focuses on the various challenges, scope, processes, and policies related to the infrastructure and on in-depth analysis of the policy, jurisdictional, technical, organizational, academic, and cooperative mechanisms involved.
- The goal of the paper focus on empirical foundation for policymakers to develop a comprehensive framework for cybercrime investigation in the country, and to offer insights and recommendations for improving the infrastructure to better combat cybercrime in Pakistan.
- The research aims to develop effective legal measures to advance the CFI infrastructure and align it with globally accepted standards and best practices. By doing so, the paper intends to enhance the overall efficacy of cyber investigations and promote the responsible use of digital technologies.
- The purpose of this paper is to address the current shortcomings in the legal framework of CFI and present recommendations for its improvement.

In order to understand the current provision, this study examined government and professional websites and their associated documentation. Because there is no central authority in Pakistan that governs academic provision in the higher education sector, course details can only be obtained through personal inquiry or internet research. Administration papers, past studies, reports by local and international center on cyber crime and cyber forensics in Pakistan, as well as presentations by governing authorities and International Telecommunication Union (ITU) publications, are regarded as the main sources of data for this work [14]. The increasing threat of cybercrime worldwide has emphasized the need for effective CFI techniques and infrastructure [15]. Despite facing numerous cyber security challenges, the CFI infrastructure in Pakistan remains in its early stages. The lack of modern techniques and resources available to local police units in Pakistan can lead to the loss of valuable evidence and contamination of crime scenes. The implementation of crime scene investigation teams is necessary to address this issue. While the PFSA in Lahore, and NFSA in Islamabad have established Crime Scene Investigation (CSI) units, the majority of crime scene processing is still carried out by local police, due to their limited access to the necessary tools and training. It is crucial to improve the CFI infrastructure in Pakistan to effectively address the growing threat of cybercrime and ensure the proper preservation of evidence.

The rest of the paper is organized as follows: The paper starts by reviewing relevant literature in Section II. Section III provides an overview of the current cyber landscape in Pakistan and highlights some of the key challenges that need to be addressed. In Section IV, the CFI infrastructure is examined through the framework for cyber security preparedness developed by the International Telecommunication Union. Finally, the paper concludes in Section V.

II. RELATED WORK

In majority of the previous works, authors are focused more on cyber security standards and guidelines against cybercrime [2], [9], [15], [16]. The mentioned work discussed the trend and future of cybercrime and wrote about cyber forensics, network forensics, memory forensics, and other topics [17]. In comparison to traditional forensics, cyber forensics is a relatively new field. Over the last 35 years, efforts have been made to improve cyber-crime investigation by proposing novel strategies to analyze computers and peripheral devices that have been used in cybercrimes [18]. Under these conditions, law enforcement agencies were required to present digital evidence at trial, which necessitated disseminating the findings of their investigations to a large audience [19]. The ease with which the conventional techniques of forensic investigation are carried out is one of the important issues at hand. The behaviour of the investigators exhibits a strong sense of cynicism and criticism towards modern methods and tactics, and their approach lacks the organization and structure that is typically seen in contemporary practices [20]. In Pakistan, the availability of training programs to acquire essential skills is scarce [21].

The formulation, standardization, and formalization of cyber forensic techniques have improved over the past few years [22], [23], [24], [25]. From an IT standpoint, the NIST [23] provides useful guidelines on how to conduct computer and network forensic analysis. The National Criminal Justice Reference Service (NCJRS), which is part of the Office of Justice Programs within the United States Department of Justice, disseminates guidelines and data on the techniques utilized by law enforcement in cyber forensics [26]. ISO/IEC 27037:2012 [27] offers guidelines for dealing with digital evidence during specific activities like identifying, gathering, acquirement, and storage. However, additional work in this area is required [28], [29]. Law enforcement and Incident Response (IR) are the two main fields where cyber forensic is used. IR is concerned with incident management in cyber incident response environments, whereas cyber forensics analysis in law enforcement is concerned with analyzing digital evidence to determine whether a criminal act has occurred and if so, assign authority and prosecute offenders. Although law enforcement and IR employ cyber forensics in very similar ways [30], this investigation's focus is on the usage of cyber forensics in law enforcement.

Due to the development of technology in many developed countries, CFIs are becoming a widely esteemed professional and academic discipline [31]. It has a well-defined infrastructure that helps during cybercrime investigations within the private sector and police/secret services. There is also specific and clear legislation dealing with computer misuse, as well nationally accepted guidelines for the presentation and processing of digital evidence. The legislative bodies, investigative policies, standards, procedures, baselines, and guidelines were discussed in many studies [24], [31]. The Criminal Justice System can be strengthened by the knowledge of the forensic sciences, research, and collaboration between forensic law enforcement agencies and university research labs. The academic community in Pakistan is working hard to convert outdated practices to more contemporary ones and to advance the forensic science domain. As it will result in a general improvement in crime detection and criminal case prosecution throughout Pakistan [15].

In the South Asian region, the field of cyber forensics remains under-explored and under-addressed [13], [32]. Most literature review and academic research in this area are carried out by developed countries, leaving a gap in the understanding of cyber forensics in the Southeast Asian context [1], [5], [21]. The digital crime landscape in the region is rapidly evolving and includes a range of issues such as false identification, credit card fraud, and SIM-box fraud, which contribute to other criminal activities such as money laundering and financing terrorism [17]. The sharp increase in cybercrime cases between 2020 and 2022 highlights the urgent need for a more comprehensive and effective approach to addressing cyber forensics in the region. As the digital landscape continues to develop, it is projected that the number of cybercrime cases will continue to grow [3]. The need for improved digital governance, increased awareness, and better understanding of cyber forensics issues in Southeast Asia is crucial for promoting cybersecurity and protecting against potential cyber threats [1], [32]. In Pakistan, the availability of reliable information on the state of cyber forensics is scarce [3]. The internet is frequently exploited by individuals for illegal activities, including intrusion and criminal acts. The government's lack of sufficient resources to combat cybercrime has resulted in an increasing number of complaints, with no proper mechanism or expertise in place for investigating these crimes.

III. CURRENT CYBER LANDSCAPE OF PAKISTAN

Pakistan ranks 79^{th} in terms of cybersecurity in the Global Cybersecurity Index (GCI) 2020 [14] published by the International Telecommunication Union (ITU). The ITU member state's commitment to cybersecurity is measured against five components: legal, technical, organizational, capacity-building, and cooperative. These pillars are used to rank the GCI, which is depicted in Figure 1.The fact that Pakistan fell from 66^{th} to 79^{th} place in 2020 is relevant to note [14]. The primary cause of this decline is the absence of any indication of progress in the above commitment areas, while other countries have begun to exhibit their commitment to the GCI's five pillars. GCI is a credible reference that assesses countries' commitment to cybersecurity on a global scale in order to raise awareness of the issue's importance and various dimensions. The primary data source for various dimensions is from an ITU publication.

Pakistan is one of the least prepared for a cyberattack, as neither the National Computer Emergency Response Team (CERT) nor any Cybersecurity Incident Response Team exists in the country [19]. This is not surprising given that the general public is susceptible to various cyber threats because of a lack of widespread knowledge about cybersecurity and an unregulated online environment [31]. The communications industry has grown significantly during the past few decades. Through contemporary communication devices, almost the entire world is connected. Institutions that use computer associated technologies are open to any malicious cyberattacks. Any attack on these systems has the potential to quickly have a large scale impact. Several organizations are working independently to develop redundancy in this area, but there is a lack of coordination among the national efforts. Even the security organizations operate in their own sectors and require additional cooperation for a thorough response [33]. Armed forces have chosen to deploy network-enabled technology, making them vulnerable to disruption from the enemy. Although cybercrime are pervasive in modern society, the majority of them go unreported. Additionally, it is becoming increasingly common practice to hack data using innovative techniques and even to steal money from bank accounts [24].

Until recently, Pakistan's management framework for its cyberspace was not properly developed. As a result of the lack of strong technical organizations like the national Computer Emergency Response Team (CERT) and sectoral CERTs, various institutions like banking, telecommunication, defence, oil and gas, etc., are working alone to prevent cyberattacks. Any successful cyberattack on one industry, such as banking or telecommunications, may also have a huge impact as these industries serve as the backbone of the country's infrastructure and provide services to public and private sectors [34]. Cooperation is always preferred among different cybersecurity organizations to adequately detect and respond to complex cyberattacks and hybrid warfare. A significant issue in Pakistan is the lack of capable cybersecurity resources [15]. This is due to a number of factors, including the lack of a well-established career in the field, a lack of possibilities for teaching professionals to expand their capacities and obtain accreditation, and a lack of opportunities for keeping a workforce in cybersecurity with high potential.

IV. CONTEXTUAL MODEL

The CFI study already established is based on primary pillar already mentioned in the 2020 Global Cybersecurity Index [14]. This incorporates the infrastructure for multistakeholder cybersecurity collaboration from the International Telecommunication Union (ITU) to create synergies between current and future endeavours. The extended version based on six pillar policy, existing legal structure, technical, organizational, capacity building and cooperation are the basic foundations. These six pillars as depicted in Figure 2 serve as the investigation infrastructure to outline the essential elements of cyber investigation worldwide.

In the customized CFI infrastructure, researchers are employing old techniques, which are not sufficient in the world of rapid technological advancements [21], [31], [35]. Overall, the state CFI infrastructure is weak in Pakistan and does not appear to be a proactive, comprehensive, or at a grassroots security level [21]. The current counter cybercrime tactics focus on "putting out the fire" and appear to be reactive in nature. The existing CFI measures are insufficiently detailed and are implemented with under-resourced programs. The "security box centric" approach to addressing CFI concerns excludes any sort of "out of the box" thinking and places an excessive emphasis on the previous studies. Even within the same organization, such as risk, compliance, security, and IT audit, there is no agreement on how to handle CFI issues. This disagreement is inconvenient since it wastes time and money. Added to that, the issues of governance and documentation overkill, where the majority of cybercrime activities and projects are academic in character, with copious policies and procedures but no solid execution strategy (In almost all cases, only $5-10\%$ of the approved policy is used).

To enable national growth of cyber-crime investigation abilities and proficiencies, political, economic, and social actors within the administrative context of the country must work together [36]. This could be done in a number of ways, such as through the judicial system, law enforcement, educational institutions, ministries, departments, and agencies. Moreover, it may be implemented through the development of public private partnerships, cooperation among the private sector, inter agency and intra-state collaboration, and by stepping up attempts to broadly adopt cyber forensics. These studies' pillars emphasize a distinct necessity for a cyber infrastructure. The first pillar deals with policy and procedure development, which defines the approach of forensic properties via a forensic policy. The second pillar lies in legal problems, considering the legislative structure of organizations in place to address CFI and cyber forensic. The third

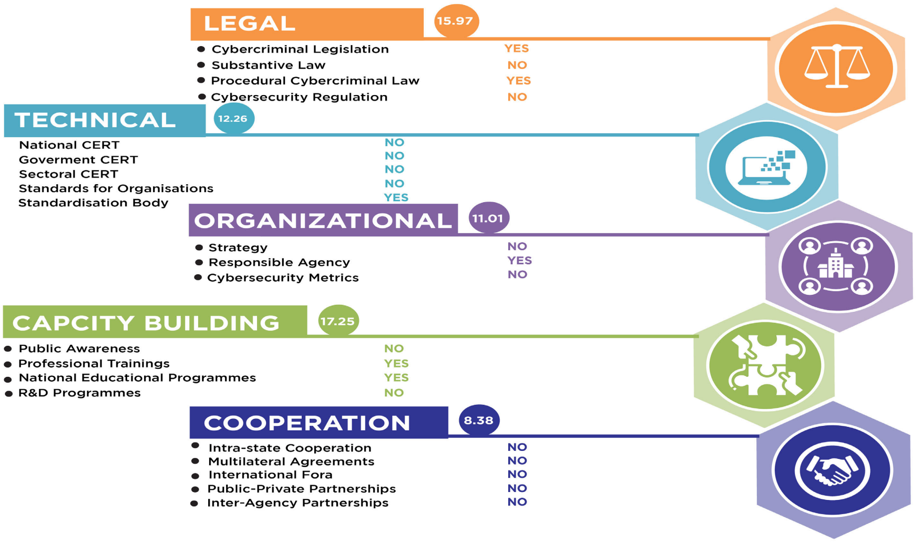

LEGAL
15.97
Cybercriminal Legislation YES
Substantive Law NO
Procedural Cybercriminal Law YES
Cybersecurity Regulation NO
TECHNICAL
12.26
National CERT NO
Goverment CERT NO
Sectoral CERT NO
Standards for Organisations NO
Standardisation Body YES
ORGANIZATIONAL
11.01
Strategy NO
Responsible Agency YES
Cybersecurity Metrics NO
CAPCITY BUILDING
17.25
Public Awareness NO
Professional Trainings YES
National Educational Programmes YES
R&D Programmes NO
COOPERATION
8.38
Intra-state Cooperation NO
Multilateral Agreements NO
International Fora NO
Public-Private Partnerships NO
Inter-Agency Partnerships NO

FIGURE 1. Pakistan current cyber landscape (Data source: ITU Publication) [14].

pillar is concerned with technical aspects and can assess the responsiveness of technical organizations. The formation of national cyber forensic programs and organizational framework for policy coordination are covered in the fourth pillar. Capacity building is addressed in the fifth pillar, as it comprises academic courses, research and development (R&D), and certifications for professional bodies. The procedures in place to encourage global collaboration and cooperation in the field of cyber forensics are finally covered in the sixth pillar.

A. POLICY AND PROCEDURE APPROACH

The significance of computer security policy research in defining the forensics capabilities of a system is explored in this section [23]. It highlights the issues faced with various approaches and the crucial steps involved in managing evidence collection during a CFI. Digital evidence, which can encompass unlawful cyber conduct, criminal collusion, or criminal intent, is of great value and prone to compromise if not properly managed and protected. Thus, it is imperative to establish and follow strict standard procedures for CFI activities. These procedures provide detailed guidance on the acceptable methods of collecting digital evidence, the correct setup of systems for evidence recovery, the secure storage of recovered evidence, and the documentation of the investigation to ensure data authenticity.

One of the major challenges in CFI is the inaccurate media framing, which often presents a general view and fails to provide a complete understanding of cybercrime and its associated problems. The lack of institutional structure and the emphasis on external security threats over cybercrime issues contribute to the underfunding of cybercrime investigations. The traditional security culture, which focuses on border security, nuclear threats, terrorism, etc., dominates the national security agenda, leaving cybersecurity and crime investigation neglected. Furthermore, the lack of public participation in the development of relevant legislation adds to the problem. The policies become bureaucratic and technologically driven, lacking the feedback from those affected by cybercrime.

Despite these challenges, the Pakistani authorities are taking steps to enhance online security as the nation experiences rapid internet adoption. With the growing reliance on internet services, individuals are becoming more vulnerable to cybercrime. The development and implementation of policies for building a cyber forensics capacity face similar legal constraints and require clear and explicit policies. To maintain the integrity of the system, it is essential to develop clear, accurate, and well-written cyber forensics policies. Additionally, during a cybercrime investigation, it is important to keep the end goal in mind by maintaining a ‘‘chain of custody’’ and ensuring that the investigator follows a clear path.

1) SECURITY POLICY STIPULATION

A security policy sets out what is and isn’t permitted in terms of security by categorizing a system’s states into secure or allowed and insecure or unauthorized. It is a set of instructions that, when followed, results in a secure system. The statements in the policy represent the security requirements of the system, which must be upheld to ensure the system only generates allowed states [37]. In other words, a security policy outlines the security objectives of a system and the actions taken to achieve those objectives. The security policies for military systems are designed to be explicit to secure sensitive data. These policies aim to prevent unauthorized information disclosure or theft [38]. For example, classified

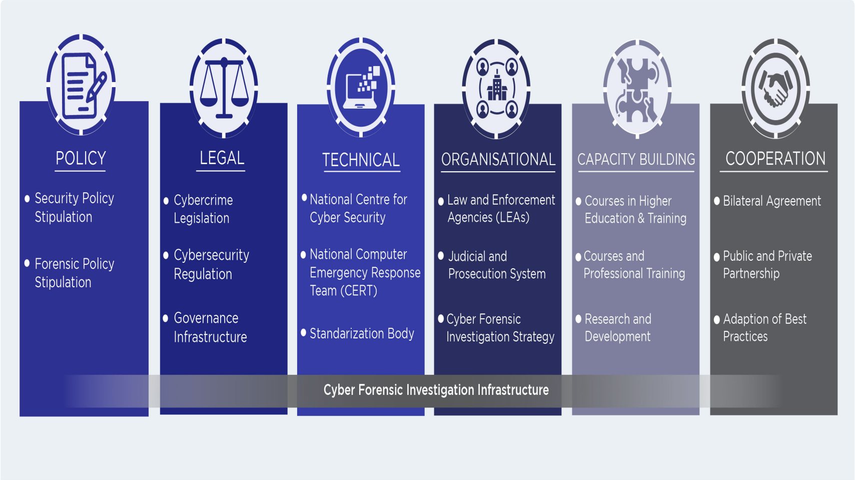

POLICY
Security Policy Stipulation
Forensic Policy Stipulation
LEGAL
Cybercrime Legislation
Cybersecurity Regulation
Governance Infrastructure
TECHNICAL
National Centre for Cyber Security
National Computer Emergency Response Team (CERT)
Standarization Body
ORGANISATIONAL
Law and Enforcement Agencies (LEAs)
Judicial and Prosecution System
Cyber Forensic Investigation Strategy
CAPACITY BUILDING
Courses in Higher Education & Training
Courses and Professional Training
Research and Development
COOPERATION
Bilateral Agreement
Public and Private Partnership
Adaption of Best Practices
Cyber Forensic Investigation Infrastructure

FIGURE 2. **Cyber Crime Investigation Infrastructure.**

information must be protected from unauthorized disclosure or declassification according to military security policies. To enforce this, user access categories are assigned based on a person's authority or clearance, and all papers must be labeled with their classification level. All those working with classified data must follow these guidelines, and enforcement is mandatory. However, the GoP does not have a clearly defined goal or priority in this regard due to the absence of a national cybersecurity strategy and policy. A well-defined security policy is essential for a country to combat threats that could compromise digitalization, rapid innovation, economic growth, and the social benefits derived from cyberspace.

2) FORENSIC POLICY STIPULATION

The goal of cyber forensics is to obtain digital evidence while maintaining its forensic integrity for potential legal use. To achieve this, forensics policies must address both the collection and preservation of evidence. The policy outlines the incidents that require forensic attention and the data related to those incidents that must be preserved, rather than listing what is allowed and prohibited [20]. This way, the policy divides all potential breaches or criminal activities into two categories: those that need forensic intervention and those that do not. For instance, a commercial system may use a simple forensics technique for handling network security breaches. Forensics aims to protect data from actual attacks or breaches. The commercial system's rules require that all incidents identified as intrusions or potential intrusions on the network must have the relevant data collected and kept on file in case legal action is taken. One way to implement the policy is by routinely retaining logs from the Intrusion Detection System (IDS), firewall, and router, as well as the public web server logs. These logs must be stored for a predetermined amount of time.

B. LEGISLATION

The main objective of legal frameworks in regards to cybercrime is to have up-to-date legislation that can effectively address the constantly changing nature of cybercrime. These regulations and laws give the government the authority to implement effective responses for the investigation and prosecution of cybercrimes.

1) LEGAL CHALLENGES

Pakistan faces numerous challenges in terms of its internal security, including a need to tackle cybercrime and carry out investigations. These challenges stem from factors such as weak democratic systems, poverty, lack of technology expertise, and corruption. The country also lacks the appropriate technology for oversight, particularly when it comes to foreign intelligence agencies like the United States National Security Agency [3]. Additionally, viruses like Gamarue, Skeeya, and Peals make Pakistan more vulnerable to cyberattacks by spreading new malware and stealing sensitive data from computer systems [12]. Another form of vulnerability is the Distributed Denial of Service (DDOS) attack, which refers to unauthorized data transmission within a computer [2]. The banking sector in Pakistan is particularly at risk of cyberattacks, as acknowledged by the Federal Investigation Agency's Cyber Crime Bureau following recent reports of data theft from all Pakistani banks [39].

In Pakistan, there is a lack of public awareness regarding cybersecurity which leads to incidents like identity theft [5]. The weak democratic structure of the country also affects the implementation of effective measures to prevent electronic crimes through the Pakistan Prevention of Electronic Crime Act (PECA) 2016 [40]. The act, however lacks adequate protection against data breaches and the penalties imposed for cybercrime, cyber warfare, and cyber terrorism are considered excessively harsh without consideration for the severity of the offense. These shortcomings highlight the ongoing challenge in developing and implementing effective cyber policies.

The current legal framework for addressing cybercrime in Pakistan is fragmented and challenging to navigate [41].

TABLE 1. Existing Electronic Crime Laws.

Law/Legislation	Year
The Telegraph Act [42]	1885
Pakistan Telecommunication (Re-organization) Act [43]	1996
National Policy and Action Plan [44]	2000
Electronic Transaction Ordinance (ETO) [45]	2002
Electronic Crimes Act [25]	2004
Electronic / Cyber Crime Bill [46]	2007
Prevention of Electronic Crimes Act (PECA) [40]	2016

Despite having a number of laws in place to address online offenses, the requirements are scattered across different legislation, making it difficult to have a unified structure for cybercrime and punishment [29]. To improve the investigation and prosecution of cybercrime, a complete legal infrastructure for cyber forensics is needed by integrating all existing laws. The existing legislation related to cybercrime in Pakistan is summarized in Table 1. The laws are also weak and can be easily circumvented by individuals with basic computer knowledge.

Pakistan faces a shortage of private sector support in developing its cybersecurity and cyber forensics infrastructure [46]. The responsibility of maintaining cybersecurity is primarily assigned to the National Response Center for Cybercrimes (NR3C) under the FIA (Federal Investigation Agency), and the Pakistan Information Security Association (PISA), a non-profit working with the private sector to address commerce-related threats [47]. Despite these efforts, there is still much work to be done to effectively address the issue of cybercrime. Better collaboration and planning between civilian and military groups is necessary to establish a robust cybercrime system, comparable to those in other modern countries [17].

2) REGULATION FRAMEWORK

In Pakistan, the regulation and standardization of CFI is still lacking, despite the acceptance of digital evidence in courts [46]. The primary responsibility for gathering cybercrime evidence lies with the Cyber Crime Wing (CCW) of the Federal Investigation Agency (FIA). However, due to the absence of a well-established CFI profession, the private sector's role in cyber investigations is limited [48]. The Communications Service Providers (CSPs) are one of the few private companies that provide cybercrime investigation services [21]. Although the FIA conducts investigations, there are no formal standards or policies in place from the Ministry of Justice [35]. This lack of regulation raises concerns about impartiality in the prosecution of cybercrime cases and the use of electronic evidence in the judicial system [41].

Cyber forensic evidence's objectivity has been acknowledged as a crucial element of CFI on a global level [34]. Because forensic investigation is typically overseen by a different entity that is independent from the agency responsible for prosecuting cases employing forensic evidence, the autonomy and independence of digital evidence are safeguarded [20]. Cyber investigation and regulation in the United Kingdom, for example, is governed by a clear governance framework [49]. The Association of Chief Police Officers (ACPO) ''Good Practice Guide for Computer-Based Electronic Evidence'' guidelines offer a framework that guarantees cyber forensic reports in the UK comply with both international standards of cyber-crime investigation and with commercially accepted tools, techniques, and procedures for gathering, processing, and analyzing exhibits. The ACPO rules are intended primarily for ''police officers, police employees, and private investigators functioning in cooperation with law enforcement'' [50]. They are divided into a set of four guiding principles and then more specific instructions. The ACPO rules are regarded as the de-facto standards for digital investigation in the UK [51]. ACPO provides a way to make sure the investigation is carried out in a way that is generally recognized as professional. Table 2 summarizes the most popular cyber forensic models and guidelines. The CFI becomes more unbiased and independent as a result of this approach. Wales and England utilize a similar approach in that both countries have independent forensics regulators that offer transparency, independence, and guidelines for excellent forensic services [52]. Finally, [51] and [53] contain further forensic recommendations and models put forth by NIST and INTERPOL. Although the CFI environment in England and Wales is divided between the public and private sectors, the Forensic Science Regulators strive to preserve uniformity in service and the delivery of high-level cyber forensic evidence [54].

Apparently, Pakistan needs a similar system and governance setup that will consider the prejudices that are most likely to show up in a police prosecution and forensic investigation. Because the public views the police as dishonest institutions, there is al-ready a significant level of mistrust between the public and the police [68]. A free public body can be constituted to control CFIs in Pakistan. Due to the numerous laws in Pakistan that control the investigation and prosecution of cybercrime, it is challenging for law enforcement entities to apply these laws during CFIs. It is therefore advised that the various pieces of legislation be merged into a single comprehensive statute for cybercrime prosecution and cyber forensic inquiry. Establishing a Cyber Law Review Committee will help the Government of Pakistan (GoP) to identify issues with the current cyber environment and develop a comprehensive legislative plan for dealing with cybercrime and prosecution. This committee should include representatives from all relevant parties. Cyber security activities and cyber forensics require a strong governance structure to ensure their longterm viability. The National Cyber Security Cyber Security Policy 2021 recommends that the government establish institutions devoted to cyber security and establishes the framework required for the efficient operation of organizations like the National Cyber Security Center (NCCS), Computer Emergency Response Team (CERT), and National Cyber Security Policy Working Group [3].

TABLE 2. Forensic Models and Guidelines.

Forensic models	Year
Digital Forensic Investigation Model [55]	2001
Digital Investigative Process Model [56]	2001
An examination of Digital Forensic Models [57]	2002
Integrated Digital Investigation Model [58]	2004
Enhanced Digital Investigation Process Model [59]	2004
Extended Model of Cybercrime Investigation [60]	2004
NIST Guide to Integrating Forensic Techniques into Incident Response [61]	2006
Digital Forensic Model for Digital Forensic Investigation [62]	2011
Systematic digital forensic investigation model [63]	2011
A new approach of digital forensic model for digital forensic investigation [62]	2011
ACPO guidelines [51]	2012
Advanced data acquisition model [64]	2012
Analytical Crime Scene Procedure Model [65]	2013
A comprehensive and harmonized digital forensic investigation process model [66]	2015
A comprehensive digital forensic investigation process model [67]	2016
Interpol review of digital evidence 2016-2019 [53]	2020

C. TECHNICAL STRUCTURE

The increased use of IT and telecom in cyberspace makes it more vulnerable to exploitation and disruption by hackers [69]. Additionally, the attack surface has expanded to the point where hackers can now shut down networks whenever they choose [70]. Consider the consequences if the banking system, electricity grid, transportation network, and military command and control systems of a country were all rendered inoperative [71]. Technology is the main line of defence against cyber threats [2]. Computer Emergency Response Teams (CERT), technological protocols and capacity for the identification and investigation of digital fraud must be in place in order to effectively fight against cyber concerns. Putting in place structure for efficient technical Incident Response coordination is also essential [72]. Millions of cyberattack have recently been directed at infrastructure and services [3], [71]. Ransomware has been employed by hackers in a number of instances to demand payment from its victims. Although it is possible to conceal oneself behind the open architecture of the internet, it is frequently impossible to identify the attacker [15]. This is true, especially when state sponsored cyberattacks are involved. Due to the asymmetry of attacks, hackers also benefit from anonymity. Countries must take steps to ensure adequate cybercrime. In the area of computers, security encompasses both cyber and physical security. Cyber security encompasses defending against disruption, hacking, and cyberattacks for computer networks, infrastructure, software applications, military command and control systems, utility services, and other systems. Household devices will be vulnerable to interruptions and hackers as technology advances quickly [3]. Because of this, the field of cybercrime and security is broad and has a rapid rate of learning.

In Pakistan, the implementation of the Prevention of Electronic Crimes Act of 2016 [40], also known as the cybercrime bill, has presented a new challenge due to a shortage of technical competence in the country. The National Response Centre for Cybercrimes (NR3C) of the Federal Investigation Agency (FIA) is the only organization with the means and technological skills to gather evidence and offer information on the issue. There is no impartial organization that can counter check the FIA findings. The new cybersecurity strategy for Pakistan would establish Security Operations Centers and Computer Emergency Response Teams (CERTs) at the institutional, sectoral, and national levels, as well as a new governance and institutional framework for a "safe cyber environment" Security Operation Centers (SOCs). The policy consists of new platforms for information exchange, initiatives for training and skill development, and public awareness campaigns. Nonetheless, cybersecurity has gotten a lot of attention, and cybercrime investigation has gotten little attention. This is a result of the wrong stake-holder having control over the policy because it has a far larger spectrum than cybersecurity. Investigations into cybercrime should be directed to the National Security Division (NSD).

The Ministry of Information Technology and Telecommunications drafted the policy in order to create a plan of action for establishing a concrete legal and structural framework for cybersecurity. To explore all aspects of cyber threats, the National Cyber Security Policy 2021 aims to establish a trustworthy national digital ecosystem that is strong and constantly improving while preserving the confidentiality, integrity, and availability of digital assets [3]. Some of its main guiding principles include the creation of a national response framework, protection of citizen data security and privacy, provision of necessary systems and support to interested public and private organizations, and, last but not least, the adoption of best practices to guarantee national digital sovereignty.

Cybersecurity and cybercrime are the two components of the National Cyber Security Policy. It has been overdue for the creation of a strategy to combat offensive cyber operations. Existing laws governing information and data security, or "cyber laws," did not consider the rising need to defend against and prevent cyberattacks. Although the current policy does not have a response structure with clear tasks and responsibilities, it does state that Pakistan will retaliate if attacked. As a result, Pakistan will respond appropriately to any cyberattack on its critical information infrastructure or critical infrastructure since it will be viewed as an infringement on its sovereignty. The choice to establish a national response team is equally crucial in this situation. As a result, Pakistan lacks the competence and skill to respond to cybercrime issues in an efficient manner [12]. Furthermore, as cybercrime is a global problem, developed countries with more cutting-edge technology may be able to assist Pakistan in enhancing its investigative capabilities. Given the global nature of cybercrime, Pakistan may be able to benefit from assistance from the National Cyber Security Centre of the GCHQ UK and the Computer Analysis and Response Team (CART) of the FBI US. The successful adoption of CFI infrastructure will depend on the country's capacity to react swiftly to cyber threats and offer mitigation measures to prevent property loss. A government without the advanced technologies to recognize and respond to cyberattacks will continue to be a target for cyber criminals.

D. ORGANIZATIONAL STRUCTURE

In the discussion of National Cybersecurity Policy, the issue of organizational structure in Pakistan arises. The country has several paramilitary organizations that fall under the jurisdiction of the Interior Ministry, including the Pakistan Rangers (Sindh and Punjab), the Pakistan Maritime Security Agency, the Frontier Corps (KPK and Baluchistan), the Frontier Constabulary, the Northern Areas Scouts (Gilgit Baltistan), the Islamabad Police, and the Federal Investigation Agency (FIA). The law enforcement system in Pakistan is illustrated in Figure 3, which shows the structure of these paramilitary groups. The state police are organized on a territorial basis, with divisions into zones, ranges, districts, and subdivisions. The main goal of the state police is to maintain peace and order within the state. The state police force is led by a hierarchy of high-ranking officials, including the Inspector General, Deputy Inspector Generals, District Police Officers, Superintendents, Deputy Superintendents, and Inspectors. Each level of leadership is responsible for ensuring the effective operation of the state police and ensuring public safety.

1) FEDERAL INVESTIGATION AGENCY (FIA) AND ITS ASSOCIATED AGENCIES

The Federal Investigation Agency (FIA) is in charge of criminal investigations and counterintelligence, and it also assists and advises state investigators on occasion [35]. The FIA Technical Wing to provide forensic and scientific support to FIA field units and Federal Courts in the field of questioned documents and fingerprints throughout Pakistan. The Federal Investigation Agency's Cyber Crime Wing (CCW) is governed by legislation enacted under the Prevention of Electronic Crimes Act (PECA) 2016, which addresses the growing issue of cybercrime [15]. The purpose of establishing this high-tech crime-fighting team was to recognize and address the phenomenon of technological abuse and it is Pakistan's sole organization of its sort, receiving complaints directly and taking legal action against cyber offenders. Law Enforcement Agencies (LEAs), government departments, and forensic bodies get forensic services, training, and direction from the National Forensic Science Agency (NFSA). Forensic science laboratories were built to increase criminal detection capabilities in Pakistan as well as to strengthen LEAs competence by providing training and equipping them with the most up-to date criminal investigation tactics utilizing modern scientific equipment. As a result, these institutions contribute to the public's trust in the country's criminal justice system.

The Federal Investigation Agency (FIA) is responsible for conducting criminal investigations and counterintelligence operations in Pakistan and also aids and advice to state investigators as needed [13]. The FIA has a Technical Wing that offers forensic and scientific support, including questioned document analysis and fingerprint analysis, to FIA field units and federal courts throughout the country [35]. The FIA's Cyber Crime Wing (CCW) is established under the Prevention of Electronic Crimes Act (PECA) 2016 to address the growing issue of cybercrime. The CCW is the country's only organization of its kind and is tasked with investigating and taking legal action against cyber offenders [15]. Complaints are received directly by the CCW. Other responsible agency is the National Forensic Science Agency (NFSA) provides forensic services, training, and guidance to Law Enforcement Agencies (LEAs), government departments, and forensic bodies in Pakistan [35]. The establishment of forensic science laboratories is aimed at improving criminal detection capabilities and equipping LEAs with modern scientific equipment and techniques. This helps to increase public trust in the country's criminal justice system [41].

In Pakistan, the National Response Centre for Cyber Crime (NR3C) is a dedicated law enforcement organization that focuses on combating cybercrime [39]. NR3C specializes in various areas, including cyber forensics, technical investigation, information system security audits, penetration testing, and training [35]. The National Forensic Science Agency (NFSA) and the Punjab Forensic Science Agency (PFSA) have merged to become the largest provider of forensic investigative services in Pakistan [73]. However, there is a need for further development to bring the lab's standards up to an acceptable level on an international scale [39]. The government needs to make a significant effort to provide the necessary funding to ensure the proper functioning of the lab.

2) JUDICIAL AND PROSECUTION SYSTEM

The foundation of substantive criminal law in Pakistan is laid by the Pakistan Penal Code, which defines offenses and their penalties [74]. The Code of Criminal Procedure, established in 1898, provides rules for preventing crimes and prosecuting

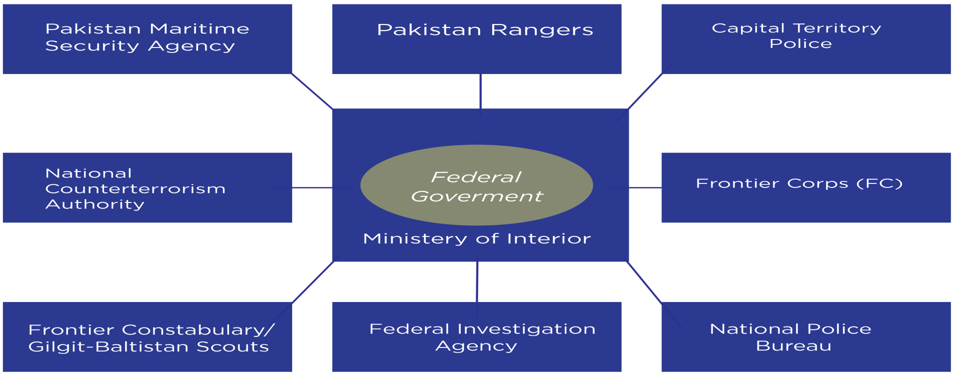

Pakistan Maritime Security Agency
Pakistan Rangers
Capital Territory Police
National Counterterrorism Authority
Federal Goverment
Ministery of Interior
Frontier Corps (FC)
Frontier Constabulary/ Gilgit-Baltistan Scouts
Federal Investigation Agency
National Police Bureau

FIGURE 3. Pakistan Federal Law and Enforcement Organogram.

offenders and supplements the Penal Code [75]. The Ministry of Justice's prosecution division is responsible for prosecuting criminals in practice [76]. The prosecutor oversees investigations conducted by various law enforcement authorities, such as the FIA, and provides legal advice on the best course of action [74]. Some law enforcement agencies have been granted the authority to pursue charges if they have strong reason to suspect a case has been made [75]. Under the Prevention of Electronic Crimes Act (PECA), the Federal Investigation Agency has been designated as the investigation agency in charge of investigating and prosecuting cases of cybercrime and other crimes committed using electronic devices [38]. The Court of Sessions and higher courts will consider such cases when the presiding judge has completed training in computer sciences, cyber forensics, electronic transactions, and data protection [20].

In Pakistan, the Prevention of Electronic Crimes Act (PECA) grants the Pakistan Telecommunication Authority the power to regulate the activities of telecom providers and block illegal internet content [38]. The Federal Investigation Agency (FIA) is responsible for investigating and prosecuting cases of cybercrime under PECA [13]. However, Pakistani law enforcement prosecutors often lack the skills needed to successfully prosecute these cases in court [38].

To address this issue, the Chief Justice should supervise the prosecution of all cyber-related offenses, and only judges who have received training in the admissibility of digital and electronic evidence should preside over these cases [75]. The police administration should identify officers who need training in technology and computer crime, and the federal government may provide financing for security agencies to pursue higher education in countries with advanced cyber security systems [20]. The National Forensic Science Agency (NFSA) provides forensic investigative services and training to law enforcement agencies, but adequate funding is needed to maintain and upgrade its Forensic Lab and Crime Scene Unit [31]. The FIA and other law enforcement organizations should also receive regular training to handle cases containing digital evidence. To prevent role duplication, each institution's capabilities should be appraised and resources effectively mobilized.

E. CAPACITY BUILDING PROGRAMS

Given the technological focus of cybercrime investigations, there are also several socio-economic and political consequences [29]. Establishing the necessary human and institutional capacity to effectively conduct digital investigations is crucial in fostering the growth of well-trained cyber forensic specialists [16]. This requires considering factors such as guidelines for forensic investigators, certification and accreditation for cyber forensic experts, training programs in cyber forensics, academic curriculum, and opportunities for research and development when building capacity [10]. These are essential components for creating a workforce equipped to handle cybercrime investigations at all stages of national development [6].

1) COURSES IN HIGHER EDUCATION AND TRAINING

Compared to the United States and the United Kingdom, Pakistan has a more complex educational system [41]. The Higher Education Commission (HEC) is responsible for maintaining the quality and standards of all tertiary education, both public and private, in Pakistan [77]. For a tertiary institution to offer higher education courses, it must first be accredited by the HEC, which also oversees high educational degree programs and assesses the infrastructure and academic faculty. Private universities are self-funded while public institutions are supported by the government [78]. Unlike in the UK, where the Universities and College Admission System (UCAS) provides a central admission system that allows students to research and compare universities digitally through their websites, Pakistan currently lacks a similar system. A thorough research and evaluation of the institutions' programs can be conducted through an online platform [31].

Forensic science courses are now a part of most countries' educational systems [24]. In the United States, over 150 colleges offer over 417 digital and forensic science courses [33], in the United Kingdom over 68 authorized institutions offer over 337 forensic science programs (UCAS, 2020), and in Australia over 54 universities offer over 206 forensic science courses (AAFS-FEPAC, 2021). However, forensic science has been neglected in Pakistan for a long time. Despite ongoing efforts to construct and maintain forensic laboratories to support criminal investigations, there are only a few reputable colleges that offer graduate-level forensic science programs [73]. Figure 4 illustrates a comparison of the number of forensic courses offered in Pakistan with those in other countries. To address this, authorities have been working to update the country's forensic science infrastructure since 2001. In 2002, the National Forensic Science Agency was established with departments for crime scene investigation, trace chemistry, questioned documents, and cyber forensics, but its goals of providing teaching and training facilities and creating other forensic science laboratories have not yet been achieved [73].

Pakistani universities offer programs in forensic sciences at the undergraduate, graduate, postgraduate, and doctoral levels [79]. Despite the fact that graduates of these courses have employment chances, the infrastructure for these courses is inadequate. Every university degree program focuses on more than just skills or knowledge. Many public institutions, including the Pakistan Federal Investigation Agency (FIA), the Intelligence Bureau (IB), and other LEAs, have voiced a need for cyber forensic experts and cyber security professionals in the case of cyber forensic. There are also twelve other different forensic labs and available forensic science courses in different universities [21], [34]. Universities are making every effort to work closely with Pakistani national organizations, such as NR3C (FIA), Pakistan Air Force (PAF), Army, Navy, and Police, to address their current problems and offer aid in fields where they lack research knowledge.

At the undergraduate, graduate, postgraduate, and doctoral levels, Pakistani universities offer programs in forensic sciences [79]. Despite the availability of employment opportunities for graduates of these courses, the infrastructure supporting these programs is insufficient. Every university degree program focuses on more than just skills or knowledge. Several public institutions, including the Pakistan Federal Investigation Agency (FIA), the Intelligence Bureau (IB), and other law enforcement agencies, have expressed a need for cyber forensic experts and cyber security professionals in the case of cyber forensics [48]. There are also twelve different forensic labs and a variety of forensic science courses available in different universities [21], [34]. To address current problems and fill in knowledge gaps, universities are working closely with national organizations, such as the NR3C (FIA), Pakistan Air Force (PAF), Army, Navy, and Police

2) ACCREDITATION CERTIFICATION AND GUIDELINES FOR FORENSIC PROFESSIONALS

In order to guarantee the credibility of forensic evidence in digital crime convictions, courts must be seen as having a zero-tolerance policy, as even minor errors could lead to an unjust outcome [80]. Mistakes in cyber forensic investigations that result in wrongful prosecution can generate widespread doubt in the field. To ensure the quality of forensic services, it is crucial to have accreditation, guidelines, and standardization of cyber forensic procedures. The ACPO and NIST principles are the basis for cyber forensic inquiries in the UK and US respectively [24], but such guidelines do not exist in Pakistan. This means that the FIA cybercrime unit, which provides most of the forensic services, lacks established rules. Without proper guidelines in place, inconsistencies may arise in CFIs across the country, especially when electronic equipment needs to be searched and confiscated for investigation purposes [39]. Adopting and modifying the ACPO guidelines for Pakistan's CFI could benefit both internal and external digital investigation practitioners and serve as professional guidelines. Currently, there is no accreditation process for establishing cyber forensic labs by public or private forensic service providers. While there are standards for managing, evaluating, and presenting digital evidence, such as NIST, which is a norm in the cybersecurity industry, there is no governmental authority responsible for accrediting cyber forensic labs. Furthermore, the certification of cyber forensic practitioners is also an issue, as all personnel providing cyber forensic services should be certified to ensure quality standards and services.

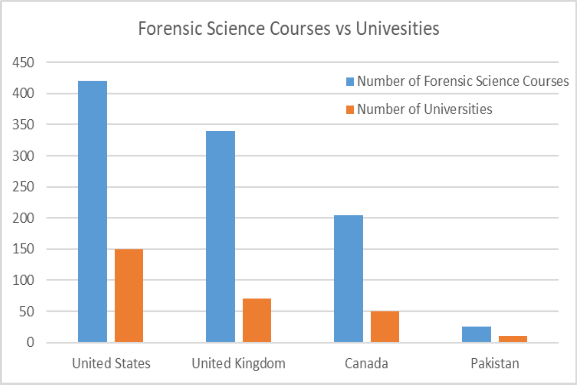


FIGURE 4. Forensic science courses in developed countries and Pakistan.

3) RESEARCH AND DEVELOPMENT

The decisions made in most industrialized nations, particularly in the US and UK, regarding scientific matters are usually supported by research and empirical investigation. This has made academic institutions and research organizations crucial in national debates. However, in Pakistan, the development of Cyber Forensic Investigations (CFIs) is limited both in academia and in the private sector. Evidence suggests that there may be a research deficit in areas such as technology, leadership, and supervision responsibilities [47]. Even in countries with a long history of forensic science, such as the UK, there is a growing demand for research to improve service quality. This article highlights the research gap in CFI in Pakistan and the pressing need for a concerted research effort to support cybercrime convictions in Pakistani courts. National decisions on cyber forensics and security often rely on anecdotal evidence rather than verifiable data. Research is crucial in shaping CFI planning in Pakistan, as it serves as the foundation of scientific decision-making.

The country's research and development budget is meagre compared to other industrialized nations [81]. According to the World Bank, Pakistan's R&D spending was 0.24% of GDP in 2017. In comparison, the UK's R&D spending reached a record high of £15.3 billion in 2020. To address the research deficit in cyber security, the National Forensic Science Agency (NFSA) should consider establishing a national research center for cutting-edge solutions. Figure 5 shows a decline in expenditure on R&D in Pakistan over the past 20 years, indicating that the country may not be prioritizing research and development.

The national organizations in charge of CFI and prosecution require reform. The UK and the US, while the ACPO and NIST, respectively, offer thorough guidelines for investigations, do not have the same recommendations as Pakistan. The ACPO and NIST could be implemented and modified to accommodate Pakistan's legal system as a set of guidelines for both internal and external digital evidence providers. The skills of Cyber Crime Investigaton in Law Enforcement Agencies must be improved. cyber forensic services in Pakistan are not regulated, accredited, or certified, which is quite concerning. Due to subpar forensic services, there may be a miscarriage of justice as a result. Therefore, it is laudable and urgent to move forward with the proposal of establishing a National Center for Cyber Security to oversee all facets of cybersecurity, cybercrime investigation and laws. To stop the provision of dubious services, the Pakistan Telecommunication Authority (PTA) may be instructed to oversee and supervise cyber-crime investigations. The government should fund cutting-edge research at institutes that can help create a national plan for forensics and cybersecurity in light of the growth in cybercrime. The organizations responsible for cyber forensic investigation (CFI) and prosecution in Pakistan require reforms to ensure the quality of their services [34]. Currently, there are no guidelines or standards in place to guide CFI, unlike the UK and the US, where the ACPO and NIST provide thorough principles for investigations. The ACPO and NIST could serve as a model for Pakistan and be modified to fit the country's legal system, serving as guidelines for both internal and external digital evidence providers. Improving the skills of law enforcement agencies in cybercrime investigation is also crucial.

The absence of proper regulation, certification, and accreditation for digital forensic services in Pakistan raises alarm as it poses the risk of wrongful convictions and undermines confidence in the credibility of such services [48]. To address this, the establishment of a National Center for Cyber Security to oversee all aspects of cybersecurity, cybercrime investigation, and laws is highly recommended. The Pakistan Telecommunication Authority (PTA) can be tasked with overseeing and supervising cybercrime investigations to prevent the provision of unreliable services. The government should also invest in cutting-edge research at institutions to create a comprehensive national plan for forensics and cybersecurity in response to the growing threat of cybercrime.

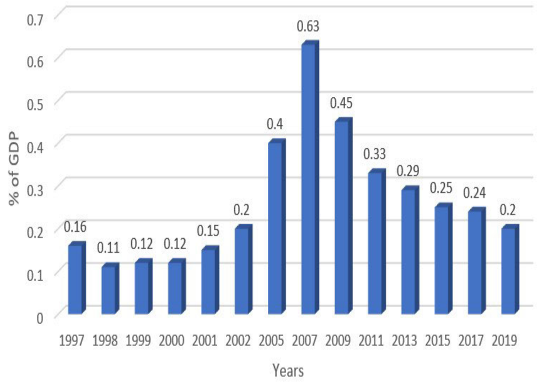


FIGURE 5. Pakistan's spending on research and development (% of GDP). Source: World Bank [82].

F. COOPERATIVE VENTURE

The report on computer networks states that corporations are heavily dependent on the infrastructure that supports the modern economy for their commercial, business, and financial transactions, as well as informational, infrastructure, and government operations [21]. These operations make corporations susceptible to both intentional and unintentional attacks from various hostile forces, such as terrorist organizations and government-sponsored espionage [83]. The threats to the privacy and security of enterprise information are diverse and numerous. Due to a lack of education on these vulnerabilities in academic institutions, some dangers and techniques for combating them may be obvious, while others may not. Cybercrime has become a global phenomenon that crosses national borders and sectoral boundaries, making it necessary for all stakeholders to work together to develop a coordinated strategy for combating it. This means that all sectors and specialties must be involved in investigating cybercrime and that participating in international conferences, organizations, and public-private partnerships can help improve forensic analysis capabilities and increase the chances of catching and convicting criminals [21]. National and international cooperation procedures, partnerships, and information exchange routes need to be reemphasized to ensure effective investigation and resolution of cybercrime.

Despite the global emphasis on making the internet a safe place, Pakistan is lagging behind in terms of cybersecurity efforts [46]. This is reflected in its failure to ratify international agreements aimed at reducing cybercrime. The Budapest Convention on Cybercrime [84], the world's first multilateral convention on this matter, calls on its member states to align their national laws to tackle cybercrime [85]. By signing onto this convention, Pakistan would have a unified strategy to protect its citizens from cyber threats and improve international cooperation in cybercrime investigations [48]. Ratifying the Budapest Convention would also allow Pakistan to track and punish individuals from member states who engage in illegal cyber activities and help trace attacks from hostile cyberspaces.

Pakistan is still considering whether to ratify the Budapest Convention on Cybercrime, a multilateral treaty aimed at harmonizing national laws to combat cybercrime [48]. The government is concerned that sharing data with international law enforcement agencies may infringe on national sovereignty. The treaty must be enacted through legislative means, and its implementation is not a simple formality. However, various international organizations such as the World Bank and UNODC have provided training for law enforcement and government personnel in cybercrime investigation [17]. To effectively prevent cybercrime in the country, law enforcement agencies need to collaborate more closely to avoid duplicated forensic investigations and prosecutions. Universities and institutions from across Pakistan can come together to pool resources such as manpower and equipment to build knowledge in the field. Enhanced international cooperation, particularly with the US and UK, could also aid Pakistan in developing its capacity for cyber forensics. Collaboration between academic institutions and research professionals is encouraged, and universities offering cyber forensics courses should establish exchange programs with firms to provide hands-on learning opportunities for students.

V. CONCLUSION

The current cyber landscape of Pakistan is facing numerous challenges, including a lack of cyber security awareness, a shortage of trained personnel, and a weak investigation infrastructure. Moreover, Pakistan is particularly vulnerable to cybercrime challenges, as it lags in technological and organizational initiatives. The implementation of CFIs holds great potential in addressing these challenges and improving the overall cyber security posture of the country. By providing a structured and comprehensive approach to identifying and investigating cybercrime, CFI can help to build a more secure and resilient cyber environment in Pakistan. While the implementation of CFI may hold potential in addressing some of the challenges facing the current cyber landscape of Pakistan, there are concerns about its efficacy and feasibility. For instance, the allocation of sufficient resources and funding towards CFI may prove to be a challenge, especially in a country where there is a limited budget for cybersecurity initiatives. Additionally, the shortage of trained personnel may also affect the implementation of CFI, as the lack of skilled professionals would limit its ability to effectively address the complex cyber threats facing the country. Furthermore, the legal and ethical implications of CFI, such as the protection of personal data and privacy rights, must be carefully considered and addressed to ensure that its implementation aligns with the values and principles of the country. It is important to ensure that the implementation of CFI is guided by proper legal, ethical, and technical frameworks to protect the privacy and rights of individuals and organizations. In conclusion, CFI represents a crucial step towards strengthening the cyber security posture of Pakistan and addressing the challenges facing its current cyber landscape.

REFERENCES

[1] R. E. Nduka and V. Basdeo, "The need for harmonised and specialised global legislation to address the growing spectre of cybercrime," *Southern Afr. Public Law*, vol. 36, no. 2, pp. 22–31, Jan. 2022.

[2] M. Bolpagni, "Cyber risk index: A socio-technical composite index for assessing risk of cyber attacks with negative outcome," *Qual. Quantity*, vol. 56, no. 3, pp. 1643–1659, Jun. 2022.

[3] K. J. Zuberi, "The attacks on the critical infrastructure of Pakistan," *Int. J. Electron. Crime Invest.*, vol. 5, no. 3, pp. 1–2, Dec. 2021.

[4] V. Vasyukov and Z. I. Khisamova, "Investigation and seizure of electronic media in the production of investigative actions," *Law, State Telecommun. Rev.*, vol. 13, no. 2, pp. 78–88, Sep. 2021.

[5] U. Haq and Q. Atta, "Cyber security and analysis of cyber-crime laws to restrict cyber crime in Pakistan," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 62–69, Jan. 2019.

[6] H. Arshad, A. B. Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," *J. Inf. Process. Syst.*, vol. 14, no. 2, pp. 346–376, 2018.

[7] G. Horsman and N. Sunde, "Unboxing the digital forensic investigation process," *Sci. Justice*, vol. 62, no. 2, pp. 171–180, Mar. 2022.

[8] N. M. Karie, V. R. Kebande, H. S. Venter, and K.-K.-R. Choo, "On the importance of standardising the process of generating digital forensic reports," *Forensic Sci. Int., Rep.*, vol. 1, Nov. 2019, Art. no. 100008.

[9] M. Barrett, "Framework for improving critical infrastructure cybersecurity version 1.1," Nat. Inst. Standards Technol., USA, Tech. Rep., 2018, doi: 10.6028/NIST.CSWP.04162018.

[10] U. P. Khan and M. W. Anwar, "Cybersecurity in Pakistan: Regulations, gaps and a way forward," *Cyberpolitik J.*, vol. 5, no. 10, pp. 205–218, 2020.

[11] M. A. Qadeer, "The cyber threat facing Pakistan," The Diplomat, Jun. 2020. [Online]. Available: https://thediplomat.com/2020/06/the-cyberthreat-facing-pakistan/

[12] M. I. Khan and M. Ayub, "Cyber-Warfare: Implications for the national security of Pakistan," *NDU J.*, pp. 117–132, 2020. Accessed: Sep. 26, 2022. [Online]. Available: https://ndu.edu.pk/ndu-journal/pub/06-Cyber-Warfare.pdf

[13] F. Aziz, "Pakistan's cybercrime law: Boon or bane? Heinrich-Böll Stiftung," Feb. 2018. [Online]. Available: https://www.boell.de/en/2018/02/07/pakistans-cybercrime-l

[14] (2020). *Global Cybersecurity Index*. [Online]. Available: https://www.itu.int/myitu/-/media/publications/2021-publicationsGlobal-Cybersecurity-Index-2020

[15] R. Zahoor, M. A. Safdar, W. Rafiq, and F. A. Rana, "Cyber war in a cyber-led world and legislative measurements taken by Pakistan," *Competitive Social Science Res. J.*, vol. 3, no. 2, pp. 151–158, 2022.

[16] K. Shaukat, S. Luo, S. Chen, and D. Liu, "Cyber threat detection using machine learning techniques: A performance evaluation perspective," in *Proc. Int. Conf. Cyber Warfare Secur. (ICCWS)*, Oct. 2020, pp. 1–6.

[17] A. Raza, W. Shah, and T. Khan, "Domestic legal responses to terrorism: An analysis of Pakistan's counterterrorism legislation through the framework of usled international norm creation," *Pakistan J. Int. Affairs*, vol. 4, no. 4, pp. 1–11, 2021.

[18] E. A. Vincze, "Challenges in digital forensics," *Police Pract. Res.*, vol. 17, no. 2, pp. 183–194, 2016.

[19] S. Even and D. Siman-Tov, "Front matter," in *Cyber Warfare: Concepts and Strategic Trends*. Institute for National Security Studies, 2012, pp. 1–4. [Online]. Available: http://www.jstor.org/stable/resrep08940.1

[20] R. Hasan, Y. Zheng, and J. T. Walker, "Digital forensics education modules for judicial officials," in *Proc. Nat. Cyber Summit*. Cham, Switzerland: Springer, 2020, pp. 46–60.

[21] T. U. Rehman, "International cooperation and legal response to cybercrime in Pakistan," in *Encyclopedia of Criminal Activities and the Deep Web*. Hershey, PA, USA: IGI Global, 2020, pp. 424–434.

[22] A. Al-Dhaqm, S. A. Razak, D. A. Dampier, K.-K. R. Choo, K. Siddique, R. A. Ikuesan, A. Alqarni, and V. R. Kebande, "Categorization and organization of database forensic investigation processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020.

[23] E. Barker, M. Smid, and D. Branstad, "A profile for U.S. federal cryptographic key management systems," Special Publication (NIST SP), Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2015. Accessed: Sep. 21, 2022, doi: 10.6028/NIST.SP.800-152.

[24] Y. S. S. Al-Husaini, "Enhancing cloud forensic investigation relationships between law enforcement and local cloud service providers: Oman as a case study," Ph.D. thesis, School Accounting, Inf. Syst. Supply Chain, College Bus. Law, RMIT Univ., Melbourne, VIC, Australia, 2022.

[25] S. Ullah, M. Amir, M. Khan, H. Asmat, and K. Habib, "Pakistan and cyber crimes: Problems and preventions," in *Proc. 1st Int. Conf. Anti-Cybercrime (ICACC)*, Nov. 2015, pp. 1–6.

[26] *Directory of Criminal Justice Information Sources*, National Institute of Law Enforcement, Criminal Justice, National Criminal Justice Reference Service (U.S.), and Aspen Systems Corporation, Wheat Ridge, CO, USA, 1986.

[27] R. A. Ramadhan, P. R. Setiawan, and D. Hariyadi, "Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on ISO/IEC 27037:2012 and NIST SP800-86 framework," *IT J. Res. Develop.*, vol. 2022, pp. 162–168, Feb. 2022.

[28] A. Ali, "Cyber security policing: Analysing national cyber security policies of India and Pakistan," *Inst. Regional Stud.*, vol. 40, no. 8 (1), 2022. [Online]. Available: http://irs.org.pk/Spotlight/SP08012022.pdf

[29] K. Shaukat, A. Rubab, I. Shehzadi, and R. Iqbal, "A socio-technological analysis of cyber crime and cyber security in Pakistan," *Transylvanian Rev.*, vol. 1, p. 84, Jan. 2017.

[30] L. Y. Chang, "Legislative frameworks against cybercrime: The Budapest convention and Asia," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham, Switzerland: Palgrave Macmillan, 2020, pp. 327–343.

[31] F. A. Faisal, S. A. S. Kazmi, and H. Abbas, "Growing digital vulnerability: A case study of threats to Pakistans national assets," in *Proc. Int. Conf. Commun. Technol. (ComTech)*, Sep. 2021, pp. 79–84.

[32] J. Lusthaus, "Cybercrime in Southeast Asia," Austral. Strategic Policy Inst., Australia, Tech. Rep. 29/2020, 2020.

[33] G. Peterson and S. Shenoi, *Advances in Digital Forensics XIV*. Cham, Switzerland: Springer, 2018.

[34] M. F. Khan, A. Raza, and N. Naseer, "Cyber security and challenges faced by Pakistan," *Pakistan J. Int. Affairs*, vol. 4, no. 4, pp. 1–10, 2021.

[35] G. Khan, S. Bashir, F. Shahzad, and S. U. Jan, "Federal investigation agency against the crime of book piracy in Pakistan," Library Philosophy Pract. (e-J.), 2021. [Online]. Available: https://digitalcommons.unl.edu/libphilprac/5034

[36] R. Apau and F. N. Koranteng, "Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior," *Int. J. Cyber Criminol.*, vol. 13, no. 2, pp. 1–10, 2019.

[37] M. Trucano, *Saber-ICT Framework Paper for Policy Analysis: Documenting National Educational Technology Policies Around the World and Their Evolution Over Time*. Washington, DC, USA: World Bank, 2016.

[38] S. Khan, P. M. Tehrani, and M. Iftikhar, "Impact of PECA-2016 provisions on freedom of speech: A case of Pakistan," *J. Manage. Info*, vol. 6, no. 2, pp. 7–11, Jun. 2019.

[39] N. Afridi, "The current status of forensic science and its impact on administration of criminal justice system in Pakistan: An analytical study," *SSRN*, 2021, doi: 10.2139/ssrn.3781586.

[40] E. A. Khan, "The prevention of electronic crimes act 2016: An analysis," *LUMS LJ*, vol. 5, p. 117, Jan. 2018.

[41] T. U. Rehman, M. A. Usmani, and S. Parveen, "A critical analysis of the criminal justice system in Pakistan," *Pakistan J. Int. Affairs*, vol. 4, no. 4, pp. 1–22, 2021.

[42] A. Shan, A. Basit, and M. M. Azhar, "Democratization in Pakistan: Role of media in civilian and military regimes," *Global Regional Rev.*, vol. 2, no. 1, pp. 405–416, Dec. 2017.

[43] *E-Services*, Pakistan Telecommunication Authority, Islamabad, Pakistan, 2019.

[44] A. K. Afridi, M. A. Ashraf, M. Hasan, M. Idrees, and T. M. Amin, "Action plan 2011 for IT-BPO industry of Pakistan," Unpublished Graduate Res. Project, Inst. Bus. Admin., Pakistan, 2011. [Online]. Available: https://ir.iba.edu.pk/research-projects-mba/162

[45] S. E. Blythe, "Pakistan goes digital: The electronic transactions ordinance as a facilitator growth for e-commerce," *J. Islamic St. Prac. Int. L.*, vol. 2, p. 5, Jan. 2006.

[46] A. Munir and M. T. Gondal, "Cyber media and vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan," *Global Media J., Pakistan Ed.*, vol. 10, no. 2, pp. 1–4, 2017.

[47] E. Irfan, Y. Ali, and M. Sabir, "Analysing role of businesses' investment in digital literacy: A case of Pakistan," *Technol. Forecasting Social Change*, vol. 176, Mar. 2022, Art. no. 121484.

[48] J. Jamshed, W. Rafique, K. Baig, and W. Ahmad, "Critical analysis of cybercrimes in Pakistan: Legislative measures and reforms," *Int. J. Bus. Econ. Affairs*, vol. 7, no. 1, pp. 10–22, 2022.

[49] C. McCartney and E. Amoako, "The U.K. forensic science regulator: A model for forensic science regulation," *Ga. St. UL Rev.*, vol. 34, p. 945, Jan. 2017.

[50] J. Williams, "ACPO good practice guide for digital evidence (2011)," Assoc. Chief Police Officers, London, U.K., Tech. Rep., 43, 2014.

[51] P. Owen and P. Thomas, "An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines," *Digit. Invest.*, vol. 8, no. 2, pp. 135–140, Nov. 2011.

[52] M. G. Baron, T. Rohrig, and J. Gonzalez-Rodriguez, "Forensic science in the U.K. Part III: Regulation of forensic science in England and Wales–The role of the forensic science regulator," *Forensic Sci. Rev.*, vol. 32, no. 1, pp. 2–7, 2020.

[53] P. Reedy, "Interpol review of digital evidence 2016–2019," *Forensic Sci. Int., Synergy*, vol. 2, pp. 489–520, Jan. 2020.

[54] J. Robertson, "Forensic science—It's bigger than you think!" *Austral. J. Forensic Sci.*, vol. 48, no. 4, pp. 363–365, Jul. 2016.

[55] W. G. Kruse and J. G. Heiser, *Computer Forensics: Incident Response Essentials*. London, U.K.: Pearson, 2001.

[56] G. Palmer, "A road map for digital forensics research," Rep. First Digit. Forensics Res. Workshop (DFRWS), Tech. Rep. DTRT001-01, 2001

[57] M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *Int. J. Digit. Evidence*, vol. 1, no. 3, pp. 1–12, 2002.

[58] B. D. Carrier and E. Spafford, "Getting physical with the digital investigation process," *Int. J. Digit. Evidence*, vol. 2, no. 2, pp. 1–20, 2003.

[59] V. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," *Digital Invest.*, vol. 2, no. 2, pp. 1–36, 2004.

[60] S. Ciardhuáin, "An extended model of cybercrime investigations," *Int. J. Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004.

[61] K. Kent, S. Chevalier, and T. Grance, "Guide to integrating forensic techniques into incident," Nat. Inst. Standards Technol., USA, Tech. Rep., 800-86, 2006.

[62] D. Chris and D. David, "A new approach of digital forensic model for digital forensic investigation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 12, pp. 1–10, 2011.

[63] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–131, 2011.

[64] R. B. Adams, V. Hobbs, and G. Mann, "The advanced data acquisition model (ADAM): A process model for digital forensic practice," *J. Digit. Forensics, Secur. Law*, vol. 8, no. 4, pp. 25–48, 2013. [Online]. Available: https://researchportal.murdoch.edu.au/discovery/fulldisplay/alma991005543937007891/61MUN_INST:ResearchRepository

[65] H. I. Bulbul, H. G. Yavuzcan, and M. Ozel, "Digital forensics: An analytical crime scene procedure model (ACSPM)," *Forensic Sci. Int.*, vol. 233, nos. 1–3, pp. 244–256, 2013.

[66] A. Valjarevic and H. S. Venter, "A comprehensive and harmonized digital forensic investigation process model," *J. Forensic Sci.*, vol. 60, no. 6, pp. 1467–1483, 2015.

[67] R. Montasari, "A comprehensive digital forensic investigation process model," *Int. J. Electron. Secur. Digit. Forensics*, vol. 8, no. 4, pp. 285–302, 2016.

[68] N. Malik and T. A. Qureshi, "A study of economic, cultural, and political causes of police corruption in Pakistan," *Policing, A J. Policy Pract.*, vol. 15, no. 2, pp. 1446–1462, 2021.

[69] R. Montasari and R. Hill, "Next-generation digital forensics: Challenges and future paradigms," in *Proc. IEEE 12th Int. Conf. Global Secur., Saf. Sustainability*, Jan. 2019, pp. 205–212.

[70] X. Cai, K. Shi, K. She, S. Zhong, and Y. Tang, "Quantized sampled-data control tactic for TS fuzzy NCS under stochastic cyber-attacks and its application to truck-trailer system," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7023–7032, Jul. 2022.

[71] X. Cai, K. Shi, K. She, S. Zhong, Y. Soh, and Y. Yu, "Performance error estimation and elastic integral event triggering mechanism design for T–S fuzzy networked control system under DoS attacks," *IEEE Trans. Fuzzy Syst.*, vol. 31, no. 4, pp. 1327–1339, Apr. 2023.

[72] A. Kershaw, "Professional standards, public protection and the administration of justice," in *Handbook of Forensic Science*. Willan, 2019, pp. 580–605. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9781843927327-27/professional-standards-public-protection-administration-justice-alan-kershaw

[73] R. M. Mateen and A. Tariq, "Crime scene investigation in Pakistan: A perspective," *Forensic Sci. Int., Synergy* vol. 1, pp. 285–287, Jan. 2019.

[74] K. Sarwar, "The offence of abetment liable to capital punishment under the Islamic criminal law and the Pakistan penal code," *Al-Azhār*, vol. 8, no. 1, pp. 101–110, 2022.

[75] A. Hussain, S. Akhtar, and M. Hassan, "Studying the causes of delay in criminal trials under the criminal justice system of Pakistan," *Proc. Global Sociol. Rev.*, vol. 6, no. 2, pp. 52–58, 2021.

[76] F. K. Boachie, "ICT infrastructure required for sustainable library services in the 21st century issues and challenges from a developing country's perspective," in *Proc. 5th Int. Symp. Emerg. Trends Technol. Libraries Inf. Services (ETTLIS)*, 2018, pp. 12–15.

[77] A. Ayaz and M. Y. Sharjeel, "Evaluation of quality assurance scheme for higher education institutions of Karachi (Pakistan) by the HEC," *Pakistan J. Appl. Econ.*, vol. 30, no. 2, pp. 283–297, 2020.

[78] S. Ansari, J. Poncela, P. Otero, A. Ansari, and O. Mahfooz, "Research in Pakistan: Structure, funding and results," *Pakistan J. Eng., Technol. Sci.*, vol. 5, no. 1, pp. 1–19, 2016.

[79] S. Cordner and M. Tidball-Binz, "Humanitarian forensic action-its origins and future," *Forensic Sci. Int.*, vol. 279, pp. 65–71, Jan. 2017.

[80] G. Tully, "Forensic science and forensic pathology: Quality standards and risks," *Medico-Legal J.*, vol. 85, no. 3, pp. 117–129, 2017.

[81] B. Dachs and G. Zahradnik, "From few to many: Main trends in the internationalization of business R&D," *Transnational Corporations J.*, vol. 29, no. 1, pp. 1–10, 2022.

[82] *Research and Development Expenditure*, UNESCO Institute for Statistics (UIS), Paris, France, 2019.

[83] B. A. Downes, "Desperate times, desperate measures: The causes of civilian victimization in war," *Int. Secur.*, vol. 30, no. 4, pp. 152–195, 2006.

[84] J. de Arimatéia da Cruz, "The legislative framework of the European Union (EU) convention on cybercrime," in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cambridge, MA, USA: MIT Press, 2020, pp. 223–237.

[85] M. Watney, "Analysing different approaches to cross-border electronic evidence data-sharing in criminal matters," in *Proc. Int. Conf. Cyber Warfare Secur.*, 2019, p. 484.

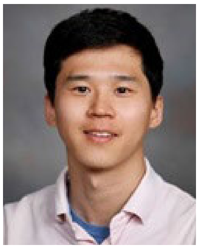
EHTISHAM UL HAQUE received the bachelor's degree in computer science with a major in networking. He is currently pursuing the master's degree in cybersecurity with Muslim Youth University, Islamabad, Pakistan. His research interests include digital forensics, the Internet of Things security, blockchain, software defined networking, and artificial intelligence.

WASEEM ABBASI received the Ph.D. degree in electrical engineering specialization in control system from the Capital University of Science and Technology, Islamabad, Pakistan, in 2018. He is currently an Assistant Professor with the Computer Science and IT Department, Superior University, Sargodha, Pakistan. From 2019 to 2020, he was a Postdoctoral Research Associate with the Network Robotic Systems Laboratory, National Cheng Kung University, Taiwan. He has published more than 16 research publications in well reputed international journals and conferences. His research interests include stabilization of nonholonomic systems, cooperative control for multi mobile robots, robust control, nonlinear control, and adaptive control. He is also the Guest Editor of the Special Issue on Advances in Grounded and Aerial Unmanned Robots in the *International Journal of iRobotics* and also a reviewer of many well-reputed international journals and conferences.

SATHISHKUMAR MURUGESAN (Member, IEEE) received the B.Sc. degree in mathematics from the Government Arts College, Coimbatore, India, in 2009, the M.Sc. and M.Phil. degrees in mathematics from the Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Bharathiar University, India, in 2011 and 2013, respectively, and the Ph.D. degree in mathematics from Anna University, Chennai, India, in 2018. He was an Assistant Professor with the Department of Mathematics, Christ the King Engineering College, Coimbatore, from 2013 to 2014. He is currently a Postdoctoral Research Associate with the Department of Mechanical Engineering, National Cheng Kung University, Tainan, Taiwan. His current research interests include networked control system and its security control, multi-agent systems, and time-delay systems.

MUHAMMAD SHAHID ANWAR is currently an Assistant Professor with the Department of AI and Software, Gachon University, South Korea. His research interests include the measurement, modeling, and evaluation of the quality of experience (QoE) of immersive content and applications e.g., 360-degree videos and immersive media, AR/VR/MR, and VR telemedicine and healthcare systems.

FAHEEM KHAN received the Ph.D. degree in computer science from the University of Malakand, Khyber Pakhtunkhwa, Pakistan. He was an Assistant Professor in Pakistan for four years and supervised many papers and students. Since April 2021, he has been an Assistant Professor with the Department of Computer Engineering, Gachon University, South Korea. His research interests include computer networking, wireless networking, MANET, sensor networking, the IoT, artificial intelligence, and AI in healthcare systems.



YOUNGMOON LEE (Member, IEEE) received the B.S. degree in electrical and computer engineering from Seoul National University, South Korea, in 2014, and the M.S. and Ph.D. degrees in computer science and engineering from the University of Michigan, Ann Arbor, in 2016 and 2019, respectively. He is currently an Assistant Professor with the Robotics Department, Hanyang University, South Korea. His research interests include real-time AI and ML, robotic sensing and applications, cyber-physical and embedded systems, and computer systems and networks.