OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 1 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

ASSESSING CYBERSECURITY CHALLENGES AND RESPONSE READINESS IN PAKISTAN: A COMPREHENSIVE ANALYSIS

Muhammad Saad Qasim
Department computer science Superior University Lahore

Zeeshan Ahmad
Department computer science Superior University Lahore

Saima Maqsood
Department of biological Sciences Superior University Lahore

Shahroz zafar
Department computer science Superior University Lahore

Dr. Muhammad Azam
Department computer science Superior University Lahore

**Corresponding author:* saadmirzaswl@gmail.com

DOI: https://doi.org/10.71146/kjmr215

Article Info

Abstract

The rapid transformation of the globe into a global village that has been brought about by the enormous rise of information technology. As a result, the distances between places have become more manageable, and information can now travel quickly throughout the world as events unfold. On the other hand, at the same time, it has also provided a boost to vulnerabilities, dangers, frauds, and criminals in the online. The ease of access, hacking tools that are favourable to users, and complexity of cyber assaults have all contributed to an invasion of privacy on the part of people, organizations, and nations. In this day and age, Pakistan is confronted with a myriad of different kinds of cyber threats. In order to determine the nature and dynamics of the danger posed to Pakistan's information and communications technology (ICT) infrastructure and resources, this study conducts an analysis of recent cyber assaults that have been launched against the government, corporate, and private sectors. The research sheds light on a broad spectrum and diversity of cyber risks, including anything from simple website defacement to complex and enduring cyber threat. In addition, the current reaction capacity at the organizational and government levels has been examined, and the deficiencies have been brought to light. It is thought that Pakistan's lack of any regulations pertaining to cyber security, the absence of any reaction mechanisms, and the absence of any organizational structure in the nation may make the country's internet a paradise for criminals and operators and users who intentionally do harm. It should be underlined that the government of Pakistan not only needs to grasp the dangers posed by the internet and the repercussions of its uncontrolled use, but it also needs an effective reaction system in order to protect itself from these dangers. This paper proposes a high level organizational structure for the development of critical cyber security organizations at multiple tiers. These bodies will be responsible for safeguarding the nation's cyber space by enacting appropriate laws and designing the reaction mechanism at different levels of government.

Introduction

The way we think about national security is evolving as a direct result of the revolutionary effects of information and communication technologies (ICT) on our everyday lives, economies, and societies. The most technologically advanced nations are harnessing the full potential of Information and Communication Technologies (ICTs) in areas such as e-governance, online education, digital commerce, and the delivery of public services. Any country that wants to keep up with the rest of the world in the modern day must invest in its people and infrastructure so that they can learn new technologies and apply them. The Internet has many benefits, but it also has some drawbacks. The lack of boundaries or established jurisdiction in cyberspace presents a significant challenge and drawback. As a result, bad actors have a fertile field in which to carry out their illicit acts online with little risk of repercussions.

being caught and getting in trouble. Each country is urged to take initiative in creating a trustworthy and safe online community for all users.

New technologies, an information and communications technology (ICT) foundation, and electronic government services are on the horizon for Pakistan. At the same period of time cyber security threats and technological risks have become more prevalent in the area [1]. Abuse, cyber espionage, and broad disruption of services are on the rise as our society becomes more reliant on ICT. We risk losing credibility in the eyes of the digital public if terrorist groups or hostile nations are allowed unfettered access to Pakistani cyberspace.

Therefore, it is crucial for Pakistan to build an ICT infrastructure with a security framework to properly detect, counteract, and react to cyber-attacks. In light of the current cyber threat environment, this article investigates the preparedness of the government of Pakistan to respond. There are four sections to this study. The paper's second section discusses the current threat landscape in Pakistan's cyber environment. The most significant cyber occurrences of recent years are examined, along with their effects on the state of cyber defenses. In Section III, we assess Pakistan's capability to deal with these challenges in light of the managerial and technological response approaches used by advanced countries. Within Section IV, we propose a framework and a roadmap for Pakistan to establish incident response operations when dealing with cyber threats. The aim is to foster a dependable, conducive, and secure digital environment by building essential technological, intellectual, and human resource infrastructure.

THREAT SCENARIO

A cyber threat, as defined in reference [2], is an unwanted incident that can originate in the digital realm and has the potential to cause harm to individual or state assets, systems, or organizations. The terminology used to describe a cyber threat depends on its origin, the capabilities of its perpetrators, and the severity of the harm they want to inflict. From simple website defacements to more elaborate assaults, Pakistan's IT users and institutions are under constant threat. In this part, we describe and demonstrate in Fig.1 how threats may be categorized according to the degree of complexity in their design, launching method, impact, and motives.

A. Insiders

The workforce is often cited as the cyber security system's weakest link. Two contract workers from the Prime Minister's Secretariat stole confidential information, according to media sources from June 2010 [3]. In this case, the authorities were unable to track down the criminals and bring them to justice. Companies and businesses are in a similar position, with many choosing not to report cybercrime or pursue prosecution of guilty personnel because of a lack of applicable laws and regulations.

B. Defacement of Websites

Most often, hackers will use a technique called "website defacement," which involves damaging the target website via unlawful and criminal behavior [2]. Since a few years ago, Pakistani websites have been hit repeatedly by this kind of cyber assault. Some recent significant defacement instances are shown in table-I below.

Serial	**Victim**	**Attacker**	**Date**
1	20 sites compromised.	Jagwar, India	**26 Jan 2012**
2	2000 sites compromised.	Destroyer Army, India	**15 Aug 2012**
3	Google.pk and 284 other high-profile sites compromised	Eboz, Turkish	**23 Nov 2012**
4	250 sites compromised.	Indishel, India	**8 Dec 2012**
5	Punjab Assembly site compromised	cr4ck-Br4in, Bangladesh	**9 Dec 2012**
6	60 website including gov.pk and edu.pk hacked	BGHH, Bangladesh	**17 Dec 2012**
7	Website of Pakistan's Election Commission compromised	NIGh7 F0x, India	**29 Mar 2013**
8	57 sites compromised	Afghan Cyber Army, Afghanistan	**Jul-Aug 2013**
9	**Website of Pakistan Army compromised**	**GODZILLA, India**	**9 Aug 2013**

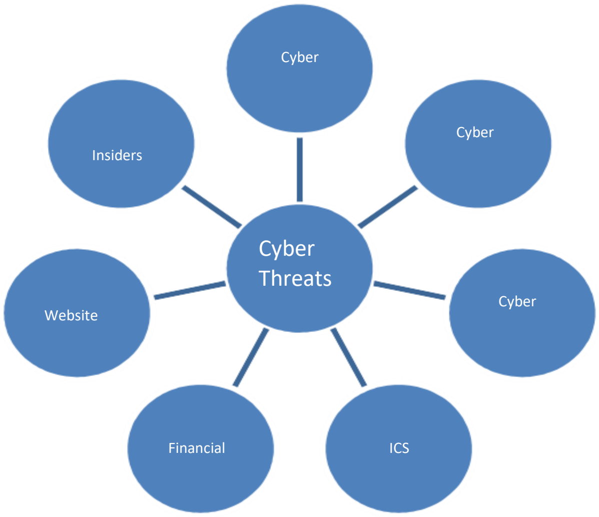
During the initial half of 2013, Tameer Bank, Allied Bank Limited, Habib Bank Limited, Soneri Bank, and Muslim Commercial Bank experienced website breaches allegedly carried out by a suspected Pakistani hacker known by the aliases Dr. Freak and Xploiter, as detailed in reference [4]. Fortunately, these hackers did not cause significant damage to the banks. Instead, their actions served as a warning for these institutions to enhance their security measures.

C. Financial Frauds

Financial fraud encompasses activities such as credit card theft, money laundering, deceit, and the manipulation of lottery outcomes. In Pakistan, the utilization of the internet for shopping, banking, and various financial transactions has been on the rise. Regrettably, cybercriminals and malicious actors view Pakistan as an attractive target due to the absence of comprehensive cyber legislation, a shortage of digital forensics professionals, and the absence of a dedicated cybercrime court.

The popular forex dealer Khanani and KKI. together together with their franchise Dunya Enterprises, were accused of being engaged in money laundering via Hawala, which would be a breach of the terms and conditions put out by the State Bank of Pakistan. In November 2008, the offices of Dunya Enterprises were subjected to a raid by agents from the Federal Investigation Agency (FIA). During the operation, the FIA team discovered incriminating evidence, including a computer, cash receipts, and Hawala cash delivery receipts, as detailed in reference [5].

In the end, FIA Karachi did track down the KKI website servers. The FIA conducted a raid and took control of the KKI website's servers in order to conduct a forensic analysis. Server forensics study connected KKI to transactions processed via the Dunya Enterprises office. However, because to the lack of cyber legislation, just the office was closed and no legal action was taken against those responsible. Most cyber-related financial scams likely go unreported or undetected because no adequate legal framework exists at the national level.



D. Cyber Espionage

There is evidence that India carried out a major cyber espionage effort against the public, private, and defense infrastructures of Pakistan in years between 2009 and 2010. This campaign was carried out in the cyberspace. Interestingly, this operation remained concealed until May 2013, when a Norwegian cybersecurity firm known as "Norman Securities" released a report titled "Unveiling an Indian Cyber-attack Infrastructure" concerning the campaign, which they referred to as Operation Hangover [3]. Among the victims of this campaign was Telenor, a prominent mobile provider in Pakistan headquartered in Norway. Telenor reached out to Norman Security and provided evidence of a security breach within their system.

The comprehensive investigation revealed that the attackers predominantly exploited well-known vulnerabilities in Java, web browsers, and Microsoft Office [9]. System logs from 2009 and 2010 yielded compelling evidence of the cyber-attack, underscoring its sustained nature and the existence of the requisite infrastructure, support modules, and framework. It is suspected that this operation, which spanned nearly three years [7], focused on the theft of substantial amounts of valuable data from a range of sectors, including the military, commercial, public, and private domains.

Detailed studies indicate that the attackers primarily exploited well-known vulnerabilities in Java, web browsers, and Microsoft Office [9]. System logs from 2009 and 2010 also revealed evidence of the cyber assault, highlighting its persistence and the presence of the required infrastructure, support modules, and framework. It is suspected that this nearly three-year-long continuous activity [7] was dedicated to the theft of substantial volumes of valuable data from various sectors, including the military, commercial, public, and private domains.

E. Cyber Spying

Information concerning the NSA's top-secret, super-powerful espionage technology "Boundless informant" was leaked in June 2013 by the prestigious UK publication The Guardian. According to the leaked top

hidden records, Boundless Global surveillance data communications may be recorded, analyzed, and categorized by Informant [10]. There is a visual user interface, and data is reflected on a world map.

In March 2013, the National Security Agency (NSA) amassed a staggering 97 billion pieces of electronic data and conducted telephone monitoring on a global scale. As revealed in a study, the countries that generated the highest number of intelligence reports were Iran, with 14.5 billion reports, and Pakistan, with 13.5 billion reports [11].

A previous article published by the same news site in the end of 2013 [12],[13] revealed specifics regarding the clandestine mass monitoring program me run by the NSA and known as "PRISM." It has been revealed that this programmer, which has been running since 2007, has provided the NSA with unfettered access to the data storage servers of key information technology companies such as Apple, Google, Yahoo, a search Hotmail, and Microsoft. The purpose of this kind of monitoring is to protect national assets, vital intelligence, and valuable electronically stored data from other cyber capabilities in the same way. It is very necessary, for this goal, to construct a cybersecurity infrastructure that is both resilient and comprehensive.

F. Attacks on ICS

The broad use of ICT (industrial control system) has also had a profound effect on the business world. Viruses and worms in networks didn't pose a problem for the older, more closed-off industrial systems. However, Ethernet technology and internet protocols have made their way into the manufacturing sector, leading to the creation of SCADA. However Because of the growing dependence on automated processes, manufacturing processes are more susceptible to malicious cyber activity. In 2010, a worm called Stuxnet was discovered to be the most advanced and well-refined threat to the SCADA system to date[6].

The Stuxnet worm, which attacked an Iranian nuclear facility, slowed down centrifuges used to enrich uranium [7]. According to the findings of an analysis of the virus, Stuxnet was not only targeting Iran but also the nations of Pakistan, India, plus a handful of additional nations in the region of Middle Eastern [8].

Since the early 1990s, Pakistan has adopted SCADA systems within its electricity and communication sectors. Since 1990, for example, the National electricity Controlling Centre (NPCC) in Islamabad has been using a SCADA system in order to monitor and control the electricity distribution network. SCADA systems have been implemented in the operations of a large number of governmental and commercial organizations in Pakistan, in addition to NPCC. These organizations have connected their SCADA systems to either an internet connection or a network of local networks (LAN). These organizations encompass a range of sectors, such as the Sui Southern Gas Company (SSGC), Oil and Gas Development Corporation (OGDC), the Dewan Group of enterprises, and various telecommunications firms [3].

However, it's crucial to acknowledge that without concerted efforts to enhance the security of these systems and provide a safe, reliable networked environment, they remain susceptible to cyber threats similar to the Stuxnet attack.

G. Cyber Terrorism

Terrorism has always posed a serious threat to countries that value international stability. Terrorism, on the other hand, has developed into a modern, specialised crime in the modern world.

Terrorists make extensive use of cyber technologies and the internet. To combat this danger, countries are embracing cutting-edge technology and high-tech weapons. Terrorist-related data may be collected, processed, and analyzed with the use of ICT technologies [9].

Pakistan has the potential to become a very profitable site for such operations in the absence of cyber regulations. Pakistani intelligence agencies broke up an al-Qaida communications center on August 21st, 2013, seizing computers and terrorists. Evidence showed that terrorists were using it as a hub for international communication, with hundreds of mobile SIMs, DSL routers, and multiple broadband internet connections being used to communicate with each other and with targets around the world. Like the KKI case study, it showed that terrorist organizations used illicit money transfers to Afghanistan to fund their operations.

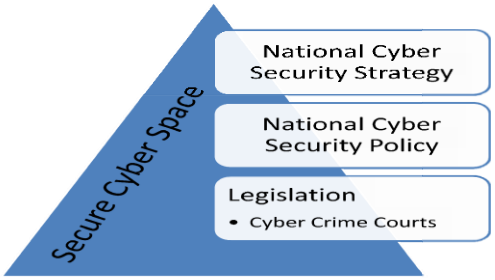
ABILITY TO RESPOND

The safety of essential national assets and infrastructure is under risk due to the increasing complexity of cyber-attacks. Similar to the case of Stuxnet, this attack is likely state-sponsored and directed against another country's vital infrastructure. Similarly, millions of computers were used by the infamous "Bredo lab" botnet, which was controlled from one state and used to attack other states [10]. However, the present trend of cyber-attacks must be met by a sound and corresponding governmental reaction.

Pakistan was ranked sixth and third, accordingly, among the top sources of trash distribution via botnets in 2012, depending to the Average Lifetime of a Bot & the main sources of spam dissemination through botnets [21]. There is currently no institutional framework in place in Pakistan to counteract cyber threats or ensure the secure use of its cyber space. If Pakistan intends to establish itself as a responsible country in the information society, it must launch concerted efforts at the national level. Management and technological responses make up the bulk of the reply mechanism and activities. Although the two parts of a reaction are distinct, they may both be set in motion and established at the same time because of their interdependence. In the next paragraphs, we'll talk about Pakistan's current capabilities with regard to of management and technological reaction.

A. Management Response

Cyberattacks move at such a dizzying rate that conventional response mechanisms can't keep up. Such occurrences may happen very quickly and in large numbers, and they can originate from a wide variety of actors, from lone hackers to whole countries. The complex and ever-changing nature of modern threats necessitates an adaptive and well-coordinated response . Fig.-2 depicts the core elements of a management response, and the status of Pakistan's efforts is addressed below.


Secure Cyber Space
National Cyber Security Strategy
National Cyber Security Policy
Legislation
• Cyber Crime Courts

1) **Strategy for National Cyber Security :**

There are currently over 100 countries with some level of government-level cyber security capability, and of those, over 50% have published their internet safety strategy, outlining their national security objectives and goals [11]. Pakistan, in order to develop a national cyber security policy, must first determine what it hopes to accomplish in this area. This policy for cyber security has to be formulated at the highest possible forum given responsibility for cyber defense.

2) **The National Strategy for Cyber Security:**

Pakistan is among the countries that lack a well-defined cybersecurity strategy. While a National Cybersecurity Policy was drafted by a Cybersecurity Task Force established by the Senate Committee on Defense in July 2013, The senate committees and the task forces both lack the requisite power inside Parliament to successfully put the recommendations they made into practise, hence their recommendations will not be implemented. To effectively accomplish each of the objectives and aims outlined in the national cybersecurity strategy, the Pakistani government should consider engaging ministers and establishing a high-level organizational entity with exclusive responsibility for formulating and executing the nation's cybersecurity policy.

3) **Legislation:**

In 2002, the government of Pakistan introduced the Electronic Transaction Ordinance (ETO) to begin enforcing laws against cybercrime. The first certification of service providers was accomplished by ETO. The law's stated purpose was to promote and record ICT-related electronic transactions and documentation.

The Prevention of Electronic Crimes Ordinance (PECO) was the first cybercrime law enacted by a government in Pakistan in 2009. PECO established the various legal concepts, categories, and penalties associated with cybercrime. However, the National Assembly never took up the ordinance for a vote, and it has since lapsed since it was not promulgated within the required time span .

In the absence of such legislation, cybercrimes committed inside Pakistani internet go unchecked and unpunished. It is past time for the government to enact comprehensive cybercrime laws.

Internet fraud is investigated, and those responsible are brought to justice. It will have a significant impact on the fight against domestic terrorism and financial fraud. Meanwhile, there are no established norms for teaching judges about cybercrime and digital forensics validation. A single and all-encompassing legislative framework for cyber security must contain a cyber-criminal code, misuse of devices and assistance, public privacy, the duty of authorities and law enforcement agencies, and other related topics.

Technical Response

Since hackers and other bad actors are always developing and trying out new methods of attack, The nature of cyber crises ranges from being steady or consistent to being everything but. Establishing a response body that is outfitted with the necessary degree of technical skill and up-to-date understanding of technology breakthroughs is necessary in order to address the wide variety of cyber threats that exist on both the government and organizational levels. The majority of the time, these teams of experts will be referred to informally as CERT and CSIRT.

A typical CERT team includes specialists in areas including detection of breaches, malware analysis, software protection, forensics, and emergency response. Common CERTs include Corporate CSIRTs, National CERT Organizations, and Coordination CERTs. Both academic and industrial CSIRTs . At the moment, there is neither a government nor a nonprofit organization called CERT in Pakistan to deal with issues pertaining to cybersecurity. Despite this, the Pakistani government created the National Responsive Centre for Information Technology Crimes (NR3C) inside the FIA sometime in the year 2009. However, neither academic institutions nor private companies have their own CSIRTs, therefore they are unable to conduct research and analysis of this kind. The NR3C is a specialised agency that is exclusively concerned with criminal investigations, works under the supervision of the FIA (MOI), and has a limited mission.

CYBERSECURITY FRAMEWORK PROPOSAL

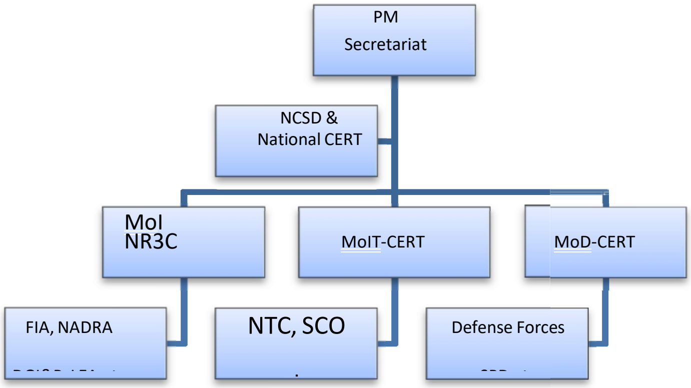
Within the current governmental structure, the Prime Minister and various ministries have the option to seek guidance from the NTISB, an entity operating under the Cabinet division [3]. Throughout its history, the NTISB has functioned with restricted financial backing and a constrained range of activities. Since it is run by the Department of Federal Investigation (FIA), the National Reaction Centers for Cyber Crimes (NR3C) has been made useless due to the lack of comprehensive cybersecurity rules.

While the Senate Committee on Defense's formation of a Task Force on Cyber Security might be considered a positive initial step, it has yet to yield any tangible legislative or policy modifications. A proposed organizational framework for cybersecurity is presented in Figure 3A, outlining the desired incident response capabilities at each tier in a top-down approach, facilitating the initiation of distinct actions. The proposal aims to replace the National Technical Information Services Board's National Cyber Security Division with a National Cyber Security Directorate located within the Prime Minister's Office. This shift would place the responsibility for cybersecurity under the purview of the NCSD.

A. NCSD

developing a plan, a policy, and the laws to keep cyberspace safe. It will be the nerve Centre for national cyber security policy coordination, implementation, assessment, and enforcement. It consists of technical personnel from the Department of Defense (DoD) and the Department of Homeland Security (DHS). Major government agencies, include the MIT (Ministry of Information Technology) and the Ministry of Law. Through the several ministries, NCSD will make its services available to all branches of government. It is recommended that a National CERT be established under this department, giving it power over cyber security policy. It will provide the government with a unified front and cost savings by reducing duplication of effort, while also making it simpler to coordinate and enforce cyber laws.

e



B. MOIT-CERT

The nation's advancement in information and communication technology (ICT) architecture is being actively addressed by the Ministry of Information Technology (MoIT), which is actively tackling a variety of challenges connected to the ICT infrastructure. This comprises its administration, expansion, training, human resource development, and personnel advancement, among other things. CERT as part of the Government's Department of Information Technology has been proposed as a way to improve the Ministry of Information Technology's ability to provide support to the various ICT-related organizations that fall under its purview, such as the National Telecommunications company (NTC), PTCL, the Pakistan The software Export Board of Directors, and the Special Communication Organization (SCO).

The suggestion entails broadening the MoIT-CERT's scope to include oversight of the PTA, the HEC, and all government and personal academic institutions. This expansion aims to facilitate research in relevant domains and enhance the effectiveness and operations of the organization. Due to its capabilities, MoIT-CERT is poised to become the primary regulatory authority for the entire industry, encompassing Internet Service Providers (ISPs), telecommunications companies, universities, and research labs. In addition, it will make use of the enormous technical resources it has in order to drive indigenous projects involving research and development in the area of information and communications technology. These initiatives will be modelled after current research trends and will be launched inside the country.

C. MOD-CERT

It is suggested that the Ministry of Defense set up a Computer Emergency Readiness Team (CERT) to analyze and respond to cyber threats. It will allow for coordinated response to cyber events of national significance and improved understanding of the cyber environment. By expanding its investigative and operational capabilities, the MOD- CERT will be able to detect and investigate complex cyber threats and provide solutions for countering them.

D. NR3C

The FIA already has a Cybercrime Response Centre in place. To better handle cybercrimes and investigations for presentation in court, it is recommended that NR3C's power be increased and put directly under MoI, and that FIA may establish a modern digital forensics laboratory. The legal basis for NR3C should also be strengthened. The National Database and Registration Authority (NADRA) will benefit from its CSIRT-like capabilities. Law enforcement agencies and the Directorate General of Immigration and Passports (DGI&P). NR3C is well-equipped to deal with cybercrime and other internal dangers to Pakistan's IT community.

CONCLUSION

Pakistan is one of the states with the highest per capita use of information technology due to its abundance of natural resources and human ingenuity. The economy isn't benefiting from the increased e-commerce and commercial prospects, and neither are national, corporate, or user interests being adequately protected in cyberspace. The absence of cyber laws and a coordinating organization to respond to cyber-attacks are the two most basic problems plaguing information and communication technologies and the online world at large. It is not just damaging the country's reputation internationally, but also robbing it of significant economic and financial potential. It is hoped that the proposed top-level cyber security organization would help states control their cyber policy and protect national interests. Only through unwavering efforts and the establishment of an organizational framework with the mission to develop the necessary ICT infrastructure and human resources that exist within the nation can the required capability be accomplished. As a result, Pakistan's reputation as a responsible state in the digital world will be restored, and the country's cyber operations will expand, bringing with them new economic benefits.

REFERENCES

[1] F. A. Momein and M. N. Brohi, “Cyber crime and internet growth in Pakistan,” *Asian J. Inf. Technol.*, vol. 9, no. 1, pp. 1–4, 2010.

[2] Z. Yunos and C. Malaysia, “The Reality of Cyber-Threats Today,” *STAR -Tech*, 2008.

[3] M. Tariq, B. Aslam, I. Rashid, and A. Waqar, “Cyber threats and incident response capability-a case study of Pakistan,” presented at the 2013 2nd National Conference on Information Assurance (NCIA), IEEE, 2013, pp. 15–20.

[4] “bank.” Accessed: Oct. 12, 2023. [Online]. Available: http://www.etechcrunch.com/%20tameer-%20bank-website-hacked-after-hbl-and-abl-websites/4504/

[5] A. Khan, U. K. Wiil, and N. Memon, “Digital forensics and crime investigation: Legal issues in prosecution at national level,” presented at the 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, IEEE, 2010, pp. 133–140.

[6] A. Mahboob and J. Zubairi, “Intrusion avoidance for SCADA security in industrial plants,” presented at the 2010 International Symposium on Collaborative Technologies and Systems, IEEE, 2010, pp. 447–452.

[7] R. Masood and Z. Anwar, “SWAM: Stuxnet worm analysis in metasploit,” presented at the 2011 Frontiers of Information Technology, IEEE, 2011, pp. 142–147.

[8] N. Falliere, “Stuxnet introduces the first known rootkit for industrial control systems,” *Publ. Online Httpwww Symantec Comconnectblogsstuxnet-Introd.-First-Known-Rootkit-Scada-Devices Last Accessed Febr.*, vol. 10, 2011.

[9] S. Ahsan and A. Shah, “Data mining, semantic web and advanced information technologies for fighting terrorism,” presented at the 2008 International Symposium on Biometrics and Security Technologies, IEEE, 2008, pp. 1–5.

[10] H. Senturk, Z. Çil, and Ş. Sağıroğlu, “Cyber security analysis of Turkey,” *Int. J. Inf. Secur. Sci.*, vol. 1, no. 4, pp. 112–125, 2012.

[11] A. Klimburg, “National Cyber Security Framework Manual (NATO CCD COE Publications),” *Tallinn*, vol. 2012, pp. 120–127, 2012.