Proposed Cyber Security Framework for Pakistan Based on Best Practices Involved in Cyber Security Framework of Contemporary Countries and International Standards

By

Aamer Latif Malik

00000325137

Submitted to the Faculty of Department of Information Security Military College of Signals, National University of Sciences and Technology, Islamabad in partial fulfillment of the requirements for the degree of MS in Information Security

AUGUST 2021

DECLARATION

I certify that this research work titled “Proposed Cyber Security Framework for Pakistan Based on Best Practices Involved in Cyber Security Framework of Contemporary Countries and International Standards” is my own work. No portion of this work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere. The material that has been used from other sources has been properly acknowledged / referred.

____

Signature of Student

Aamer Latif Malik

0000325137

Abstract

Data security has become a global issue due to the fact that it is the most valuable asset. Data leaks and security vulnerabilities have the potential to damage the global economy. Many modern nations, like Russia, China, and Malaysia, have adapted the NIST cyber security framework (2013) to their own needs and developed their own cyber security framework. In Pakistan, internet usage has increased dramatically in recent years, resulting in a rise in cyber security incidents. With the growth of information and technology, there has been a worldwide increase in cybercrime. At the national level, there was a perceived need to establish cyber laws, rules, and regulations to cope with cybercrime resulting from technological progress. Pakistan currently lacks adequate legislation to combat cyber dangers. In this context, a cyber legislation known as the **Prevention of Electronic Crimes Act (PECA)** was drafted and adopted in 2016 to address cyber-crime threats and offences. In following years, changes were made to meet new developing risks, however it is considered that there is a need to establish a cyber security framework that deals with cybercrime by combining these cyber laws, rules, and regulations, so that the threat of cybercrime may be dealt with efficiently. As a case study, cyber-crimes particular to the banking industry are emphasized and thus included in the research effort.

Table of Contents

List of Figures

List of Tables

Chapter - 1

Introduction

World’s total economy can be placed at risk due to data breaches and information security failures. Realizing the level of threat, the US President in 2013 issued an executive order [1] to develop a Cybersecurity framework to help reduce cyber risks and cybercrimes. Thus, NIST Framework for Improving Critical Infrastructure Cybersecurity (**NIST Cybersecurity Framework, or CSF**) was originally published [2] in February 2014 in response to Presidential Executive Order, “Improving Critical Infrastructure Cybersecurity,” which asked for the creation of a voluntary framework to assist enterprises in improving their systems’ cybersecurity, risk management, and resilience. The majority of countries have a specific organization or groups to handle national cybersecurity needs. Following the same level of cyber threats and security requirements other sovereign countries like **China, Russia** and **Malaysia** took lead [3] and developed their own Cyber Security Framework through coordinated effort amongst business industry and government. These Framework comprises of measures, rules, practices and anti-cybercrime laws and regulations to showcase the safety of imperative foundation.

The security of the nation’s essential infrastructure is a major investment. Cybercrimes which are generated due to breaches of data and information needs to address with complete dedication and professionalism.

This require a great deed for formulation of cyber laws and regulation and their implementation in true letter and spirit. “The art of war” is a constantly evolving phenomena and a method for determining how, when, and where to engage the opponent. A comparatively newer menace is emerging globally, posing a threat not only to status but also to the private profit-driven world. Hundreds of millions of dollars have been fraudulently transferred or stolen, personal information has been revealed, state secrets have been obtained, and key public infrastructure has been hacked. This is where cyber security comes into play. Cyber security issues are becoming more prevalent as the globe gets more connected via the internet or digitized through information technology [4].

Pakistan, being a nuclear state and future hub of trade activities in the region due to CPEC and its peculiar geographical location, requires developing a comprehensive policy or framework on cyber security at National level. In Pakistan no solid work on the creation of national cyber security policy or framework has been carried out till date and till 2016 no formal law was formed to deal with cybercrimes taking place in the country and in the region. Presently, **Pakistan Electronic Crime Act (PECA) – 2016**, is all the whole sole body to deal with all sort of cyber-crimes and related activities [5] but still it has not been enforced in true letter and spirit. The establishment of **National Centre for Cyber Security (NCCS)** has been commenced by Government of Pakistan in June 2018 [6]. The NCCS project [7] is a joint initiative of **Higher Education Commission (HEC)** and **Planning Commission** which are working to formulate national cyber security framework however it is still not finalized. The **Securities and Exchange Commission of Pakistan (SECP)** in May 2020, has only issued guidelines on cybersecurity framework for the insurance sector but detailed framework has not been proposed [8]. Pakistan does not have an official national cyber security policy. Cyber security appears in the national dialogue from time to time, but there is never a protracted discussion on the subject.

Thus, a dire need is felt to formulate a comprehensive cyber security framework incorporating anti-cybercrime laws and regulations and best international practices so that we can secure our cyber space and could deal with upheaving cyberattacks and cybercrimes in our country.

1.1 Background

The first and most important priority is a national strategy or framework that describes the state's mission, objectives, and goals for maintaining cyber security, as well as anti-cybercrime legislation. Unfortunately, data security is not at the top of Pakistan's national or organizational agendas. Pakistan is no different, as a nuclear state with a significant geopolitical position is becoming increasingly vulnerable to cyber assaults. The private sector and the business sector are also affected. Pakistan has a sizable internet user base, as well as a growing computerized security apparatus and banking system, all of which rely on internet connectivity. Pakistan has also enacted laws to address the threat posed by cyber-attacks, however these laws do not appear to cover the threats in depth or in their whole [9]. As threats develop and emerge from a variety of opponents and adversaries, we must constantly analyze them and make appropriate adjustments to our approach. In this perspective, **This research examines current nations' cyber security frameworks as well as international norms dealing with cybercrime, and then recommends a Cyber Security Framework for Pakistan based on best practices in the form of anti-cybercrime legislation and regulations.**

1.2 Problem Statement

In this light, this research examines current nations' cyber security frameworks and international standards dealing with cybercrime, and then recommends a Cyber Security Framework for Pakistan based on best practices in the form of anti-cybercrime legislation and regulations.

1.3 Objectives

The main objectives of this study are:

- Analyzing already implemented Cyber Security Frameworks in contemporary countries including **China, Russia, Malaysia** and **Saudi Arabia** dealing with cyber-crimes.
- Analyzing **National Institute of Standards and Technology (NIST)** Cyber Security Framework (CSF) as an approved international standard.
- Proposing a high-level **Cyber Security Framework for Pakistan** that incorporates best practices in the form of anti-cybercrime legislation and regulations.

1.4 Relevance to National needs

The technology, procedures, and policies that secure the digital (also known as cyber) infrastructure and its capacity to offer vital and desired services are referred to as cybersecurity. Pakistan is one of the world's most targeted countries, and it has to strengthen its legal, technological, and organisational capabilities to protect its digital assets. **Terrorism and sectarianism**, which used to be one of the root causes of unrest in the country, was also being spread with the help of modern communication technologies. In terms of data protection and security, **Symantec,** which keeps the most comprehensive civilian database of events, **places Pakistan in the top 10 most targeted destinations in the world.** [10]. With publicly acknowledged attempts on a range of telecommunications, financial, government, health, transportation, utilities, and ridesharing institutions, Pakistan's nuclear and other critical sites are likely to be targeted. **Snowden files revealed that the NSA was spying on Pakistan's civilian and military leadership**, using a malware called **SECONDATE** [11].

Pakistan does not have an official national cyber security policy. Cyber security appears in the public conversation from time to time, but there is seldom a continuous discussion on the issue [12]. However, the research work proposed a high-level description of a cybersecurity framework that includes anti-cybercrime laws and regulations that will be used by government and public sector ministries and agencies to plan the necessary protection for their respective cyberspaces and to make the procedure for cyber-criminal convictions easier.

1.5 Advantages

The impacts of proposed framework will be to:

- Provide a more effective and comprehensive cybersecurity protection against cyber-crimes.
- Minimize the damage caused by cyber-attacks.
- Increase stakeholder confidence by ensuring the seamless execution of existing government services.

1.6 Delimitations

This study will concentrate on national cyber security legislation and policies that deal with cybercrime on a national level. Existing cyber security rules have limits in coping with increasing cyber dangers and new cyber-crimes, therefore this study will point out such gaps so that concerned authorities may include the most up-to-date anti-cybercrime legislation into the national cyber security framework. Anti-cybercrime legislation and regulations have been included into the framework for developing a national cyber security framework.

1.7 Areas of Application

This suggested framework would assist all business sectors that may be impacted by cyber-attacks or targeted by cyber criminals.

- Government and private organizations using Information and Communication Technologies (ICT) services.
- Military and critical installations.
- National cyber security elements.
- IT industry.
- Telecom industry.
- Transport industry.
- Banking sector.
- Health industry.

Chapter - 2

Literature Review

Pakistan has a large internet-based user, banking system and digitized security apparatus which is linked to internet connectivity for day to day functioning. Due to its important geopolitical position and being a nuclear state, it is very much exposed to cyber threats. It has enacted rules and regulations to combat the threat of cyber-attacks, but it still needs to improve since new threat vectors emerge as technology develops. In this context, a National Cyber Security Framework is being developed, and Cyber Crime legislation are being enacted to address existing and future cyber threats.

The purpose of this literature research is to find the gaps in the NIST Cyber Security Framework that pertain to anti-cybercrime legislation. Furthermore, the current cybercrime act and legislations in Pakistan must be revised in order to handle current growing cyber risks and crime, and a new component in the proposed cyber security framework must be developed to address the issue.

2.1 NIST Cyber Security Framework

NIST CSF was introduced in 2013 on the US presidential directive [13] and was later upgraded in 2018. The basic motive was to formulate best practices to secure data and information from potential threats and breaches. Thus, a framework was introduced to cater for the data protection needs of US government in particular and other nations in general. NIST directed that basic needs for data protection have been incorporated in the formulated framework however every country can mold this framework as per their own requirements. Currently Pakistan is being targeted by a variety of cyber-attacks and cybercrimes. These include data theft, breach of security, ransomware, hate speeches, child pornography and few more. Because these challenges necessitate the inclusion of national laws and regulations, the NIST CSF has not issued any guidelines on how to deal with these cyber-crimes.

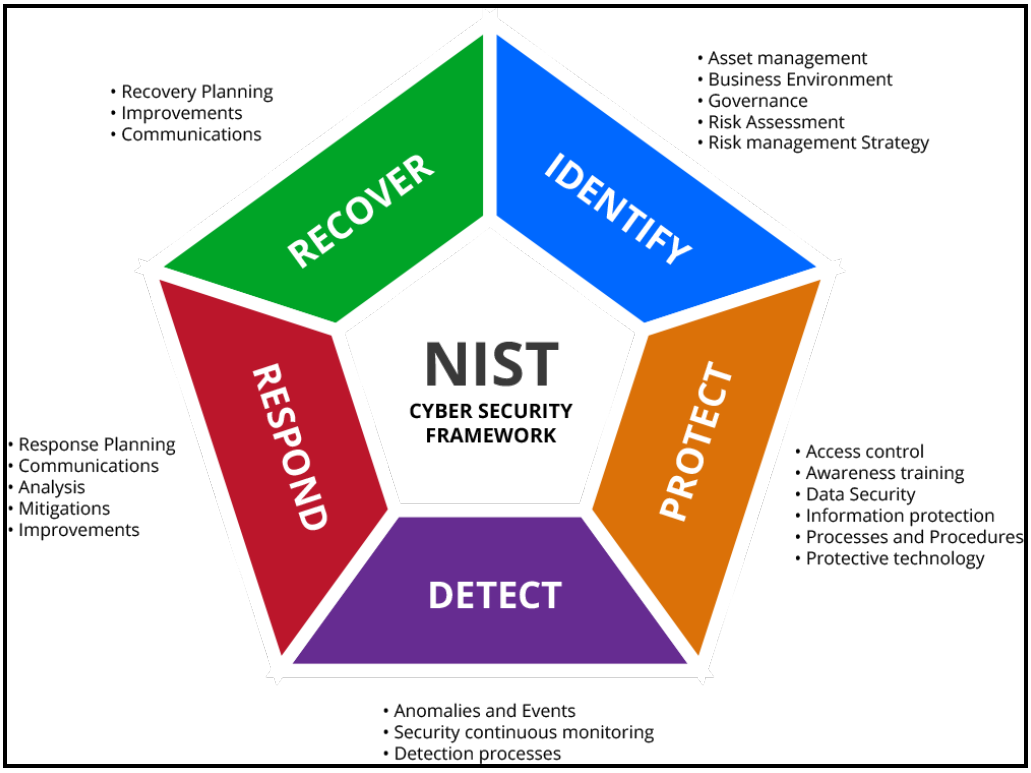


Figure-2.1: Five Components of NIST Cyber Security Framework

The main five components of NIST CSF include **Identify, Protect, Detect, Respond** and **Recover** [14] however all these components deal purely with data and information protection. Thus, a need was felt to incorporate another component namely **Cyber Crime Laws** to deal with the cyber threats at national level. This will help our governmental, public sector organizations and law enforcement agencies to deals with cyber related crimes under the same umbrella of Cyber Security Framework. Many developed countries like Russia, China and Malaysia have incorporated NIST CSF to formulate their own cyber security framework but all these countries have initially framed strong laws and ordnances to curb cyber-attacks and later have incorporated them in the national cyber security framework.

2.2 Malaysian Cyber Security Framework

A cyber security framework provides a general perspective on all components of cyber security that needs to be taken into account by ministries and government agencies in protecting information in cyberspace. Thus Malaysian Cyber Security Framework [15] first version was developed in April 2016 so that ministries, agencies and public sector can develop their cyber security policies based on this framework and to ensure that cyber activities that are carried out comply with the requirements set out in the framework.

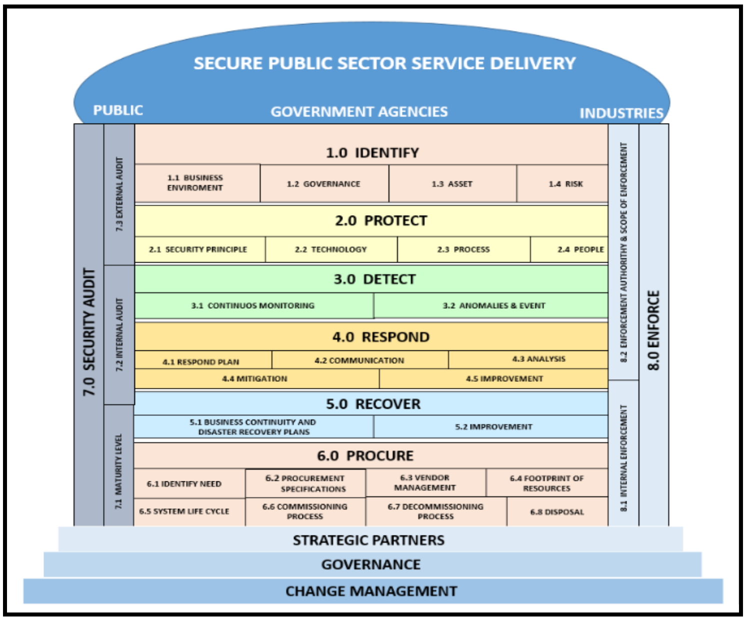


Figure-2.2: Malaysian Cyber Security Framework (RAKKSSA)

This framework was developed based on the existing NIST CSF that was improved by the project team to produce a local cyber security framework specifically for Malaysian Public Sector agencies. This framework [15] consists of eight main components whose functions are defined below:

- **Identify**: It aimed at identifying the Department's functional environment, governance policies and structures as well as assets that needs to be protected, identifying related risks and risk management. **The department shall identify the laws and regulatory requirements that must be followed in carrying out its role as governance structure at each level.**
- **Protect**: It requires the principles of safety, technology, processes, and human competence to be determined to mitigate the risks that have been identified.
- **Detect**: It carries the objective detecting malicious code threats by emphasizing on differences in the use and form of network traffic.
- **Respond**: It ensures that action against the malicious code threat is taken and reported to stakeholders and the public.
- **Recover**: It takes into account the capacity to assure information availability, as well as the ability to recover from malicious code threats and system failure.
- **Procure**: It guarantees that security rules and requirements are followed throughout the system's life cycle, for both external and internal

development. These are crucial components since they involve procurement requirements and supplier management.

- **Security Audit**: It deals with the security audit across all components of the framework.
- **Enforce**: It deals with the audit and enforcing laws and regulation carried out by the audit agency and enforcement authorities.

This framework further specifies the method for managing Official Confidential Information, as well as the requirement to contact the Office of the Chief Security Officer (CGSO) for information generation, classification, treatment, storage, premises, and destruction. A key component of this framework is ensuring that suitable safety standards are followed depending on the risk assessment and risk management that is necessary.

Malaysia's National Cyber Security Policy [16] has been integrated with the National Cyber Security Framework. This policy defines the technology related threats and cyber content related threats.

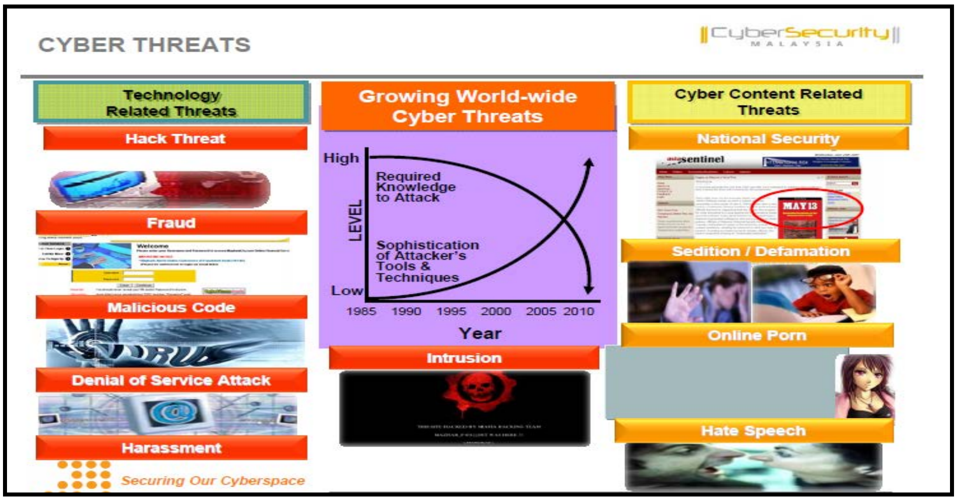
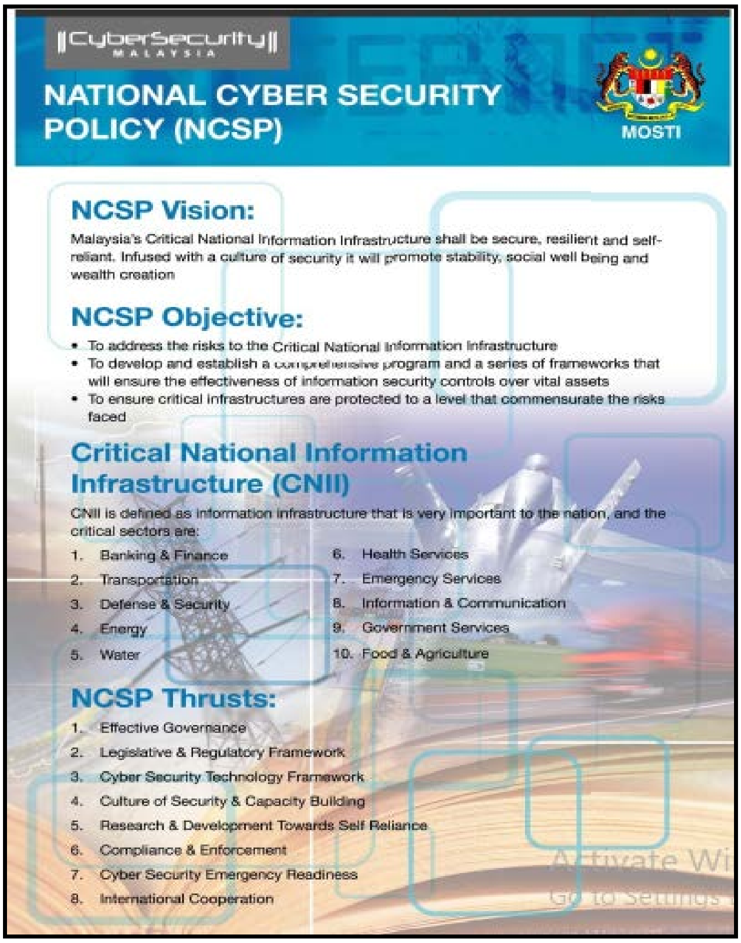


Figure-2.3: Malaysian Cyber Security Policy and Cyber Threats

The policy goal was to address the threats to vital national information infrastructures and guarantee that they were safeguarded to a degree that was commensurate with the threats they faced.


CyberSecurity
MALAYSIA
MOSTI

NATIONAL CYBER SECURITY POLICY (NCSP)

NCSP Vision:

Malaysia's Critical National Information Infrastructure shall be secure, resilient and self-reliant. Infused with a culture of security it will promote stability, social well being and wealth creation

NCSP Objective:

- To address the risks to the Critical National Information Infrastructure
- To develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of information security controls over vital assets
- To ensure critical infrastructures are protected to a level that commensurate the risks faced

Critical National Information Infrastructure (CNII)

CNII is defined as information infrastructure that is very important to the nation, and the critical sectors are:

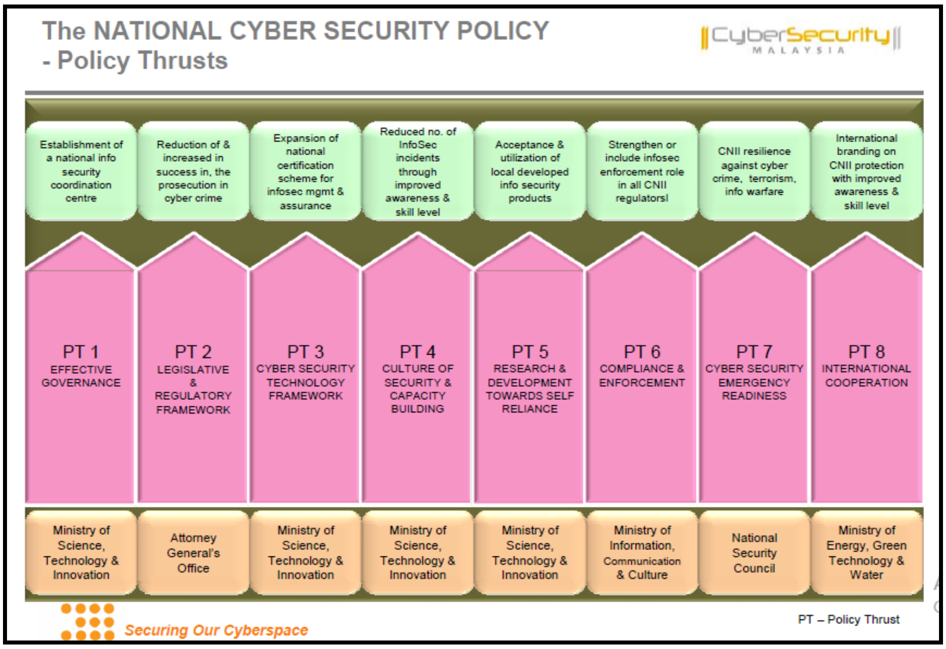
1. Banking & Finance
2. Transportation
3. Defense & Security
4. Energy
5. Water
6. Health Services
7. Emergency Services
8. Information & Communication
9. Government Services
10. Food & Agriculture

NCSP Thrusts:

1. Effective Governance
2. Legislative & Regulatory Framework
3. Cyber Security Technology Framework
4. Culture of Security & Capacity Building
5. Research & Development Towards Self Reliance
6. Compliance & Enforcement
7. Cyber Security Emergency Readiness
8. International Cooperation

Figure-2.4: Malaysian National Cyber Security Policy Framework

Under the umbrella of policy thrusts different functions have been incorporated in the policy framework to deal with the formation and implementation of National Cyber Security Policy [16]. The **Policy Thrusts – 2 deals with Legislative and Regulatory framework** which works under the supervision of Attorney General to bring reduction and increased in success in, the prosecution in cyber-crime.



The NATIONAL CYBER SECURITY POLICY
- Policy Thrusts

Establishment of a national info security coordination centre	Reduction of & increased in success in, the prosecution in cyber crime	Expansion of national certification scheme for infosec mgmt & assurance	Reduced no. of InfoSec incidents through improved awareness & skill level	Acceptance & utilization of local developed info security products	Strengthen or include infosec enforcement role in all CNII regulatorsl	CNII resilience against cyber crime, terrorism, info warfare	International branding on CNII protection with improved awareness & skill level
PT 1 EFFECTIVE GOVERNANCE	PT 2 LEGISLATIVE & REGULATORY FRAMEWORK	PT 3 CYBER SECURITY TECHNOLOGY FRAMEWORK	PT 4 CULTURE OF SECURITY & CAPACITY BUILDING	PT 5 RESEARCH & DEVELOPMENT TOWARDS SELF RELIANCE	PT 6 COMPLIANCE & ENFORCEMENT	PT 7 CYBER SECURITY EMERGENCY READINESS	PT 8 INTERNATIONAL COOPERATION
Ministry of Science, Technology & Innovation	Attorney General's Office	Ministry of Science, Technology & Innovation	Ministry of Science, Technology & Innovation	Ministry of Science, Technology & Innovation	Ministry of Information, Communication & Culture	National Security Council	Ministry of Energy, Green Technology & Water

Securing Our Cyberspace

PT – Policy Thrust

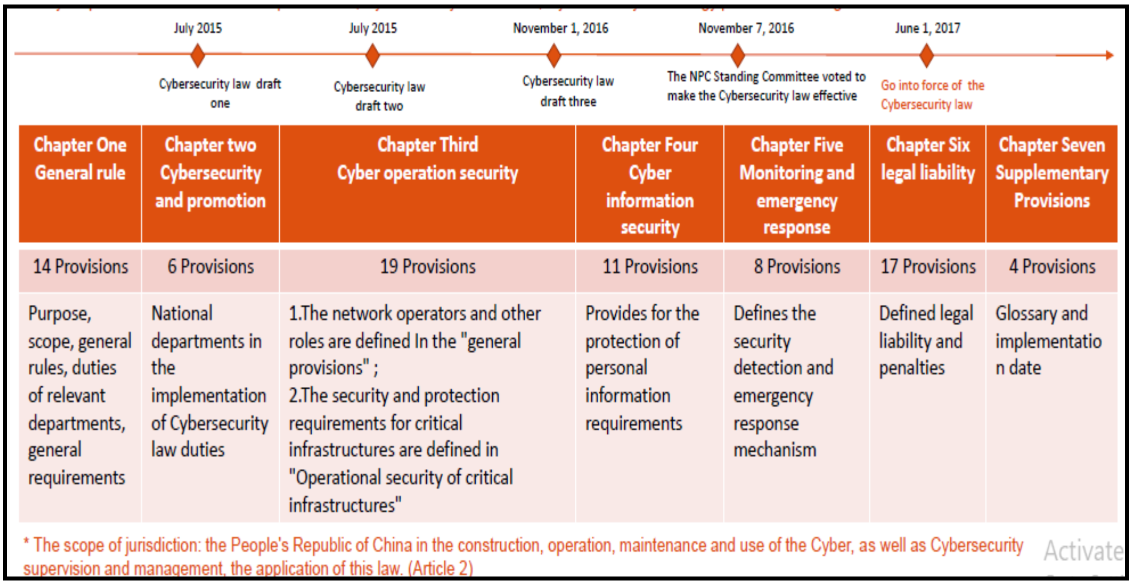
Figure-2.5: Policy Thrusts of Malaysian National Cyber Security Policy Framework

National Cyber Security Policy implementation approaches to three phases ranging from 1 to 5 years plan. The governance body comprises of IT Council, Advisory committee, Coordination Committee and Working Group. The Legislative and Regulatory Framework examines Malaysian legislation in order to address legal issues in the Cyber Environment. They have following three main purposes:

- To address the present legislative framework, both cyber-specific and conventional, and to determine if the current law is sufficient to combat such threats.
- To provide recommendations on the kind of changes that should be made. This would also involve discussing techniques and processes for reconciling and harmonizing laws, as well as making general comments on the present legislation.

2.3 Chinese Cyber Security Framework

Chinese Cybersecurity Laws [17] interpretation basic theme is to grow data confidentiality. The Cybersecurity Law was implemented in June 2017 which was the main driving force to deepen the practice of Cybersecurity and to improve the overall national cyber security levels and it has been incorporated with the national cybersecurity framework. Main protection objects involved in this law includes key infrastructure, network and personal information and the protection methods which involve the implementation of classified protection, cybersecurity assessment and early warning, cybersecurity emergency management, security responsibilities and violation and punishments, cybersecurity awareness, cybersecurity technology personnel training and much more.


July 2015
Cybersecurity law draft one
July 2015
Cybersecurity law draft two
November 1, 2016
Cybersecurity law draft three
November 7, 2016
The NPC Standing Committee voted to make the Cybersecurity law effective
June 1, 2017
Go into force of the Cybersecurity law

Chapter One General rule	Chapter two Cybersecurity and promotion	Chapter Third Cyber operation security	Chapter Four Cyber information security	Chapter Five Monitoring and emergency response	Chapter Six legal liability	Chapter Seven Supplementary Provisions
14 Provisions	6 Provisions	19 Provisions	11 Provisions	8 Provisions	17 Provisions	4 Provisions
Purpose, scope, general rules, duties of relevant departments, general requirements	National departments in the implementation of Cybersecurity law duties	1.The network operators and other roles are defined In the "general provisions" ; 2.The security and protection requirements for critical infrastructures are defined in "Operational security of critical infrastructures"	Provides for the protection of personal information requirements	Defines the security detection and emergency response mechanism	Defined legal liability and penalties	Glossary and implementation date

* The scope of jurisdiction: the People's Republic of China in the construction, operation, maintenance and use of the Cyber, as well as Cybersecurity supervision and management, the application of this law. (Article 2)

Figure-2.6: Chinese Cybersecurity Law Framework

Implementation of additional security regulations on classified protection systems, protection requirements on Critical Infrastructure Information and Cross-border data transfer, certification and testing on certain network products may be on the way.

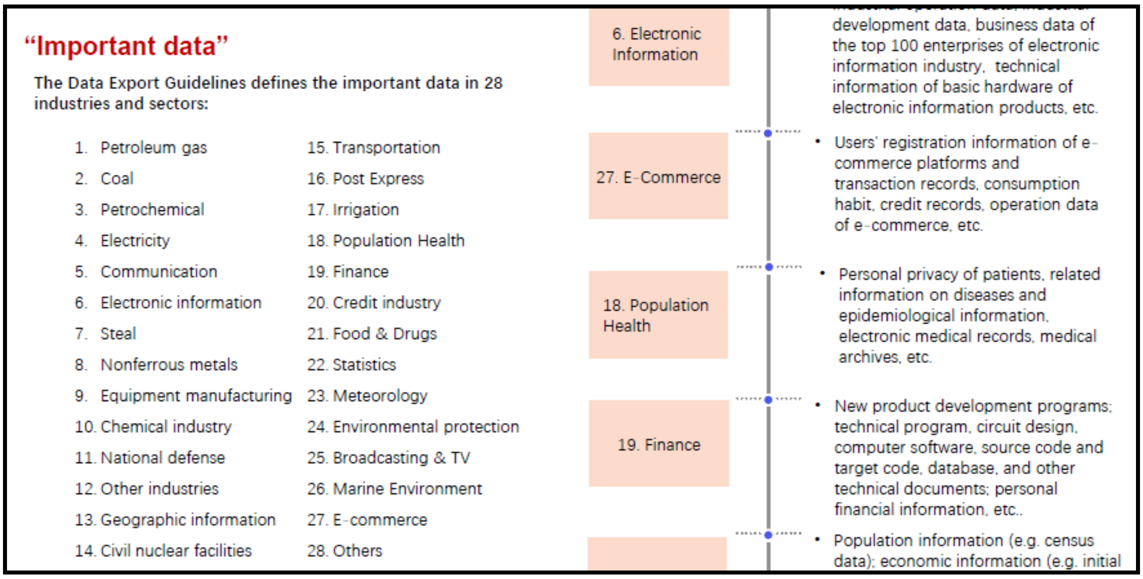
It is the first law on cybersecurity in China and it **created new legal regime and landscape for cyberspace administration**. It also emphasized on cyberspace sovereignty. It imposed new obligations and highlighted punishments for violators. It was implemented through a series of different published regulations and standards. In general, CSL applied to construction, operations, maintenance, and network within the territories of China especially the network operators, critical information Infrastructure operators, network products and service providers.

Government organizations and institutions in the fields of energy, finance, transportation, integration, healthcare, education, social security, environmental protection, public utilities, and others have been classified as CII-Critical Information Infrastructure under the CSL umbrella. Telecommunication networks, radio and television networks, the internet, and businesses that provide large-scale cloud computing, big data, and other public information network services are examples of information networks. Sectors such as national defence and science, heavy equipment, chemical, and food and pharmaceutical industries all include scientific research and production units. Radio stations, television stations, news agencies, and other significant institutions that report on the news. Other CII that, in the event of damage, function loss, or data leaking, might jeopardize national security, people's livelihoods, and the public interest. The major protection requirements for CII include:

- Local storage of personal information and important data.

- Security assessment for transferring these data abroad.
- National security review requirement on security and reliability.
- National laws and regulations related to data breach or cybercrime.
- Technical and organizational protection measures.
- Operation and maintenance of CII.
- Security testing on the system and software developed by outsourcing vendors.

Requirements that has the most important significant impact is the cross border data transfer [18]. All network operators are subjected to data localization and fulfilling of security assessment requirements. The data export guidelines defines the important data in 28 industries and sectors.



"Important data"

The Data Export Guidelines defines the important data in 28 industries and sectors:

1. Petroleum gas
2. Coal
3. Petrochemical
4. Electricity
5. Communication
6. Electronic information
7. Steal
8. Nonferrous metals
9. Equipment manufacturing
10. Chemical industry
11. National defense
12. Other industries
13. Geographic information
14. Civil nuclear facilities
15. Transportation
16. Post Express
17. Irrigation
18. Population Health
19. Finance
20. Credit industry
21. Food & Drugs
22. Statistics
23. Meteorology
24. Environmental protection
25. Broadcasting & TV
26. Marine Environment
27. E-commerce
28. Others

6. Electronic Information

development data, business data of the top 100 enterprises of electronic information industry, technical information of basic hardware of electronic information products, etc.

27. E-Commerce

- Users' registration information of e-commerce platforms and transaction records, consumption habit, credit records, operation data of e-commerce, etc.

18. Population Health

- Personal privacy of patients, related information on diseases and epidemiological information, electronic medical records, medical archives, etc.

19. Finance

- New product development programs; technical program, circuit design, computer software, source code and target code, database, and other technical documents; personal financial information, etc..

- Population information (e.g. census data); economic information (e.g. initial

Figure-2.7: Data Export Guidelines

Penalties for non-compliance have also been introduced. At company level different penalty tiers have been marked like **order to make correction, warning, confiscating of illegal gains, business suspension, closure of website or suspension**

of business permit or license. At individual level penalty in the form of **monetary fine or trial under the criminal law with penalty of imprisonment, detention, public surveillance or fine**. Individuals convicted of the relevant cybercrime will be **barred from holding any significant job in network security management or operations for the rest of their lives**.

The China Cybersecurity law compliance program discussed with GDPR Team on compatibility and interconnectedness issue of GDPR and CSL which highlighted following differences and interconnectedness:

- GDPR focuses personal data protection whereas CSL includes personal data protection requirements as well as requirements on cybersecurity and CII protection
- GDPR requirements on personal data protection is more onerous and specific than those of CSL.
- In data localization it highlights following:
    - GDPR focuses personal information whereas CSL focuses on personal information and important data
    - GDPR personal rights oriented whereas CSL is state security oriented
    - GDPR has clear data transfer rules whereas CSL has ambiguous assessment standards.

2.4 Russian Cyber Security Framework

Russian Cyber Security Framework was approved in April 2016. This framework [19] comprises of cyber security legal, technical, organizational measures, capacity building, cooperation and child Protection. These are further described below:

- **Legal Measures**: It is concerned with the criminal legislative process, particularly in relation to cybercrime, which has been implemented through a Criminal Code instrument (Chapter 28: Article 272-274). Additional cybersecurity legislation has been enacted, including steps to combat spam, safeguard legal entities and individual information, and technological and legislative regulation, among other things.
- **Technical Measures**: Russia has created the Cyber Incident Response Team (CIRT), which is a hub for cyber incident response in government information systems. This center is in charge of coordinating the operations of the corporations and government entities involved in the detection, prevention, and repression of unlawful behavior involving government network resources. At the national level, Russia has established standards and certificates for adopting internationally recognized cybersecurity requirements.
- **Organizational Measures**: Russia has also accepted and developed the Russian Federation's Basic Principles for State Policy in the Field of International Security (2020). Depending on the information needs, each government institution in Russia conducts an annual audit of its own networks and systems.
- **Capacity Building**: At the university level, Russia has begun several R&D programmes connected to cyber security certification. The task of

training professionals in this sector has been allocated to national institutes.

- **Cooperation**: A programmed has been developed under the umbrella of Russian CIRT to collaborate with adjacent countries in order to ease the sharing of information relevant to cyber security. The Russian Federal Security Service (FSB) collaborates with a variety of foreign groups to provide cyber security information.
- **Child Online Protection**: In the cyber security framework, special rules and regulations on kid online safety have been created. In addition, a federal law was enacted to protect children from material that is damaging to their health and development.

Russia has also put in place **a strong legislative framework that includes cyber laws and regulations aimed at ensuring Russia's Digital Sovereignty**. A Data Localization Law and a Law Legislating Imports have been proposed as alternatives to IT goods used by government agencies, vital infrastructure, and state-owned enterprises.

2.5 Saudi Arabia Cyber Security Framework

Government of Saudi Arabia formed their National Cyber Security Agency in 2017 whose role is to protect their cyber space and same organization developed their Cyber Security Workforce Framework in June 2020 [20]. **They have also incorporated Anti-Cyber Crime Law in their framework which deals with growing cyber-crimes**. They have introduced punishments and fines for cybercrime committers and have formulated a method for prosecution purposes.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

KINGDOM OF SAUDI ARABIA
THE SAUDI CYBERSECURITY
WORKFORCE FRAMEWORK
(SCyWF)

SCyWF - 1 : 2020

Sharing Indicator: White, Document Classification: Unclassified

Figure-2.8: Saudi Cybersecurity Workforce Framework

The main objective of Cybersecurity Framework was to serve as a reference model and a guideline for preparing and managing cybersecurity workforce. Organizations have been directed to adopt this framework to align their cyber security activities with national framework and guidelines, however they can customize it as per their requirements. They have developed their framework in alignment with US National Institute of Standards and Technology (NIST).

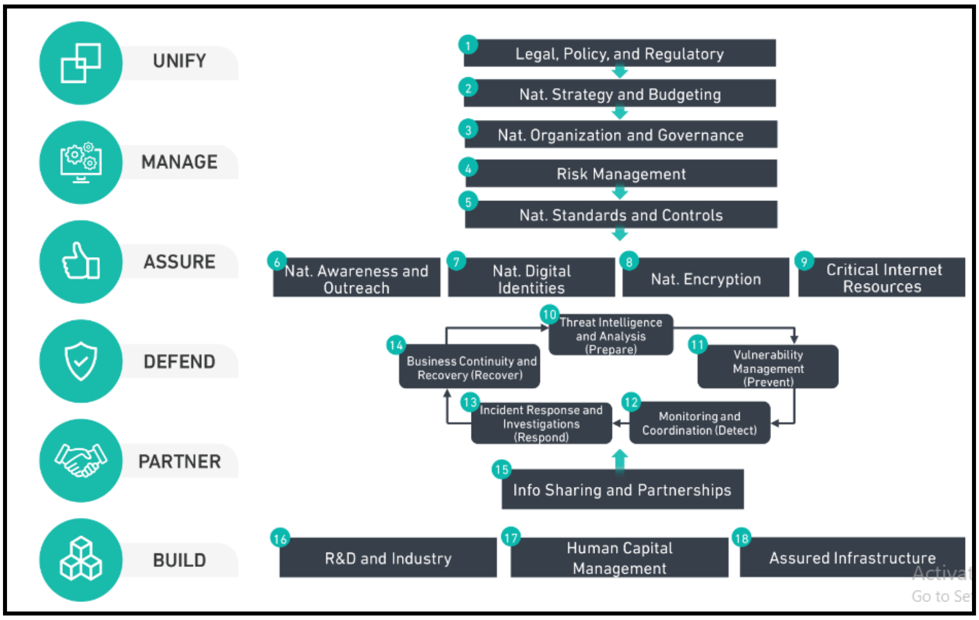

UNIFY
MANAGE
ASSURE
DEFEND
PARTNER
BUILD
1 Legal, Policy, and Regulatory
2 Nat. Strategy and Budgeting
3 Nat. Organization and Governance
4 Risk Management
5 Nat. Standards and Controls
6 Nat. Awareness and Outreach
7 Nat. Digital Identities
8 Nat. Encryption
9 Critical Internet Resources
10 Threat Intelligence and Analysis (Prepare)
11 Vulnerability Management (Prevent)
12 Monitoring and Coordination (Detect)
13 Incident Response and Investigations (Respond)
14 Business Continuity and Recovery (Recover)
15 Info Sharing and Partnerships
16 R&D and Industry
17 Human Capital Management
18 Assured Infrastructure

Figure-2.8: Saudi Arabia Cybersecurity Framework

In order to develop a reference framework for national agencies, NCA developed a reference framework for cybersecurity based on international best practices [21]. This framework comprises of six basic themes and eighteen elements of cybersecurity for developing an understanding of kingdom cyber space. Basing on this framework a cyber security strategy at national level has been developed.

The first theme of unify is used to integrate all components of cyber security in relation to national regulations and laws. It contains legal, policy and regulatory directions for formulating anti-cyber laws and legislations. First Saudi Anti-Cyber Crime Law [22] was passed in March 2007 which has been incorporated within the Cyber Security Framework. **This law addresses different cyber-crimes related activities like unauthorized access to data, illegal viewing if information, violations of laws in computer networks and systems and likewise**. Punishments and fines of different categories have been defined keeping in view the nature and severity of crime committed.

2.6 Prevention of Electronic Crime Act (PECA) – 2016

With the advent of digital technology and increase in use of digital media cyber-crimes have also evolved and in this regard government and institutions at national level are continuously monitoring cases and efforts are in hand to amend the current law to incorporate new cyber-crimes under those laws. PECA Law was formulated in the gab of anti-terrorism agenda and was made part of National Action Plan (NAP). PECA Law [23] is considered to be the first of its kind which deals with all sort of electronic crimes at national level. After its approval in 2016, few non-governmental organizations did not accept it in the realm of freedom of speech act however after few amendments and additional powers given to law enforcement agencies like FIA in 2016 it got approved by the parliament. This law basically deals with **prevention, investigation, prosecution, and trial of cybercrimes**.

It has about 7 different chapters which deals with short titles, offences and punishments, establishment of an investigation agency, international cooperation, prosecution and powers of court, preventive measures and its relations with other laws. Under PECA law all offences are cognizable except cyberterrorism, sexual harassment and child pornography however money laundering and theft of credit card details are not included in cognizable offences. Issuance of unauthorized SIM is cognizable only if complaint is entered by Pakistan Telecommunication Authority otherwise it will not be entertained. In case of any investigation by FIA in non-cognizable offence it had to take prior approval of magistrate which leads to slowing down of investigation process and delays in interrogation. PECA law also allows for the establishment of independent forensic lab for cybercrime related cases however no such lab has been formulated which was supposed not to be under the jurisdiction of any law enforcement agency.

PECA law can only be implemented in true letter and spirit if local courts don't hamper the working system of law enforcement agencies otherwise it wouldn't do its best as expected out by the citizens. It was assumed by the civil human rights organizations that PECA Law is just not more than an anti-speech, anti-privacy and anti-internet provisions for the individuals. It was expected that such a law be formulated which remains with in the constitutional framework. Cyber terrorism has been defined in section 10 in a very broad concept, which is the main core concept of this act. The language of the act like in section 10 tends to confuse incitement of violence and hostility with offences of terrorism. Section 37 gives powers to PTA to remove or block unlawful online content however here unlawful has not been defined in detail which corresponds to a vast amount of data.

2.7 Prevention of Electronic Crimes Ordnance – 2007

The purpose of this ordinance is to protect the confidentiality, integrity, and availability of sensitive data and information as defined by government and law enforcement authorities [24]. Any attempt of breach was to be dealt as a crime and punishments have been introduced against the culprit. Criminal data access or data damage have been considered as a crime and punishment of minimum of 2 years have been approved. Electronic frauds and electronic forgery have been regarded as electronic crimes and minimum 7 years punishment have been recommended. Use of malicious code and cyber stalking have been considered as cyber-crimes and punishment of minimum 7 years have been recommended. However due to the current advancement in technological arena cyber-crimes have extended their boundaries which include credit card transaction frauds and money laundering which are totally neglected by this ordnance.

2.8 Electronic Fund Transfers Act - 2007

This Act was formulated to deal with crimes related to money transfer or theft. All crimes related to electronic money or credit card have been addressed by this Act [25]. Staff of banks or of any money transfer facility have been charged in this law in case of any fraudulent activity and will be dealt as an electronic crime. Truncated cheques have also been marked as electronic forgery in this Act. All sort of funds transfer via ATMs and frauds linked to it have been incorporated in this Act. Anyone providing wrong information willfully will be subjected to criminal proceeding under this Act with a punishment of detention of minimum 3 years. Under this Act all financial institutions have been bound to maintain privacy and secrecy of their customers and are not allowed to share their personal information without their consent.

2.9 Electronic Transactions Ordnance (ETO) - 2002

Before the approval and promulgation of PECA, ETO-2002 was in place to deal with data and information privacy issues [26]. It was enforced to criminalize unlawful or unauthorized access to information. During and after its implementation the issue arose were mainly related to the protection of digital rights of the individuals. It was observed that these laws were meant to protect the civil rights of the citizens however on the other end they gave boosted power to government bodies to glance into civilian privacy and dig down their private life. It also made government the authority to certify electronic documents. In this complete ordnance electronic documents authentication have been defined in detail. Major offences which are being dealt under this law are provision of wrong information or issuance of false electronic certificates. It only deals with misusing of data and information and using of false certification data however other major cyber-crimes were not being addressed by this ordnance.

2.10 Pakistan Penal Code (PPC)

Pakistan Penal Code (PPC) [27] is a criminal act code for offences that are charged in Pakistan. It was prepared in 1860 and was later amended in 1947 after the independence of Pakistan. It is a mixture of both English and Islamic laws. This law does not directly deal with cybercrimes however its sections are being used for conviction of cyber criminals as these are elaborated in such a way that leads to a successful investigation of a cybercrime.

2.11 The Removal and Blocking of Unlawful Online Content Rules 2020

The Pakistani government established social media guidelines [28] in October 2020, in accordance with section 37 of the Prevention of Electronic Crimes Act – 2016. **Social Media Regulations 2020** is another name for these rules. These regulations establish safeguards, procedures, and mechanisms for the Authority to use its powers under the Act to remove or prevent access to unlawful Online Content via any information system. It also addresses the protection of freedom of speech and expression. It also lays out the steps for submitting, processing, and disposing of complaints.

Chapter - 3

Research Methodology

The study technique used in this research thesis is that a cyber security framework is needed to decrease cyber-crime instances in Pakistan and to deal with them in an effective and lawful manner. Following its formation, it will include a legal and legislative component that will address the threat of cyber-crime in the country under the cover of anti-cybercrime laws and regulations. Different cyber security frameworks were examined and evaluated as a preliminary step, however the NIST cyber security framework was chosen as the most suited for our needs and combining worldwide best practices.

3.1 NIST Cyber Security Framework

NIST Cyber Security Framework [29] was introduced in 2013 and was upgraded in 2018. In the proposed framework, best practices for data protection have been integrated. Pakistan is now the victim of a number of cyber-attacks. Data theft, security breaches, ransomware, hate speeches, child pornography, and other types of assaults are among them. To deal with these emerging risks, a new component of cybercrime must be introduced to the framework by combining national cyber laws and regulations.

3.2 Malaysian Cyber Security Framework

Malaysian government formulated their cyber security framework [30] in 2016 so that their ministries, agencies, and public sector can formulate their cyber security policies based on this framework. They've used the NIST CSF as a starting point, but they've added cyber laws and regulatory needs to the Identity component, which will be created for governance at each level.

3.3 Chinese Cyber Security Framework

Chinese government has formulated cybersecurity law [31] which was implemented in 2017 whose main objective was to practice cybersecurity and improve national cyber security levels. In chapter-6 of cyber security law they have defined legal liabilities and penalties as part of anti-cybercrime act. Penalties for individual and company level for breaching the information security and data have also been defined to reduce cybercrime rate.

3.4 Russian Cyber Security Framework

Russian Cyber Security Framework [32] was approved in April 2016. This framework comprises of legal, technical, and organizational measures, capacity building, cooperation, and child protection. It is concerned with the criminal legislative process, especially in relation to cybercrime, which has been adopted through a Criminal Code instrument (Chapter 28: Article 272-274). Additional cybersecurity law has been enacted, with several instruments containing provisions to combat spam, safeguard legal entities, individual information, and technical and legislative regulation.

3.5 Saudi Arabia Cyber Security Framework

Government of Saudi Arabia formulated their National Cyber Security Agency in 2017 whose role is to protect their cyber space and same organization developed their Cyber Security Workforce Framework [33] in June 2020. They have also incorporated Anti-Cyber Crime Laws in their framework which deals with cyber-crimes and cyber criminals. They have introduced punishments and fines for cyber-crime committers and have formulated a method for prosecution purposes.

Following an examination of modern nations' cyber security frameworks, it was deemed that Pakistan's present cybercrime legislation needed to be reviewed. As a result, any anti-cybercrime legislation, ordinances, and regulations enacted or authorized by governing bodies were considered to be included into the framework. A review in this regard is discussed below:

3.6 Prevention of Electronic Crime Act (PECA)-2016

PECA was formulated in the gab of anti-terrorism agenda and was made part of National Action Plan (NAP) by government of Pakistan. PECA Law [34] is considered to be the first of its kind which deals with electronic crimes at national level. This law basically deals with **prevention, investigation, prosecution and trial of cybercrimes**. It is divided into seven chapters that cover offences and penalties, the formation of an investigation agency, international cooperation, prosecution and judicial powers, preventative measures, and the relationship with other anti-cybercrime legislation.

3.7 Prevention of Electronic Crimes Ordnance – 2007

This ordinance was created in 2007 to protect the confidentiality, integrity, and availability of sensitive data and information [35] as defined by the government and law enforcement. Any attempt at breach was to be treated as a crime, with penalties imposed on the perpetrator. Criminal data access or data damage, electronic frauds and electronic forgery have been regarded as electronic crimes under this ordnance.

3.8 Electronic Fund Transfer Act – 2007

This Act was formulated in 2007 to deal with crimes related to money transfer or theft. All crimes related to electronic money or credit card have been addressed by this Act [36]. Banking staff or staff of any money transfer facility have been charged in this law in case of any fraudulent activity and will be dealt as an electronic crime. Truncated cheques have also been marked as electronic forgery in this Act. All sort of funds transfer via ATMs and frauds linked to it have been incorporated in this Act.

3.9 Electronic Transaction Ordnance – 2002

Before the approval and promulgation of PECA Law, ETO-2002 was in place to deal with data and information privacy issues [37]. It was enforced to criminalize unlawful or unauthorized access to information. During and after its implementation the issue arose were mainly related to the protection of digital rights of the individuals. In this complete ordnance electronic documents authentication have been defined in detail. Major offences which are being dealt under this law are provision of wrong information or issuance of false electronic certificates.

3.10 The Removal and Blocking of Unlawful Online Content, Rules 2020

The Pakistani government established social media guidelines [38] in October 2020, in conjunction with section 37 of the Prevention of Electronic Crimes Act – 2016. **Social Media Regulations 2020** is another name for these rules. These regulations establish safeguards, a procedure, and a mechanism for the Authority to use its powers under the Act to remove or prevent access to unlawful Online Content via any information system. It also addresses the protection of freedom of speech and expression. It also lays out the steps for submitting, processing, and resolving complaints.

3.11 Pakistan Penal Code

The Pakistan Penal Statute (PPC) [39] is a criminal conduct code that governs the charges that are brought against people in Pakistan. It was first drafted in 1860 and then revised in 1947 upon Pakistan's independence. It is a mixture of both English and Islamic laws. This law does not directly deal with cybercrimes however its sections are being used for conviction of cyber criminals as these are elaborated in such a way that leads to a successful investigation of a cybercrime.

During this research data was collected basing on cybercrime statistics in Pakistan. These statistics help in identifying those high rated cybercrimes which are affecting citizens at the most and highlighting measures which are necessary to curb this menace.

3.10 Cyber-Crime Statistics in Pakistan

Despite technical improvements and anti-cybercrime legislation, the rate of cybercrime in Pakistan has grown by roughly five times in the year 2020 [40]. **The absence of implementation of anti-cybercrime laws is a key contributor to the rise of cybercrime in the country**. According to the Federal Investigation Agency (FIA), which is the sole government agency that deals with cybercrime, 621 people from 22 distinct cybercrime organizations have been detained, and over 20,000 electronic devices have been seized. Thousands of complaints have been filed with the Federal Investigation Agency (FIA) since the passage of the Prevention of Electronic Crimes Act (PECA) in 2016.

“The sale of illegal SIMs is an arrestable offence,” according to PECA, “while illegal access to someone's computer or mobile phone, hate speeches or writing, defining or refining crimes in relation to terrorism or banned organisations, electronic fraud or tampering, stealing and illegally using the identities of others, are all arrestable offences.” According to the Act, cybercrime also includes things like bank account and national identity card details. Cyber stalking or stalking or harassing someone by sending repeated phone or Internet communications without the recipient's agreement, is likewise a felony under the Act.”

According to the FIA, the conviction rate in cybercrime cases is extremely low, which is one of the causes for the rise in crime. The cybercrime wing is confronted with a number of challenges. The data is not available in situations of social media complaints since the cell carriers do not handle it correctly. Financial organisations, such as banks, take time to provide information, and there is no single data bank where all of an identification card's accounts can be verified.

According to the Federal Investigation Agency, cybercrime instances of harassment, blasphemy, anti-religion material, and child pornography have increased dramatically in Pakistan during the last three years (FIA). The most significant increase occurred last year, when the FIA received about 260 complaints per day, resulting in a total of 94,500 complaints in 2020 [41]. The FIA is the only state authority dealing with online crimes which has a meager capacity of handling 12 to 15 complaints per day therefore thousands of complaints remain unattended for months.

These complaints mostly included cybercrime issues such as spamming, identity theft, sexual harassment, child pornography, financial scams, anti-government, hacking, defamation, and the list goes on. The table below provides data for cybercrime complaints received by the FIA in the previous three years, with a total of 159,187 complaints received in the last three years:

Year	Complaints Received	Complaints per day	Rise as compared to previous year	Complaints disposed year wise
2020	94,500	260	98 %	100,357
2019	48,301	133	195 %	1,808
2018	16,122	44	-	9,263

Table-3.1: Cybercrime complaints received in last 3 years

Federal Investigation Agency received complaints of 26 different categories in last 3 years with details as follows:

Category of Complaint	Number of Complaints
Financial Frauds	44,481
Harassment	22,256
Hacking	14,974
Defamation	10,358
Unauthorized Access	9,201

Fake Profiles	6,601
Blackmailing	5,320
Miscellaneous Nature	3,019
Online Shopping	2,678
Threats	2,145
Stalking	1,970
Anti-Religion Content	1,479
Blasphemous Content	1,467
Identity Theft	1,252
Online Jobs Frauds	814
Spoofing	663
Lottery Frauds	612
Online Banking Frauds	450
Illegal SIMs	395
Spamming	361
Pornography	280
Phishing	149
Child Pornography	103
Ant-governmental Stuff	103

Fake Digital Currency	92
Cheaters of BISP	59

Table-3.2: Categories of Cyber-Crimes and number of complaints received

According to certain official estimates, around 111,000 complaints have been addressed in the previous three years, while 50,000 remain unresolved [42]. The FIA received cyber-crime complaints from several zones, and the accompanying table and official statistics reflect zone-specific data:

Zones	**Number of Complaints Received**
Lahore	36,700
Karachi	22,386
Islamabad	20,701
Rawalpindi	15,891
Multan	1,599
Faisalabad	12,145
Gujranwala	8,792
Peshawar	6,605
Hyderabad	4,955
Abbottabad	4,950

DI Khan	2,105
Gilgit-Baltistan	412
Gwadar	184
Sukkur	1,186

Table-3.3: Zone wise cyber-crime complaints received by FIA

As per official data different complaints received by FIA via different communication channels. Following table shows the statistics:

Complaints received from Different Communication Channels	**Number of Complaints Received**
Facebook	42,357
WhatsApp	17,693
Emails	14,109
Phones	8,618
Official Website	5,563
Other Social Media Medium	6,308

Table-3.4: Different communication medias used for registering complaints

According to the data shown above, cybercrime in Pakistan is increasing at an alarming rate, and methods to combat this threat must be implemented in both word and spirit. In this regard, a robust cyber security framework comprised of legal and regulatory frameworks must be developed and implemented so that the prosecution of cyber offenders may begin as soon as feasible and as efficiently as possible.

Chapter - 4

Proposed Cyber Security Framework – A Novel Solution

4.1 NIST Cyber Security Framework

Internationally, the NIST cyber security framework is used as a reference to develop a requirement-based cyber security framework. It consists of five components that are utilized to safeguard information and data. These components are utilized to detect cyber security concerns in a methodical manner, and counteractions are also defined; nevertheless, none of its example components deal with cybercrimes, cyber laws, or cyber dangers, as per our needs. This leads to the inclusion of this new component in the current cyber security framework, which also includes the identification of cyber-crimes and national cyber laws and regulations governing those crimes. The figure below depicts the five initially suggested components of the NIST cyber security architecture [43].

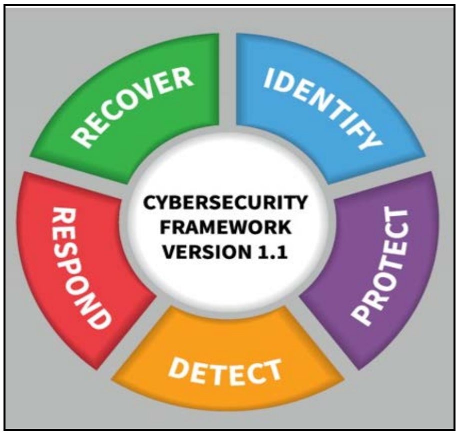
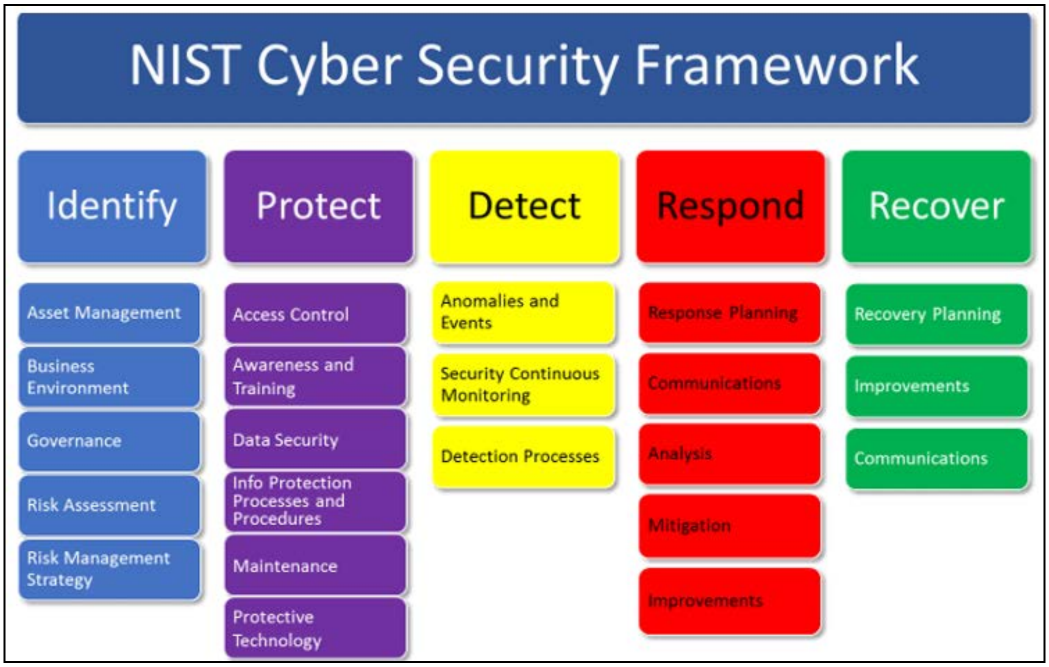


Figure-4.1: Five Main Components of NIST Cyber Security Framework

These five components have been developed in such a way that Identify is used to identify any security breach, Protect is used to provide protection, Detect is used for the mechanism of detection of any loop hole, Respond is for the response mechanism implemented, and Recovery is used to recover any lost data in the event of a cyberattack or security breach. These components have been further sub-categorized in order to elaborate the complete process. As shown below each component is further divided into categories and subcategories [44] to streamline the process of threat detection and mitigation.

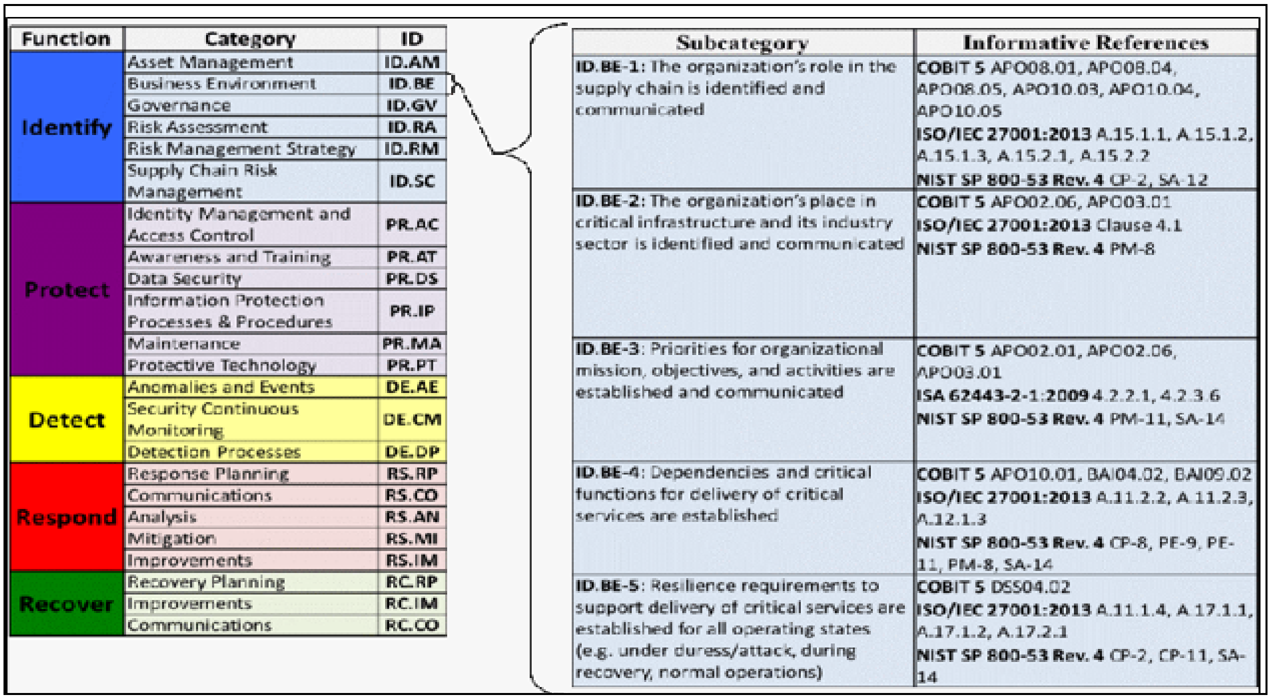


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Figure-4.2: NIST CSF and its Components

The NIST cyber security framework has provided a model for developing one's own cyber security framework to meet national needs in light of the envisioned danger. Basic NIST CSF functions have been classified and sub-categorized [45] in depth to address the framework needs and components contained in the process, and additional useful references have been provided.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure-4.3: Categories and subcategories of NIST CSF components

4.2 Cybercrimes in Pakistan

Pakistan, as a developing digital platform economy, is vulnerable to a wide range of cyber-threats and cyber-attacks. A thorough investigation was conducted in order to highlight the cybercrimes that are currently occurring in the nation [46]. Because of the growing use of the internet and social media, these crimes have also risen, necessitating a concerted effort to contain them, which can only be accomplished by developing and implementing robust cyber laws and regulations and combining them into a unified framework. The following table categorizes the cybercrimes that have been reported in the nation.

Category	Subcategory
Cyber Terrorism	Cyber Terrorism
	Glorification of an offence related to terrorism or banned organizations
	Sectarian violence using social media
	Spreading ethnic hatred using social media or information system
	Projection of banned organizations narrative
	Hate speeches related to inter-faith, sectarian or racial hatred
	Invitation or motivation of funding, recruiting for terrorism or plans for terrorism
	Money Laundering
	Sales of drugs using electronic and information system or websites
Unauthorized data/ Information access	Unauthorized access to information system and data
	Unauthorized copying or transmission of data
	Dishonest Interference with Information system or data
	Unauthorized access to critical infrastructure information system or data
	Unauthorized copying or transmission of critical infrastructure or data
	Interference with critical infrastructure info system or data
	Unauthorized interception of data and information
	Intention to corrupt, destroy or alter information system or data using

	malicious code
	Theft or loss of information system or data using malicious code
Electronic Forgery	Electronic Forgery
	Damage or injury to public property using information system
	Cheating in exams or sharing of papers on social media using information system knowing it to be illegal
	Making illegal claims or titles of property using unauthorized data
	Distribution of false lottery tickets or running fake lottery offices
	Intent to commit fraud by input, alteration, deletion or suppression of data
	Intent to commit fraud by alteration, deletion or suppression of data of a deceased person
	Using unauthentic data for legal purpose knowing its illegal
	Deceiving any person with the help of information system or data
	Making, obtaining or supplying electronic devices for use in offence related to theft of information or data
	Using another person identification information without authorization
	Issuance of illegal SIMs for bank accounts authentication and verification purpose
	Tampering of communication equipment data

Modesty of a Person or Minor	Damaging modesty/ dignity of a person or minor
	Harming personal reputation
	Displaying false information about a person on social/ electronic media
	Superimposing sexually explicit image or photo on the face of a natural person
	Publicly sharing sexually explicit photo or video of a natural person
	Forcing a natural person to engage in sexually explicit act using social or electronic media to take revenge, blackmail or create hatred
	Distribution of child pornographic material
	Illegal production, availability or transmission of child pornographic data using information system
	Possession of data that visually depict minor engaged in sexually explicit conduct
	Distribution of obscene material to underage using information system or social media
	Access/ possession of Dark Web data
	Running brothel houses using social media or information system
	Buying/ Selling of person using social media or information system for prostitution purpose

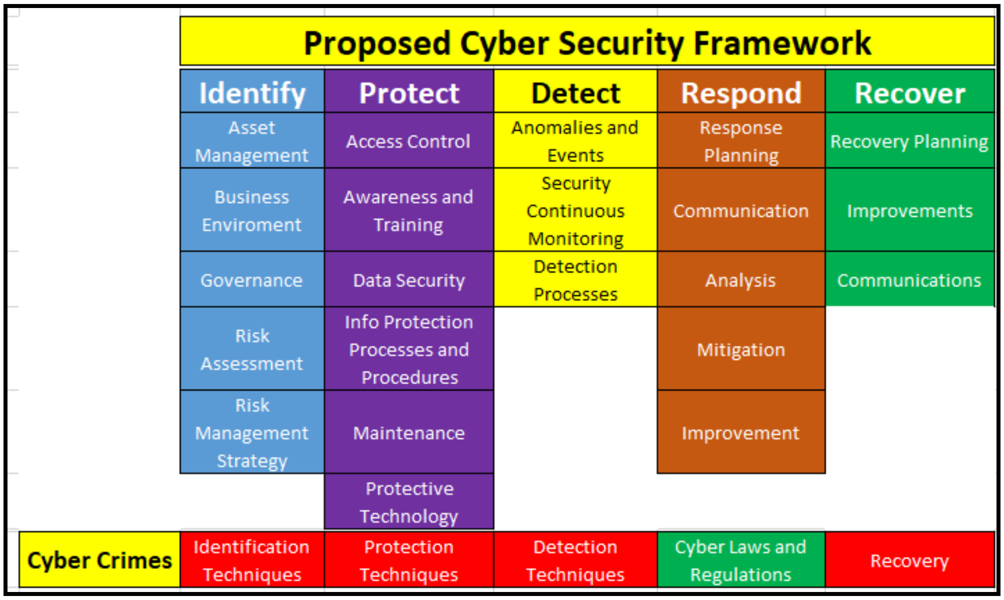
Personal Harassment/ Threat	Harass any person using internet, website, email or information system network
	Monitoring or spying of any person using internet, website, email or information system network
	Putting any person in distress of mind by taking his photo or video without his consent
	Sending unnecessary information to someone without his consent
	Sexual harassment using social media or information system
	Sending advertisement SMS/ messages without unsubscribe option
	Kidnapping using electronic/ social media or information/ communication system
	Sending harmful, misleading or lottery schemes SMS/ messages
	Making fake websites for extracting PII of customer followed by harassment or threat
	Disclosing PII of customer by service provider to third party/ agent for illegal purposes
	Sale/ sharing of customer mobile number with agents without consent of customer
	Criminal intimidation by anonymous calls using information and

	communication media
Unlawful Online Content/ Activity	Blasphemy
	Threat to Interest of glory of Islam by social media
	Creating/ distributing desecrate version of Holy Quran using social media applications or information system
	Hurting religious feeling using social media or information system
	Use of derogatory remarks against holy personages using electronic or social media
	Threat to security or defense of Pakistan using social/ electronic media or information system
	Threat to public order maintenance, decency or morality using information system
	Public incitement against government using media or information system
	Contempt of court using social media or information system
	Selling online goods marked with a counterfeit trademark or property mark
	Online selling of counterfeit currency notes using social media or information system

Table-4.1: Categories of Cybercrimes in Pakistan

4.4 Proposed Cyber Security Framework

The NIST cyber security framework was used as a starting point for developing a national cyber security framework that includes a new component to handle the threat of cybercrime in light of national cyber laws and regulations. Cyber-crimes that are now in the spotlight have been designated as offences, and desirable legislation and regulations have been connected to combat these crimes. As technology advances, new cyber-crime strategies and approaches emerge throughout the world that are now unaddressed by our current laws and regulations. However, at the conclusion of this study, it was recommended to the Higher Education Commission and the relevant ministries of the government of Pakistan to include them into the current anti-cyber legislation. Following the integration of new components into the NIST framework, the proposed cyber security framework includes six main functions, as illustrated below.

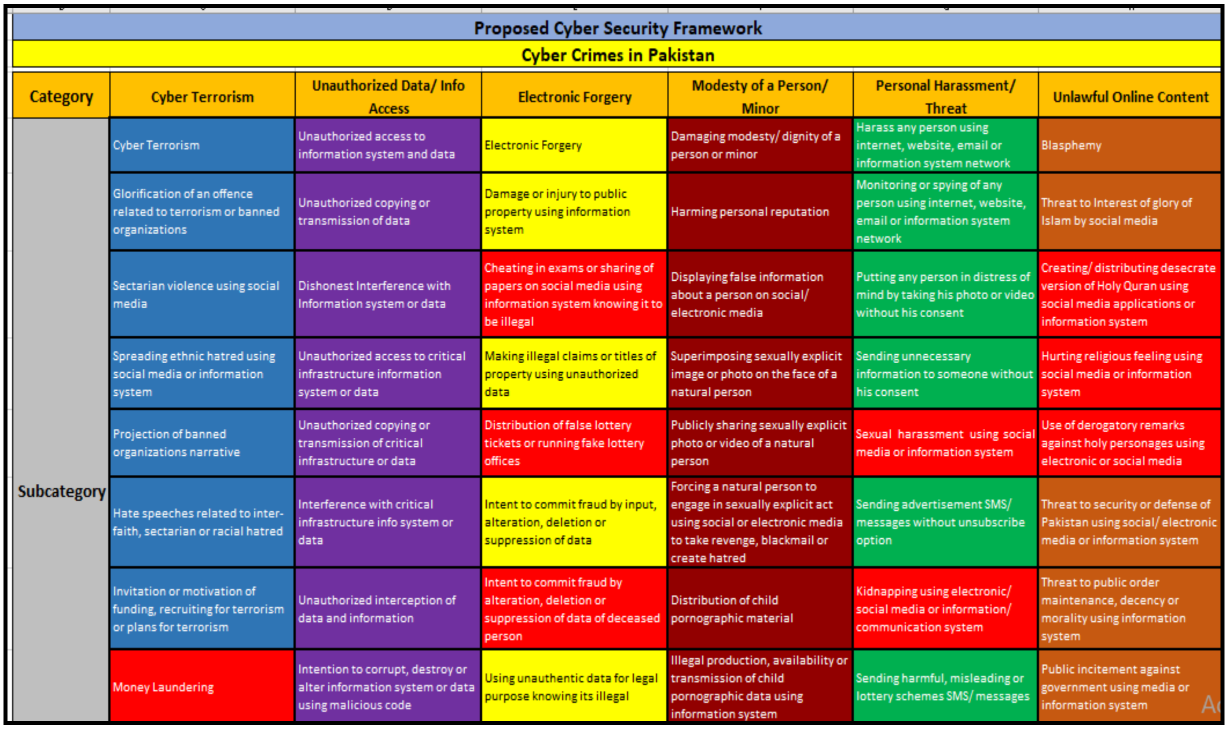


Proposed Cyber Security Framework

	Identify	Protect	Detect	Respond	Recover
	Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
	Business Enviroment	Awareness and Training	Security Continuous Monitoring	Communication	Improvements
	Governance	Data Security	Detection Processes	Analysis	Communications
	Risk Assessment	Info Protection Processes and Procedures		Mitigation	
	Risk Management Strategy	Maintenance		Improvement	
		Protective Technology			
Cyber Crimes	Identification Techniques	Protection Techniques	Detection Techniques	Cyber Laws and Regulations	Recovery

Figure-4.4: Proposed Cyber Security Framework

Cybercrime is introduced as a new component in this proposed cyber security framework, which deals with cyber-crimes that are reported in the country and are classified as offences under national cyber laws. This component is further classified into six categories and seventy subcategories. Cybercrimes that have been identified at national level have been incorporated in these subcategories.



Proposed Cyber Security Framework						
Cyber Crimes in Pakistan						
Category	Cyber Terrorism	Unauthorized Data/ Info Access	Electronic Forgery	Modesty of a Person/ Minor	Personal Harassment/ Threat	Unlawful Online Content
Subcategory	Cyber Terrorism	Unauthorized access to information system and data	Electronic Forgery	Damaging modesty/ dignity of a person or minor	Harass any person using internet, website, email or information system network	Blasphemy
	Glorification of an offence related to terrorism or banned organizations	Unauthorized copying or transmission of data	Damage or injury to public property using information system	Harming personal reputation	Monitoring or spying of any person using internet, website, email or information system network	Threat to Interest of glory of Islam by social media
	Sectarian violence using social media	Dishonest Interference with Information system or data	Cheating in exams or sharing of papers on social media using information system knowing it to be illegal	Displaying false information about a person on social/ electronic media	Putting any person in distress of mind by taking his photo or video without his consent	Creating/ distributing desecrate version of Holy Quran using social media applications or information system
	Spreading ethnic hatred using social media or information system	Unauthorized access to critical infrastructure information system or data	Making illegal claims or titles of property using unauthorized data	Superimposing sexually explicit image or photo on the face of a natural person	Sending unnecessary information to someone without his consent	Hurting religious feeling using social media or information system
	Projection of banned organizations narrative	Unauthorized copying or transmission of critical infrastructure or data	Distribution of false lottery tickets or running fake lottery offices	Publicly sharing sexually explicit photo or video of a natural person	Sexual harassment using social media or information system	Use of derogatory remarks against holy personages using electronic or social media
	Hate speeches related to inter-faith, sectarian or racial hatred	Interference with critical infrastructure info system or data	Intent to commit fraud by input, alteration, deletion or suppression of data	Forcing a natural person to engage in sexually explicit act using social or electronic media to take revenge, blackmail or create hatred	Sending advertisement SMS/ messages without unsubscribe option	Threat to security or defense of Pakistan using social/ electronic media or information system
	Invitation or motivation of funding, recruiting for terrorism or plans for terrorism	Unauthorized interception of data and information	Intent to commit fraud by alteration, deletion or suppression of data of deceased person	Distribution of child pornographic material	Kidnapping using electronic/ social media or information/ communication system	Threat to public order maintenance, decency or morality using information system
	Money Laundering	Intention to corrupt, destroy or alter information system or data using malicious code	Using unauthentic data for legal purpose knowing its illegal	Illegal production, availability or transmission of child pornographic data using information system	Sending harmful, misleading or lottery schemes SMS/ messages	Public incitement against government using media or information system

Figure-4.5: Categories and subcategories of Cybercrimes in Proposed Cyber Security Framework

Cybercrime in the country has been addressed in six primary areas, which are further subdivided into 70 subcategories in the proposed framework component. The majority of cybercrimes included in this component are dealt by national cybercrime legislation; nevertheless, fewer have been discovered that require the attention of related departments. Presently **Prevention of Electronic Crime Act (PECA) – 2016** [47], **Pakistan Penal Code (PPC)** [48], **Electronic Transactions Ordnance (ETO) – 2002** [49] are dealing which majority of these crimes. Cyber-crimes and their reference laws are mentioned in the following table.

Category	Subcategory	Reference Law
Cyber Terrorism	Cyber Terrorism	PECA Sec-10
	Glorification of an offence related to terrorism or banned organizations	PECA Sec-9
	Sectarian violence using social media	PECA Sec-10 PPC Sec-154 A
	Spreading ethnic hatred using social media or information system	PECA Sec-10 PPC Sec-154 A
	Projection of banned organizations narrative	PECA Sec-10
	Hate speeches related to inter-faith, sectarian or racial hatred	PECA Sec-10A PPC Sec-154 A
	Invitation or motivation of funding, recruiting for terrorism or plans for terrorism	PECA Sec-10B
	Money Laundering	Not included in Cybercrime Laws
	Sales of drugs using electronic and information system or websites	PPC Sec-276
Unauthorized data/	Unauthorized access to information system and data	PECA Sec-3 ETO Sec-36

Information access	Unauthorized copying or transmission of data	PECA Sec-4 ETO Sec-37
	Dishonest Interference with Information system or data	PECA Sec-5 ETO Sec-37
	Unauthorized access to critical infrastructure information system or data	PECA Sec-6 ETO Sec-36
	Unauthorized copying or transmission of critical infrastructure or data	PECA Sec-7 ETO Sec-37
	Interference with critical infrastructure info system or data	PECA Sec-8 ETO Sec-37
	Unauthorized interception of data and information	PECA Sec-17 ETO Sec-36
	Intention to corrupt, destroy or alter information system or data using malicious code	PECA Sec-20 ETO Sec-37
	Theft or loss of information system or data using malicious code	PECA Sec-20
Electronic Forgery	Electronic Forgery	PECA Sec-11 PPC Sec-463
	Damage or injury to public property using	PECA Sec-11

	information system	
	Cheating in exams or sharing of papers on social media using information system knowing it to be illegal	PPC Sec-415
	Making illegal claims or titles of property using unauthorized data	PECA Sec-11 PPC Sec-403
	Distribution of false lottery tickets or running fake lottery offices	PPC Sec-294 A
	Intent to commit fraud by input, alteration, deletion or suppression of data	PECA Sec-11
	Intent to commit fraud by alteration, deletion or suppression of data of deceased person	PPC Sec-404
	Using unauthentic data for legal purpose knowing its illegal	PECA Sec-11
	Deceiving any person with the help of information system or data	PECA Sec-12
	Making, obtaining or supplying electronic devices for use in offence related to theft of information or data	PECA Sec-13

	Using another person identification information without authorization	PECA Sec-14
	Issuance of illegal SIMs for bank accounts authentication and verification purpose	PECA Sec-15
	Tampering of communication equipment data	PECA Sec-16
Modesty of a person or minor	Damaging modesty/ dignity of a person or minor	PECA Sec-18
	Harming personal reputation	PECA Sec-18 PPC Sec-499
	Displaying false information about a person on social/ electronic media	PECA Sec-18
	Superimposing sexually explicit image or photo on the face of a natural person	PECA Sec-19
	Publicly sharing sexually explicit photo or video of a natural person	PECA Sec-19
	Forcing a natural person to engage in sexually explicit act using social or electronic media to take revenge, blackmail or create hatred	PECA Sec-19
	Distribution of child pornographic material	PECA Sec-19A
	Illegal production, availability or transmission of	PECA Sec-19A

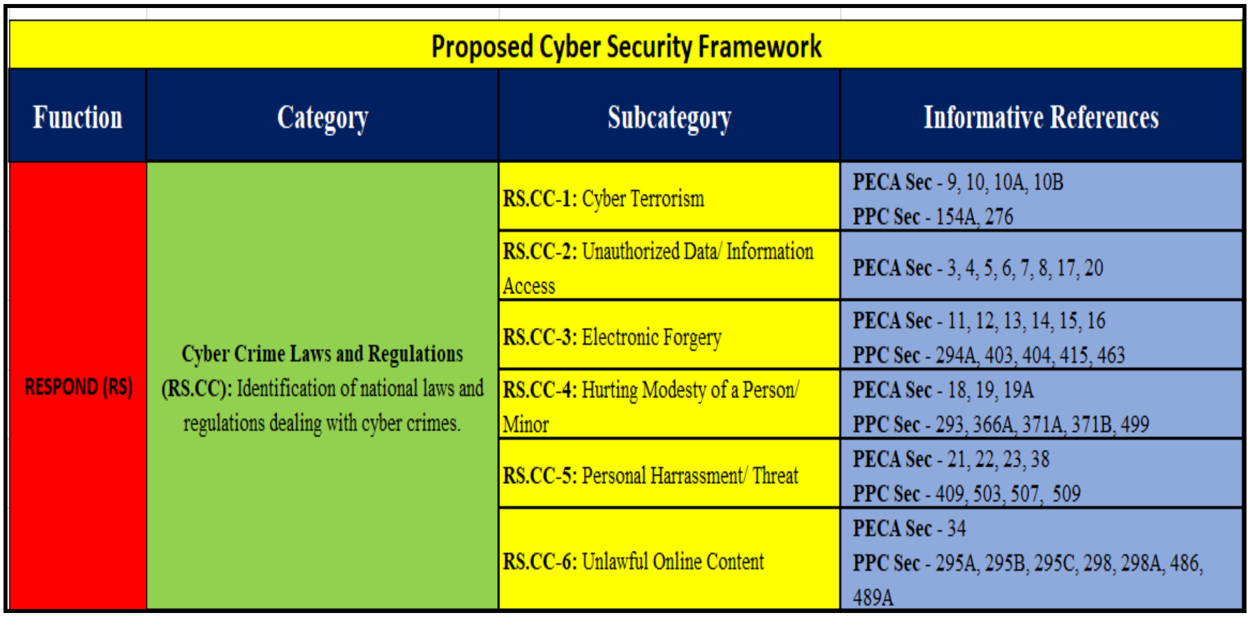
	child pornographic data using information system	PPC Sec-366 A
	Possession of data that visually depict minor engaged in sexually explicit conduct	PECA Sec-19A
	Distribution of obscene material to underage using information system or social media	PPC Sec-293
	Access/ possession of Dark Web data	Not included in Cybercrime Laws
	Running brothel houses using social media or information system	PPC Sec-371 A
	Buying/ Selling of person using social media or information system for prostitution purpose	PPC Sec-371 B
Personal Harassment/ Threat	Harass any person using internet, website, email or information system network	PECA Sec-21 PPC Sec-503
	Monitoring or spying of any person using internet, website, email or information system network	PECA Sec-21
	Putting any person in distress of mind by taking his photo or video without his consent	PECA Sec-21
	Sending unnecessary information to someone without his consent	PECA Sec-22

	Sexual harassment using social media or information system	PPC Sec-509
	Sending advertisement SMS/ messages without unsubscribe option	PECA Sec-22
	Sending harmful, misleading or lottery schemes SMS/ messages	PECA Sec-22
	Making fake websites for extracting PII of customer followed by harassment or threat	PECA Sec-23
	Disclosing PII of customer by service provider to third party/ agent for illegal purposes	PECA Sec-38 PPC Sec-409
	Sale/ sharing of customer mobile number with agents without consent of customer	PPC Sec-409
	Criminal intimidation by anonymous calls using information and communication media	PPC Sec-507
Unlawful Online Content	Blasphemy	PECA Sec-34 PPC Sec-295 C
	Threat to Interest of glory of Islam by social media	PECA Sec-34 PPC Sec-295 A
	Creating/ distributing desecrate version of Holy	PPC Sec-295 B

	Quran using social media applications or information system	
	Hurting religious feeling using social media or information system	PPC Sec-298
	Use of derogatory remarks against holy personages using electronic or social media	PPC Sec-298 A
	Threat to security or defense of Pakistan using social/ electronic media or information system	PECA Sec-34
	Threat to public order maintenance, decency or morality using information system	PECA Sec-34
	Public incitement against government using media or information system	PECA Sec-34
	Contempt of court using social media or information system	PECA Sec-34
	Selling online goods marked with a counterfeit trademark or property mark	PPC Sec-486
	Online selling of counterfeit currency notes using social media or information system	PPC Sec-489 A

Table-4.2: National laws dealing with domestic cyber-crimes

In order to combat the threat of cybercrime, national cyber laws have also been integrated into the proposed Cyber Security Framework. The chart below depicts the detailed structure in which cyber-crimes have been designated as offences under national cyber legislation.



Proposed Cyber Security Framework

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Cyber Crime Laws and Regulations (RS.CC):** Identification of national laws and regulations dealing with cyber crimes.	**RS.CC-1:** Cyber Terrorism	**PECA Sec** - 9, 10, 10A, 10B **PPC Sec** - 154A, 276
		RS.CC-2: Unauthorized Data/ Information Access	**PECA Sec** - 3, 4, 5, 6, 7, 8, 17, 20
		RS.CC-3: Electronic Forgery	**PECA Sec** - 11, 12, 13, 14, 15, 16 **PPC Sec** - 294A, 403, 404, 415, 463
		RS.CC-4: Hurting Modesty of a Person/ Minor	**PECA Sec** - 18, 19, 19A **PPC Sec** - 293, 366A, 371A, 371B, 499
		RS.CC-5: Personal Harrassment/ Threat	**PECA Sec** - 21, 22, 23, 38 **PPC Sec** - 409, 503, 507, 509
		RS.CC-6: Unlawful Online Content	**PECA Sec** - 34 **PPC Sec** - 295A, 295B, 295C, 298, 298A, 486, 489A

Figure-4.6: Incorporation of National Cyber Laws in the Proposed Framework

4.5 Beneficiaries

Because of the inclusion of country cyber laws, the following companies will be able to profit from the development of this cyber security framework in order to address their cyber security related issues and mitigate cyber-crime. This will aid them in prosecuting cyber criminals and expediting their legal obligations, as well as improving their time management skills while dealing with cybercrime.

- Government and Private Organizations using Information and Communication Technologies (ICT) services.
- Military and Critical Installations.
- National Cyber Security elements.
- IT Industry.
- Telecom Industry.
- Transport Industry.
- Banking Sector.
- Health Industry.

4.6 Recommendations

As the single dealer of cyber and electronic crimes in Pakistan, PECA must be well stocked with all types of cybercrime. As a result, it requires an overhaul. Keeping in mind the most recent developments in cyber-attack regimes and the lack of laws dealing with new cyber-crimes and cyber bullying, the following items have been proposed to government via responsible departments for incorporation into existing cyber-crime legislation.

- Because PECA does not address the issue of theft, stealing credit card credentials or identity theft must be stated in detail.
- Money laundering should be included in PECA since electronic media is currently being exploited for this threat of money crimes. It should be included

in cyber terrorism since it indicates that a large portion of money moved illegally is utilized for terrorism and corruption.

- Child abuse should be prioritized in PECA since electronic media is utilized to spread it, affecting the bereaved family.
- Dark web content, including its reading, copying, transfer, and dissemination, is not covered by PECA, which must be handled immediately.
- There is no reference in any legislation of an organization's or company's reaction to cyber-attacks, such as the requirement to notify the government cyber-attack response team (FIA CERT) within 24 hours, as is customary worldwide.
- Hacking should be classified as a non-bailable offence rather than a bailable offence.
- The online sale of drugs or the selling of drugs through any information system, which is becoming a prevalent practice in the country, is to be classified as cyber terrorism.
- The distribution of obscene content to minors via information systems or social media should also be included in PECA.
- False lottery ticket distribution and the operation of bogus lottery offices should be classified as electronic crimes under PECA.

- The sale or sharing of a customer's cell number with an agent for marketing purposes without the customer's agreement, which might cause undue disruption for the consumer, is a violation of this act.
- Creating and disseminating a desecrated version of the Holy Quran via social media applications or an information system will be classified as an electronic crime.
- Harming religious feelings through social media or information systems should also be included in this conduct.
- Use of disparaging statements about holy figures on electronic or social media will be classified as an electronic crime.
- Using social media or an information system to run brothel houses, which will be addressed by PECA.
- Using social media or an information system to buy or sell people for prostitution should be classified as an electronic crime.
- The intent to commit fraud by entering, altering, deleting, or suppressing data of a deceased person should likewise be classified as an electronic crime.
- Cheating in examinations or distributing documents on social media while knowing it is prohibited should be classified as electronic crime.
- Selling items online that bear a counterfeit trademark or property mark will be classified as an electronic crime.

- Online selling of counterfeit currency notes via social media or information systems should be classified as electronic crime under PECA, as should criminal intimidation via anonymous calls via information and communication media.
- PECA should handle the crime of sexual harassment through the use of social media or information systems. In PECA, a balance must be struck between cyber security and citizens' basic rights. If the former infringes on the latter, it will fail.
- Any individual convicted of a relevant cybercrime should be barred from serving in any important position linked to network security management or operations for the rest of their lives, as is standard practice across the world.
- It takes time for financial institutions, such as banks, to give information, and there is no central data bank where all of an identification card's accounts may be checked. As a result, the government should compel one bank to keep a record of all identity cards and account holders' data as a data bank.

Chapter - 5

Threat Modeling of Cyber Attacks on a Banking System - A Case Study

Because of the current COVID-19 environment, online banking, data operations, and internet usage in Pakistan have risen several times, resulting in an increase in cyber-crime. Banks have been shown to be the most often attacked by hackers throughout the world, resulting in financial and reputational harm. Because cyber-crime laws in Pakistan are not strict in dealing with cybercriminals, an attempt has been made to streamline the procedure of detecting, protecting, identifying, and prosecuting a cybercriminal, particularly by those establishments dealing with financial concerns. A cyber security framework that has previously been established may be utilized successfully to decrease these dangers, as can be used as a procedure for prosecuting cyber offenders under national cyber laws. In this case study, a complete threat modelling method for the banking industry was established, and national cyber laws were highlighted in order to prosecute offenders utilizing the proposed cyber security framework.

The National Institute of Standards and Technology (NIST) Cyber Security Framework [50] was established as a suite for dealing with cyber risks and cyber-attacks. It provides a detailed method for identifying, protecting, detecting, responding to, and recovering from cyberattacks, as well as industry best practices and standards.

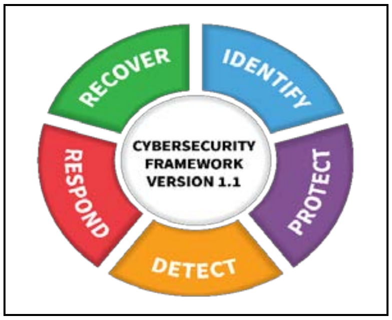
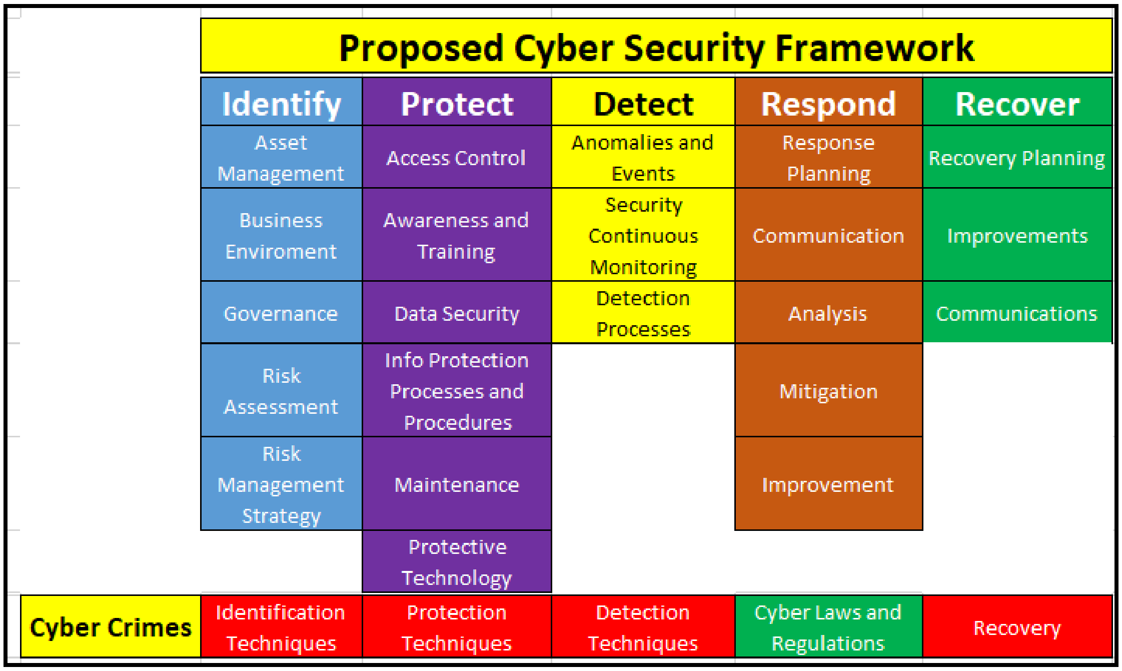


Figure-5.1: NIST Cyber Security Framework

The proposed cyber security framework as shown below deals with cyber-crimes by incorporating national cyber laws and regulations.



	Proposed Cyber Security Framework				
	Identify	Protect	Detect	Respond	Recover
	Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
	Business Enviroment	Awareness and Training	Security Continuous Monitoring	Communication	Improvements
	Governance	Data Security	Detection Processes	Analysis	Communications
	Risk Assessment	Info Protection Processes and Procedures		Mitigation	
	Risk Management Strategy	Maintenance		Improvement	
		Protective Technology			
Cyber Crimes	Identification Techniques	Protection Techniques	Detection Techniques	Cyber Laws and Regulations	Recovery

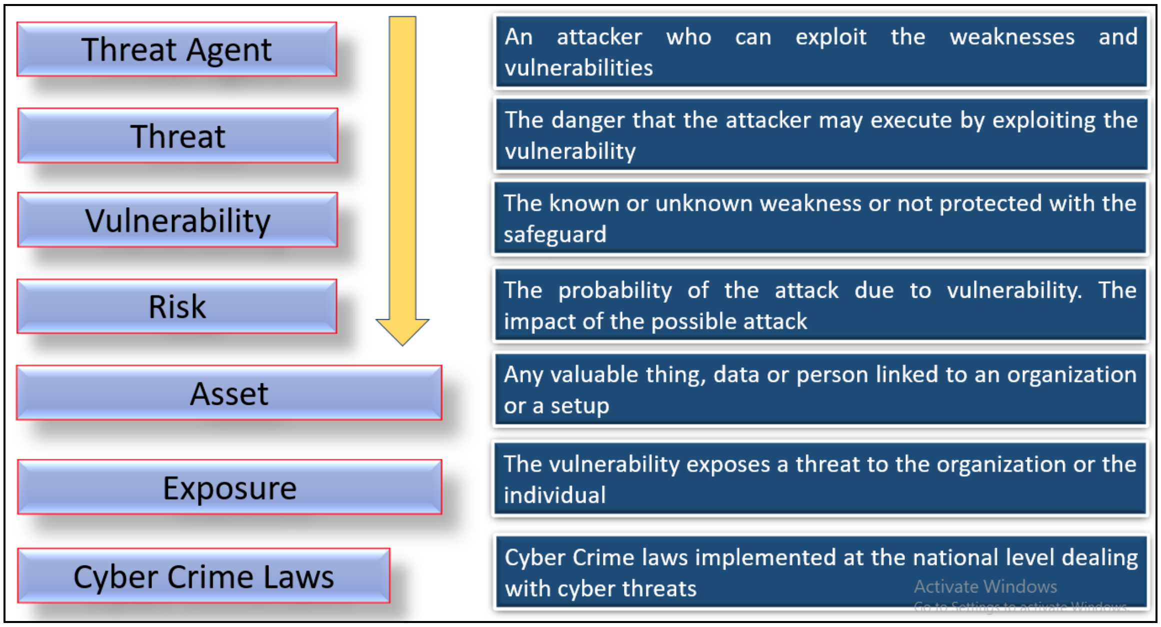
Figure-5.2: Proposed Cyber Security Framework dealing with Cyber Crimes

5.1 Threat Modeling: Banking System

Threat modelling of Pakistan's banking system has been used as a case study to develop the proposed cyber security framework, which would aid in the regulation of national cyber laws. This framework operates by substituting strong national cyber laws for mitigation measures used in response to cyber-attacks. Different types of potential cyber-attacks on the financial system and its assets have been identified, and national laws and regulations addressing such cyber-crimes have been integrated into this case study. This threat modelling method [51] will assist various governmental and private entities in Pakistan in dealing with diverse threats in light of the country's existing cyber regulations. Following the adoption and execution of the **Prevention of Electronic Crimes Act (PECA) – 2016** [52] in Pakistan, the protection of consumer data and information has been accorded appropriate significance [53], and associated regulations and sanctions for perpetrators of security breaches have been specified. **PECA can also contribute to enhance the security of banking system**.

5.2 Audience

This case study has been particularly designed to integrate national cyber laws for the offences that are most likely to be committed in the banking or financial industry. It will assist managers and security administrators in dealing with various legal concerns linked to cybercrime and financial transaction fraud [54]. This case study is intended for security managers in businesses that deal with financial problems and data security in relation to financial transactions. It may also be used as a guideline for companies that face a direct or indirect danger from cyber-attackers to their customers' data and privacy [55]. The picture below depicts a typical threat modelling environment [56,57] in which cyber-attack mitigation measures have been substituted by cyber laws to facilitate the prosecution of cyber offenders.



Threat Agent

An attacker who can exploit the weaknesses and vulnerabilities

Threat

The danger that the attacker may execute by exploiting the vulnerability

Vulnerability

The known or unknown weakness or not protected with the safeguard

Risk

The probability of the attack due to vulnerability. The impact of the possible attack

Asset

Any valuable thing, data or person linked to an organization or a setup

Exposure

The vulnerability exposes a threat to the organization or the individual

Cyber Crime Laws

Cyber Crime laws implemented at the national level dealing with cyber threats

Figure-5.3: Threat Modeling Landscape

5.3 Document Structure

This document is organized into following sections.

- **Section – 1**: Possible Threat Agents and Attack Vectors
- **Section – 2**: Banking Assets
- **Section – 3**: National Cyber Laws dealing with Attack Vectors

Section - 1: Possible Threat Agents and Attack Vectors

5.3.1 The Attack Side

"If you know the enemy and know yourself, you need not fear the results of a hundred battles", Sun Tzu wrote in his famous book, The Art of War.

Knowledge of the adversary is critical because defeating your opponent requires knowledge about your enemy, and the same is true in the realm of cyber security. The financial services business is the most often targeted by cyber thieves. When preparing an assault on the financial industry, the attackers' primary focus remains on fraud, burglarizing ATMs, performing transactions using fast systems, and infiltrating financial companies' intranets using banking malware.

- **Vulnerability**

A vulnerability is defined as any trust assumption involving people, procedures, or technology that may be broken in order to exploit a system [51]. The most prevalent vulnerabilities in the banking industry are:

  - Software flaw vulnerability.
  - Security configuration issue vulnerability.
  - Software feature misuse vulnerability like user credentials stolen and misused by someone else to gain access.
  - Leakage profiling of banking system in which an attacker tries to steal customer password, as shown in the following figure.

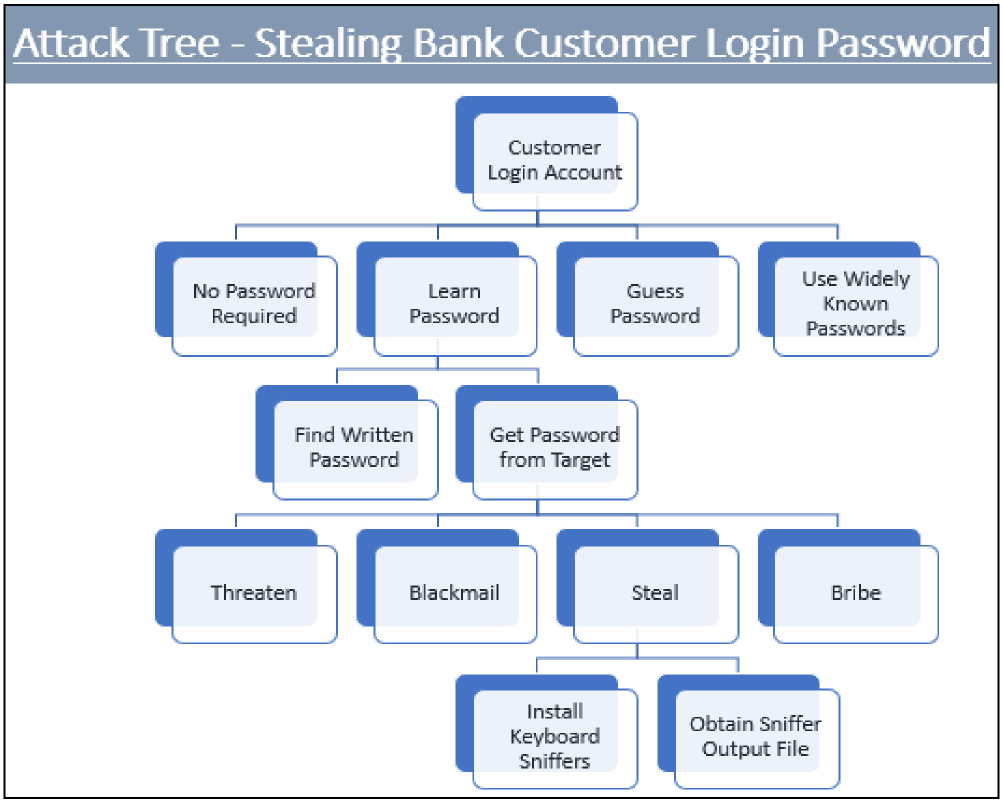


Figure-5.4: Relationship diagram of a scenario of stealing login password of a customer

- **Exploit and Attack**

Exploiting a vulnerability is using it to breach security goals like confidentiality, integrity, and availability. A successful assault (activity) is also known as an exploit [51]. Exploitation is further classified into two types:

- **Intentional**

There are two types of motivations: a desire to make political or social comments for financial benefit, or a desire to engage in cyberwarfare. An attacker may have short-term goals, such as money transactions, or long-term goals, such as getting access to sensitive data.

A malevolent insider may potentially collaborate with an external attacker, for example, by selling their usernames and passwords to third parties.

- o **Inadvertent**

  Attackers who inadvertently exploit vulnerabilities do so by mistake or due to a lack of understanding, such as executing activities that they are unaware are security breaches or do not perceive to be a serious security concern [51].

- **Threat Agents**

These are the potential attackers/criminals [57], and in our case study, the financial system may be attacked by the following threat agents:

- ▪ **Cyber Attackers**

  These are the types of attackers who may target the financial system for monetary or personal gain.

- ▪ **Hackers-for-hire**

  These are individuals that have specialized expertise in hacking computer systems and are recruited by third parties to hack financial systems in exchange for monetary compensation.

- ▪ **Banking Staff**

  Banking employees might potentially engage in harmful behavior by exchanging personal identity information with third parties for monetary gain.

- **Criminal Gangs**

  These individuals are constantly on the lookout for methods to attack people for monetary gain, and bank clients and account holders are their primary targets.

- **Insiders – Bank technical staff**

  The most dangerous force in the banking system is its technological team, which is the primary source of exposing personal information of clients and transaction data if compromised.

- **Money Launderers**

  These are the rising skilled crooks in our society who route their money through various unlawful ways in order to escape the taxes procedure.

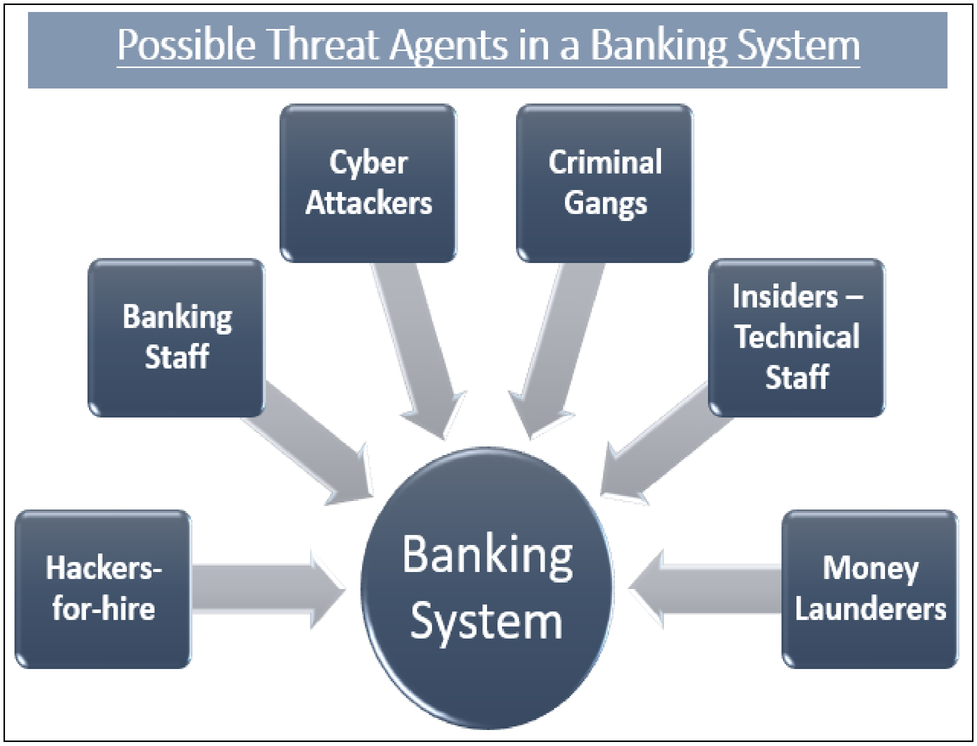


Figure-5.5: Likely Threat Agents in a Banking System

These attackers can inflict significant damage to a financial system and its clients, whereas cyber criminals will attempt to acquire remote access to systems where they can manage all data [58] and perform the following crimes:

- They may result in financial loss (by making false transaction).
- They have the ability to steal sensitive information and sell it, as well as utilise it for spying or terrorism.
- They can target customers by launching an attack on a company. It might lead to consumer annoyance or identity theft.
- A company's public image might suffer as a result of inadequate information security compliance.

- **Attack Vector**

  It is the section of the whole pathway that an attacker utilizes to reach a vulnerability [59], and the following attack vectors might be suspected in a financial system:

  - A malicious web page content.
  - A malicious email attachment.
  - A network service with inherent vulnerabilities.
  - Social-engineering-based conversation.
  - Stolen user credentials.
  - Personal information retrieval using weak password.

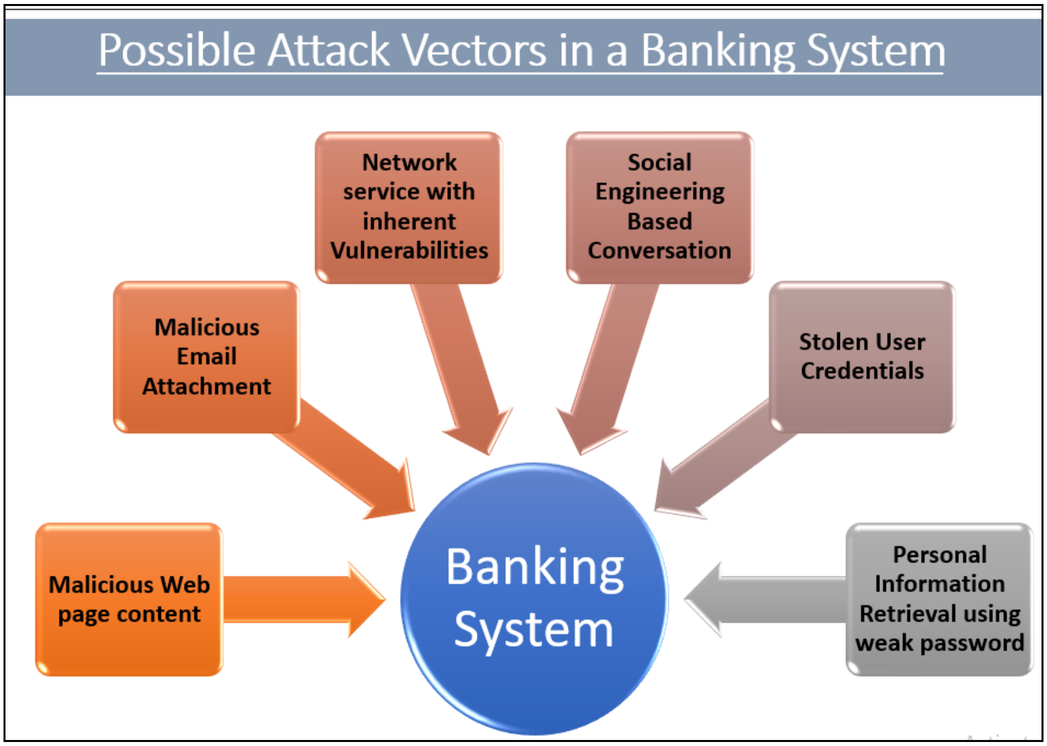

Possible Attack Vectors in a Banking System
Network service with inherent Vulnerabilities
Social Engineering Based Conversation
Malicious Email Attachment
Stolen User Credentials
Malicious Web page content
Banking System
Personal Information Retrieval using weak password

Figure-5.6: Possible Attack Vectors in a Banking System

- **Attack Vectors Specific to Our Case Study**

The following are the attack vectors or cyber-crimes that were highlighted in our case study. Each attack vector index indicates an attack type, along with a description.

- **T-1**: Hacking (Illegal Access to Data).
- **T-2**: Unauthorized Access to Critical Infrastructure Information System or Data.
- **T-3**: Unauthorized Copying or Transmission of Critical Infrastructure Data.
- **T-4**: Interference with Critical Infrastructure Information System or Data.

- **T-5**: Cyber Terrorism.
- **T-6**: Electronic Forgery – Critical Infrastructure Information System.
- **T-7**: Electronic Fraud.
- **T-8**: Unauthorized use of Identity Information.
- **T-9**: Malicious Code.
- **T-10**: Unauthorized Issuance of SIM cards for Banking Authentication Purpose.
- **T-11**: Unauthorized Interception of Communication.
- **T-12**: Cyber Stalking – Threat to Customer (Bank Asset).
- **T-13**: Spoofing – Creation of Illegal Bank Account Login Pages.

- **Threat**

“An incident that has the potential to have a negative impact on organizational operations and assets, individual other organizations, or the nation via an information system through illegal access, destruction, disclosure, or alteration of information, and/or denial of service.” A threat source causes a threat event. In our case study, banking information security assets are always under threat from cyber attackers.

Section – 2: Banking Assets

5.3.2 Assets

Banking sector has following information security assets [60] each represented by asset vector followed by its description:

- **A-1: Customer Bio Data Information** – It provides information on the customer's personal information.
- **A-2: Information Assets** – Customers' and employees' communication security and login passwords are all saved.
- **A-3: Electronic Financial Transactions** – Data pertaining to a customer's financial transactions is saved as a bank asset.
- **A-4: E-Commerce** – Payment information from consumers utilized during online purchases via computers is saved as a bank asset.
- **A-5: M-Commerce** – Payments-related data from consumers utilized during online sales purchases made with mobile devices is saved as a bank asset.
- **A-6: Government Securities** – Transactions done by governmental agencies utilizing the banking online system, as well as their employees' financial security, are recorded and handled.
- **A-7: Investments** – Online transaction statistics of investors who have put money into bank-leading initiatives.

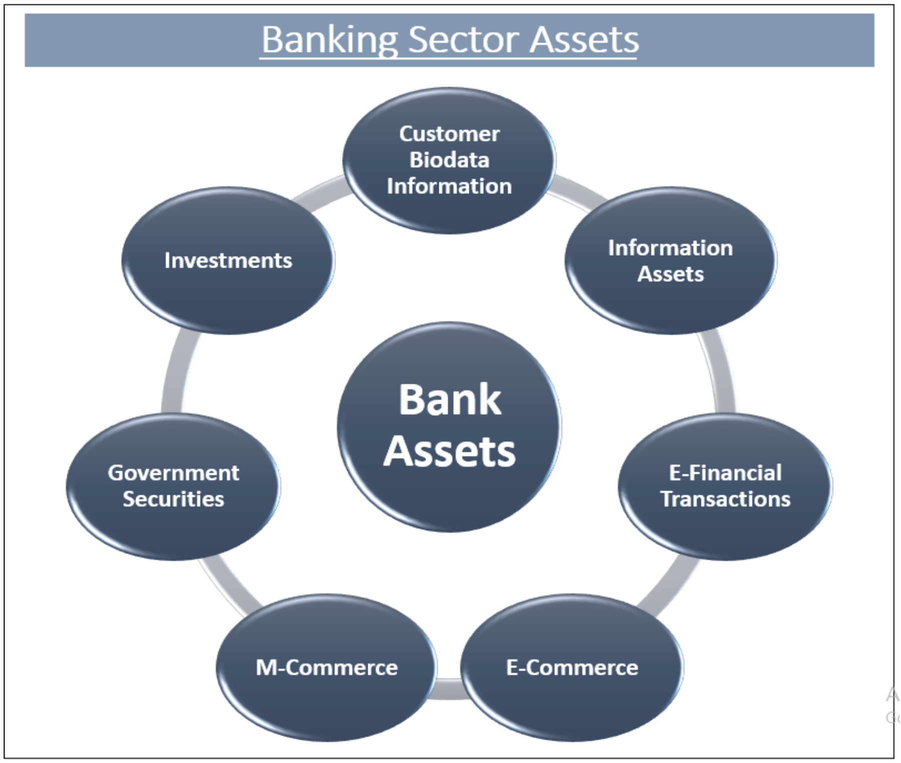
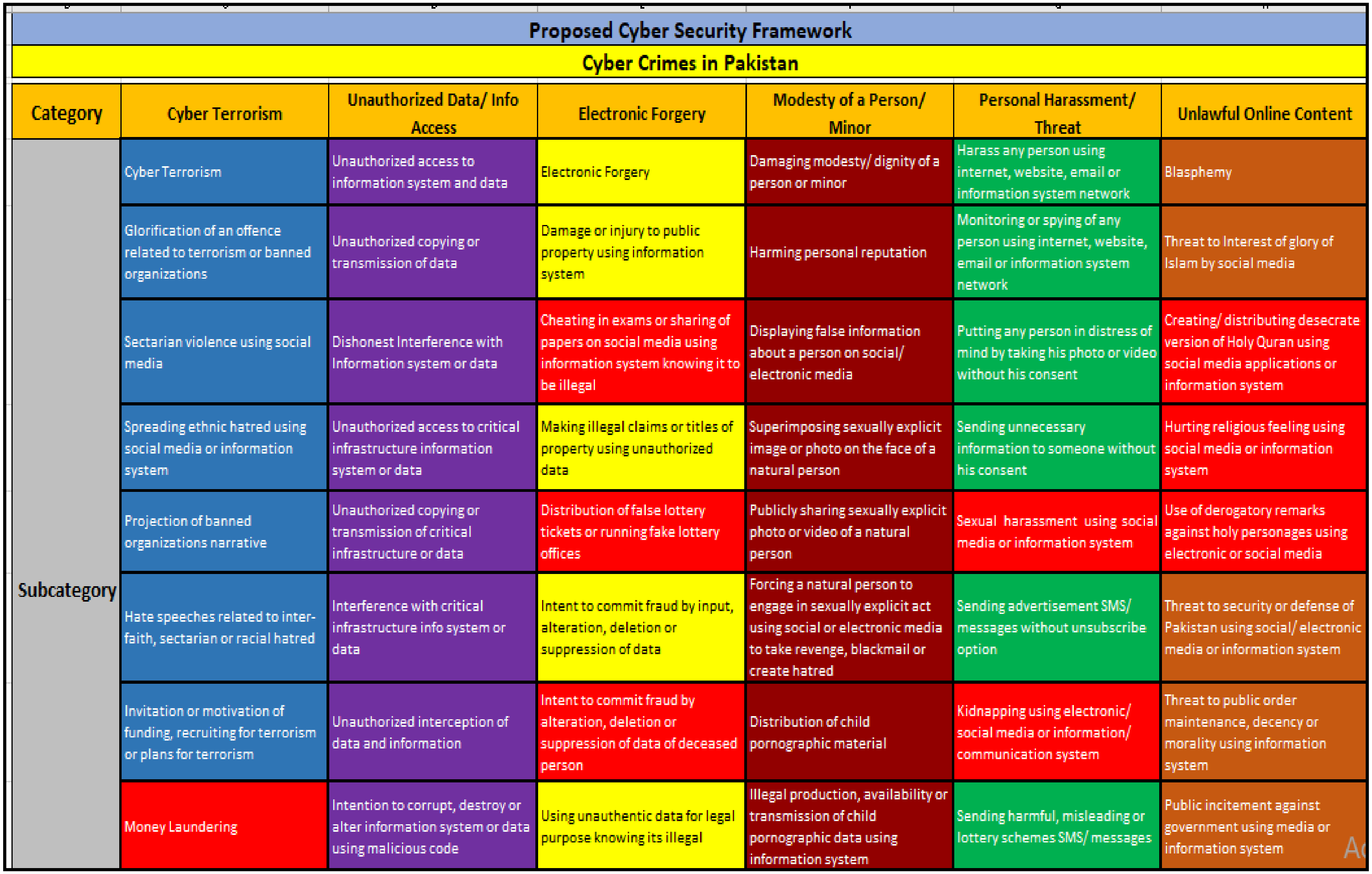


Figure-5.7: Assets related to a Banking Sector

Section - 3: National Cyber Laws Dealing with Attack Vectors

5.3.3 A new component dealing with cybercrime has been included to the proposed cyber security framework. This component falls under the Respond function, which involves the modification of cyber-crime mitigation strategies in accordance with national cyber laws and regulations. These cybercrimes have been further classified, and country laws and regulations dealing with them have been included as useful references [61].

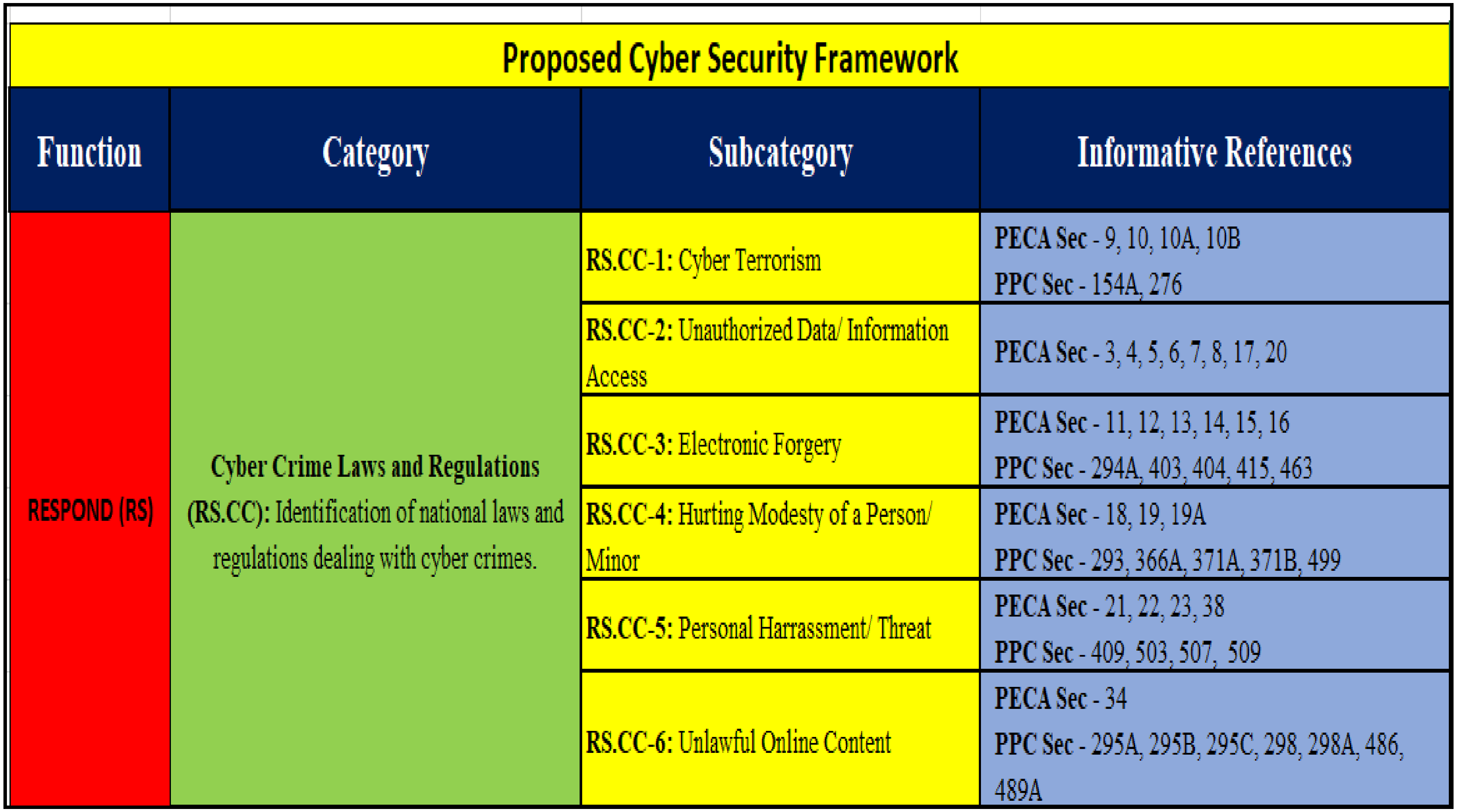


Proposed Cyber Security Framework

Cyber Crimes in Pakistan

Category	Cyber Terrorism	Unauthorized Data/ Info Access	Electronic Forgery	Modesty of a Person/ Minor	Personal Harassment/ Threat	Unlawful Online Content
Subcategory	Cyber Terrorism	Unauthorized access to information system and data	Electronic Forgery	Damaging modesty/ dignity of a person or minor	Harass any person using internet, website, email or information system network	Blasphemy
	Glorification of an offence related to terrorism or banned organizations	Unauthorized copying or transmission of data	Damage or injury to public property using information system	Harming personal reputation	Monitoring or spying of any person using internet, website, email or information system network	Threat to Interest of glory of Islam by social media
	Sectarian violence using social media	Dishonest Interference with Information system or data	Cheating in exams or sharing of papers on social media using information system knowing it to be illegal	Displaying false information about a person on social/ electronic media	Putting any person in distress of mind by taking his photo or video without his consent	Creating/ distributing desecrate version of Holy Quran using social media applications or information system
	Spreading ethnic hatred using social media or information system	Unauthorized access to critical infrastructure information system or data	Making illegal claims or titles of property using unauthorized data	Superimposing sexually explicit image or photo on the face of a natural person	Sending unnecessary information to someone without his consent	Hurting religious feeling using social media or information system
	Projection of banned organizations narrative	Unauthorized copying or transmission of critical infrastructure or data	Distribution of false lottery tickets or running fake lottery offices	Publicly sharing sexually explicit photo or video of a natural person	Sexual harassment using social media or information system	Use of derogatory remarks against holy personages using electronic or social media
	Hate speeches related to inter-faith, sectarian or racial hatred	Interference with critical infrastructure info system or data	Intent to commit fraud by input, alteration, deletion or suppression of data	Forcing a natural person to engage in sexually explicit act using social or electronic media to take revenge, blackmail or create hatred	Sending advertisement SMS/ messages without unsubscribe option	Threat to security or defense of Pakistan using social/ electronic media or information system
	Invitation or motivation of funding, recruiting for terrorism or plans for terrorism	Unauthorized interception of data and information	Intent to commit fraud by alteration, deletion or suppression of data of deceased person	Distribution of child pornographic material	Kidnapping using electronic/ social media or information/ communication system	Threat to public order maintenance, decency or morality using information system
	Money Laundering	Intention to corrupt, destroy or alter information system or data using malicious code	Using unauthentic data for legal purpose knowing its illegal	Illegal production, availability or transmission of child pornographic data using information system	Sending harmful, misleading or lottery schemes SMS/ messages	Public incitement against government using media or information system

Figure-5.8: Categories of Cyber Crimes in Pakistan

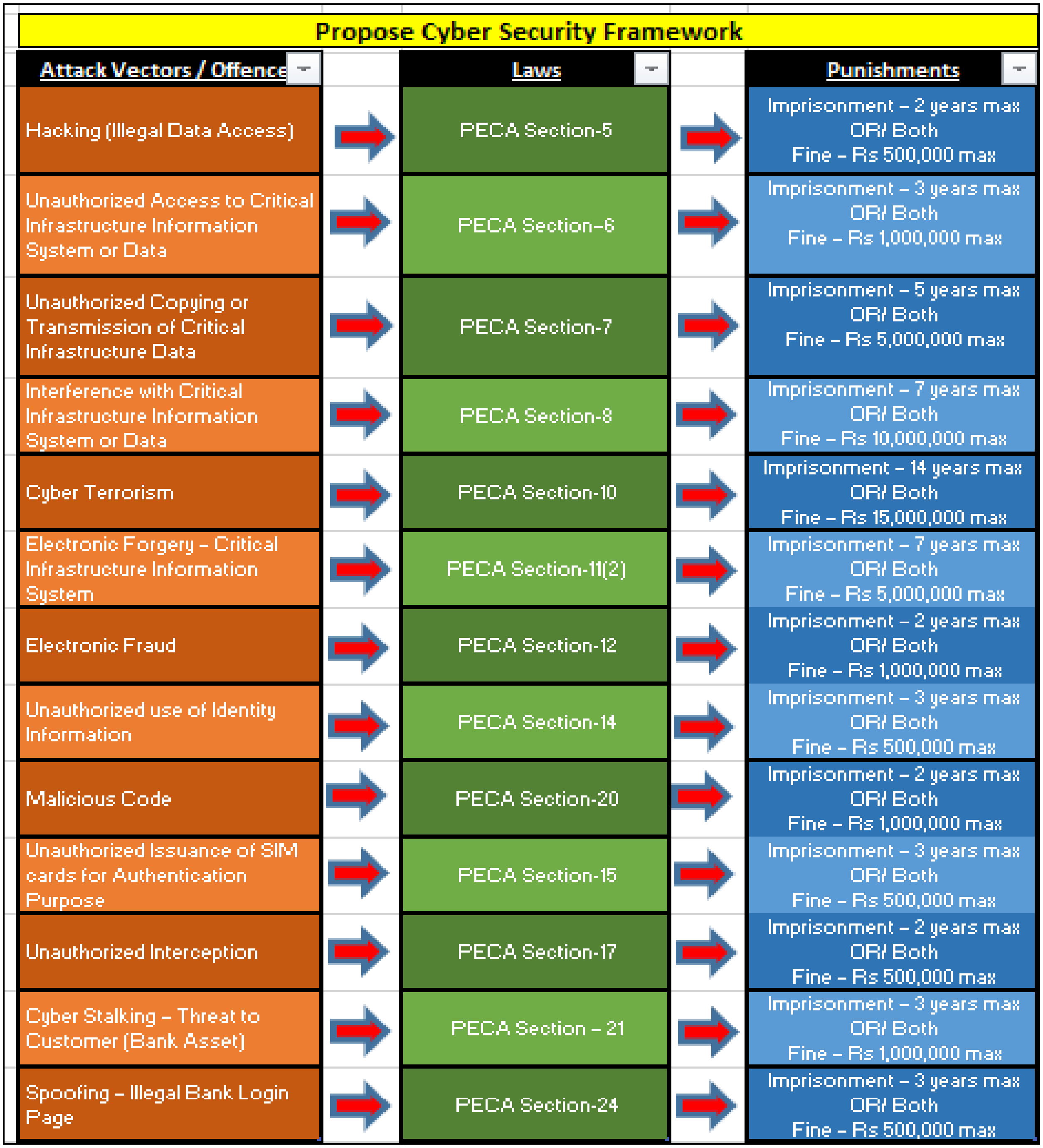


Proposed Cyber Security Framework

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Cyber Crime Laws and Regulations (RS.CC):** Identification of national laws and regulations dealing with cyber crimes.	**RS.CC-1:** Cyber Terrorism	**PECA Sec** - 9, 10, 10A, 10B **PPC Sec** - 154A, 276
		RS.CC-2: Unauthorized Data/ Information Access	**PECA Sec** - 3, 4, 5, 6, 7, 8, 17, 20
		RS.CC-3: Electronic Forgery	**PECA Sec** - 11, 12, 13, 14, 15, 16 **PPC Sec** - 294A, 403, 404, 415, 463
		RS.CC-4: Hurting Modesty of a Person/ Minor	**PECA Sec** - 18, 19, 19A **PPC Sec** - 293, 366A, 371A, 371B, 499
		RS.CC-5: Personal Harrassment/ Threat	**PECA Sec** - 21, 22, 23, 38 **PPC Sec** - 409, 503, 507, 509
		RS.CC-6: Unlawful Online Content	**PECA Sec** - 34 **PPC Sec** - 295A, 295B, 295C, 298, 298A, 486, 489A

Figure-5.9: Categories of Cyber Crimes and Informative References in Proposed Cyber Security Framework

In our banking sector case scenario, cybercrimes are classified as offences, and following identification and conviction under a specific portion of national cyber legislation, punishments have been specified to reduce such offences in the future.



Propose Cyber Security Framework

Attack Vectors / Offence	Laws	Punishments
Hacking (Illegal Data Access)	PECA Section-5	Imprisonment – 2 years max OR/ Both Fine – Rs 500,000 max
Unauthorized Access to Critical Infrastructure Information System or Data	PECA Section-6	Imprisonment – 3 years max OR/ Both Fine – Rs 1,000,000 max
Unauthorized Copying or Transmission of Critical Infrastructure Data	PECA Section-7	Imprisonment – 5 years max OR/ Both Fine – Rs 5,000,000 max
Interference with Critical Infrastructure Information System or Data	PECA Section-8	Imprisonment – 7 years max OR/ Both Fine – Rs 10,000,000 max
Cyber Terrorism	PECA Section-10	Imprisonment – 14 years max OR/ Both Fine – Rs 15,000,000 max
Electronic Forgery – Critical Infrastructure Information System	PECA Section-11(2)	Imprisonment – 7 years max OR/ Both Fine – Rs 5,000,000 max
Electronic Fraud	PECA Section-12	Imprisonment – 2 years max OR/ Both Fine – Rs 1,000,000 max
Unauthorized use of Identity Information	PECA Section-14	Imprisonment – 3 years max OR/ Both Fine – Rs 500,000 max
Malicious Code	PECA Section-20	Imprisonment – 2 years max OR/ Both Fine – Rs 1,000,000 max
Unauthorized Issuance of SIM cards for Authentication Purpose	PECA Section-15	Imprisonment – 3 years max OR/ Both Fine – Rs 500,000 max
Unauthorized Interception	PECA Section-17	Imprisonment – 2 years max OR/ Both Fine – Rs 500,000 max
Cyber Stalking – Threat to Customer (Bank Asset)	PECA Section – 21	Imprisonment – 3 years max OR/ Both Fine – Rs 1,000,000 max
Spoofing – Illegal Bank Login Page	PECA Section-24	Imprisonment – 3 years max OR/ Both Fine – Rs 500,000 max

Figure-5.10: National Cyber Laws dealing with Cyber Crimes

National cyber laws integrated in the proposed cyber security framework that deals with cyber-crime attack vectors in a financial system [62] have been emphasized. Attack vectors that are deemed cybercrimes are defined in the legislation, and corresponding sanctions are also listed in order to convict such cybercrimes. The following table lists the attack vectors/offenders and sections of cyber laws that deal with those attack vectors under the proposed framework.

ID	**Attack Vectors / Offences**	**Laws**	**Punishments**
T-1	Hacking (Illegal Data Access)	PECA Section – 5	Imprisonment – 2 years max OR/ Both Fine – Rs 500,000 max
T-2	Unauthorized Access to Critical Infrastructure Information System or Data	PECA Section – 6	Imprisonment – 3 years max OR/ Both Fine – Rs 1,000,000 max
T-3	Unauthorized Copying or Transmission of Critical Infrastructure Data	PECA Section – 7	Imprisonment – 5 years max OR/ Both Fine – Rs 5,000,000 max
T-4	Interference with Critical Infrastructure Information System or Data	PECA Section – 8	Imprisonment – 7 years max OR/ Both Fine – Rs 10,000,000 max
T-5	Cyber Terrorism	PECA Section – 10	Imprisonment – 14 years max OR/ Both Fine – Rs 15,000,000 max
T-6	Electronic Forgery – Critical Infrastructure Information System	PECA Section – 11(2)	Imprisonment – 7 years max OR/ Both Fine – Rs 5,000,000 max
T-7	Electronic Fraud	PECA Section – 12	Imprisonment – 2 years max OR/ Both

			Fine – Rs 1,000,000 max
T-8	Unauthorized use of Identity Information	PECA Section – 14	Imprisonment – 3 years max OR/ Both Fine – Rs 500,000 max
T-9	Malicious Code	PECA Section – 20	Imprisonment – 2 years max OR/ Both Fine – Rs 1,000,000 max
T-10	Unauthorized Issuance of SIM cards for Authentication Purpose	PECA Section – 15	Imprisonment – 3 years max OR/ Both Fine – Rs 500,000 max
T-11	Unauthorized Interception	PECA Section – 17	Imprisonment – 2 years max OR/ Both Fine – Rs 500,000 max
T-12	Cyber Stalking – Threat to Customer (Bank Asset)	PECA Section – 21	Imprisonment – 3 years max OR/ Both Fine – Rs 1,000,000 max
T-13	Spoofing – Illegal Bank Login Page	PECA Section – 24	Imprisonment – 3 years max OR/ Both Fine – Rs 500,000 max

Table-5.1: Cyber Crimes addressed by National Cyber Laws

This case study will assist governmental and commercial businesses, particularly financial institutions, that are directly threatened by cyber-criminals and cyber-attackers in convicting any such threat agent under the cover of national cyber laws and regulations.

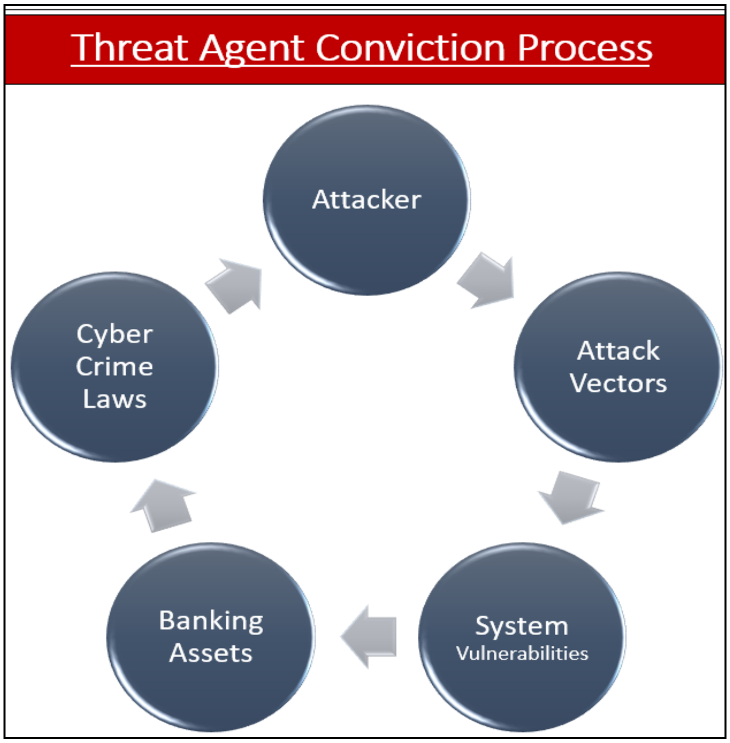


Figure-5.11: Attack Process and Conviction through Cyber Laws

An attacker who follows attack protocols can be prosecuted under national cybercrime legislation. With the aid of national cyber legislation, the proposed framework has expedited the process of prosecuting a cybercriminal. This conviction procedure might lead to a reduction in cybercrime on a nationwide scale.

Chapter - 6

Conclusion and Future Work

6.1 Conclusion

Because of advancements in information technology, cyber risks will continue to emerge, necessitating the need for our national cyber strategy and corresponding legislation to combat new cybercrimes sooner or later. It is high time to create a long-term national cyber security framework for dealing with cyber threats and cybercrime by combining national cyber legislation in order to further improve the global landscape of national cyber security and cyber defense. Further refining and incorporation of new cyber laws as useful references in this framework will save time, labor, and resources during the investigation and conviction process. The use of this suggested framework by investigators or associated organizations can assist them in dealing with cybercrime cases in a timely and productive manner, therefore increasing the efficiency of national cybercrime control centers.

6.2 Future Work

The following are the open areas for further research in the proposed cyber security framework:

- Improving national cybercrime legislation and including them as an instructive reference in the proposed framework.
- Incorporation of cybercrime identification techniques.
- Integration of cybercrime protection techniques.
- Combination of data recovery approaches for cybercrime-related data losses.

- Amalgamation of cybercrime detection techniques in the proposed framework.

References :

[1] "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress", EveryCRSReport, December 2014, Available: https://www.everycrsreport.com/reports/R42984.html

[2] "National Institute of Standards and Technology, Cybersecurity Framework", NIST Framework version 1.1, February 2014, Available at: https://www.nist.gov/cyberframework

[3] "World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks", FireEye Report, August 2014, Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf

[4] Syed Rubab, Khaver Ahmed & Muhammad Yasin, "Cyber Security: Where Does Pakistan Stand?", Sustainable Development Policy Institute, February 2019, https://think-asia.org/handle/11540/9714

[5] Prevention of Electronic Crimes Act – 2016, Available at: http://www.na.gov.pk/uploads/documents/1462252100_756.pdf

[6] The News, 18 August 2020, Available at: https://www.thenews.com.pk/print/702208-na-panel-takes-up-proposal-to-set-up-national-cybercrime-centre

[7] "What is Cybersecurity?", National Centre for Cyber Security", https://www.nccs.pk/nccs/what-is-cyber-security

[8] "SECP Guidelines on Cybersecurity Framework", The Nation, 18 March 2020, Available at: https://nation.com.pk/18-Mar-2020/secp-issues-guidelines-on-cybersecurity-framework-for-insurance-sector

[9] Basma Khalil, "Cybercrime effecting banking sector/ economy of Pakistan", ModernDiplomacy, 22 March 2020, https://moderndiplomacy.eu/2020/03/22/cybercrime-effecting-banking-sector-economy-of-pakistan/

[10] "The Pentagon's Secret Plans to Secure Pakistan's Nuclear Arsenal", National Threat Initiative, 9 November 2011, Available at: https://www.nti.org/gsn/article/the-pentagons-secret-plans-to-secure-pakistans-nuclear-arsenal/

[11] Muhammad Abdul Qadir, "The Cyber Threat Facing Pakistan", The Diplomat, 6 June 2020, Available at: https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/

[12] Yusuf Huaasin, "Why Cybersecurity is Critical to our Future", Hilal Magazine, Available at: https://www.hilal.gov.pk/eng-article/why-cybersecurity-is-critical-to-our-future/MjMwMw==.html

[13] "The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress", EveryCRSReport, December 2014, Available: https://www.everycrsreport.com/reports/R42984.html

[14] “National Institute of Standards and Technology, Cybersecurity Framework”, NIST Framework version 1.1, February 2014, Available at: https://www.nist.gov/cyberframework

[15] “Malaysian Cyber Security Framework for Public Sector”, Government of Malaysia, Available at:
https://www.malaysia.gov.my/portal/content/30090

[16] “Malaysia National Cyber Security Policy”, Government of Malaysia, Available at:
https://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/hashim-cybersecurity-malaysia-june-09.pdf

[17] Jack Wagner, “China’s Cybersecurity Law: What you need to know”, The Diplomat, June 2017, Available at:
https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

[18] China Cybersecurity and Data Protection: Review of 2020 and outlook of 2021”, Herbert Smith Freehills, January 2021, Available at: https://www.lexology.com/library/detail.aspx?g=44eee916-38fc-4132-8924-44377262ab4d

[19] “Cyber Wellness Profile Russian Federation”, April 2016, Available at:
http://www.bdo3c.fsc.org/fichiers%20LMSCHERRER%20FSC%20uniquement_transfere_serveur_crownmakers_le_09juillet/2477.pdf

[20] “The Saudi Cybersecurity Workforce Framework”, June 2020, Available at:
https://nca.gov.sa/files/scywf_en.pdf

[21] “Saudi National Cyber Strategy”, June 2020, Available at: https://nca.gov.sa/en/pages/strategic.html

[22] “Saudi Anti-Cyber Crime Law”, March 2007, Available at: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf

[23] “Prevention of Electronic Crimes Act – 2016”, <*Accessed 15 January 2021*> http://www.na.gov.pk/uploads/documents/1462252100_756.pdf

[24] “Prevention of Electronic Crimes Ordnance – 2007”, Government of Pakistan, Available at: http://www.pakistanlaw.com/electronic_prevention_ord.pdf

[25] “Electronic Fund Transfers Act – 2007”, Government of Pakistan, Available at: http://www.documents.pk/file/State%20Bank%20of%20Pakistan%20(SBP)%20-%20Payment%20Systems%20and%20Electronic%20Fund%20Transfer%20Act,%202007.pdf

[26] “Electronic Transactions Ordnance – 2002”, Government of Pakistan, Available at: http://www.pakistanlaw.com/eto.pdf

[27] “Pakistan Penal Code”, Government of Pakistan, Available at: http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html

[28] “The Removal and Blocking of Unlawful Online Content, Rules 2020”, Published by Government of Pakistan, 20 October 2020, Available at: https://moitt.gov.pk/SiteImage/Misc/files/Social%20Media%20Rules.pdf

[29] “National Institute of Standards and Technology, Cybersecurity Framework”, NIST Framework version 1.1, February 2014, Available at: https://www.nist.gov/cyberframework

[30] “Malaysian Cyber Security Framework for Public Sector”, Government of Malaysia, Available at:
https://www.malaysia.gov.my/portal/content/30090

[31] Jack Wagner, “China’s Cybersecurity Law: What you need to know”, The Diplomat, June 2017, Available at:
https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

[32] “Cyber Wellness Profile Russian Federation”, April 2016, Available at:
http://www.bdo3c.fsc.org/fichiers%20LMSCHERRER%20FSC%20uniquement_transfere_serveur_crownmakers_le_09juillet/2477.pdf

[33] “The Saudi Cybersecurity Workforce Framework”, June 2020, Available at:
https://nca.gov.sa/files/scywf_en.pdf

[34] “Prevention of Electronic Crimes Act – 2016”, <*Accessed 15 January 2021*>
http://www.na.gov.pk/uploads/documents/1462252100_756.pdf

[35] “Prevention of Electronic Crimes Ordnance – 2007”, Government of Pakistan, Available at:
http://www.pakistanlaw.com/electronic_prevention_ord.pdf

[36] “Electronic Fund Transfers Act – 2007”, Government of Pakistan, Available at:

http://www.documents.pk/file/State%20Bank%20of%20Pakistan%20(SBP)%20-%20Payment%20Systems%20and%20Electronic%20Fund%20Transfer%20Act,%202007.pdf

[37] "Electronic Transactions Ordnance – 2002", Government of Pakistan, Available at: http://www.pakistanlaw.com/eto.pdf

[38] "The Removal and Blocking of Unlawful Online Content, Rules 2020", Published by Government of Pakistan, 20 October 2020, Available at: https://moitt.gov.pk/SiteImage/Misc/files/Social%20Media%20Rules.pdf

[39] "Pakistan Penal Code", Government of Pakistan, Available at: http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html

[40] "Cyber-Crime rate increase in Pakistan", Pakistan Today, 21 February 2021 https://www.pakistantoday.com.pk/2021/02/14/cybercrime-rate-increased-more-than-five-times-in-2020/

[42] "Country witness massive jump in cybercrime cases", The News, 6 May 2021, https://www.thenews.com.pk/print/831322-country-witnesses-massive-jump-in-cybercrime-cases

[43] "Framework for Improving Critical Infrastructure Cybersecurity", Version 1.1, National Institute of Standards and Technology, Apr 2018, Available at: https://www.nist.gov/cyberframework

[44] Kenny Mesker, "Adapting NIST Cybersecurity Framework for Risk Assessment", NIST Conference, Oct 2014, Available at:

https://www.nist.gov/system/files/documents/cyberframework/cybersecurityframework_6thworkshop_chevron.pdf

[45] “An Introduction to Components of the Framework”, Version 1.1, National Institute of Standards and Technology, Apr 2018, Available at: https://www.nist.gov/cyberframework/online-learning/components- framework

[46] Zia Ul Islam, M. Aqeel Khan & Muhammad Zubair, “Cyber Crime and Pakistan”, Global Political Review, Vol-IV No.II (Spring 2019) https://www.gprjournal.com/jadmin/Auther/31rvIolA2LALJouq9hkR/7EFv9UDoIP.pdf

[47] “Prevention of Electronic Crimes Act – 2016”, <*Accessed 15 January 2021*> http://www.na.gov.pk/uploads/documents/1462252100_756.pdf

[48] “Pakistan Penal Code (Act of 1860)”, <*Accessed 15 January 2021*> http://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html

[49] “Electronic Transactions Ordnance ETO – 2002”, <*Accessed 15 January 2021*> http://www.pakistanlaw.com/eto.pdf

[50] “NIST Cyber Security Framework”, National Institute of Standards and Technology, Available at: https://www.nist.gov/cyberframework

[51] Murugiah Souppaya and Karen Scarfone, “Guide to Data-Centric System Threat Modeling”, NIST SP 800-154, Apr 2016, https://csrc.nist.gov/publications/detail/sp/800-154/draft

[52] Prevention of Electronic Crimes Act (PECA) – 2016, Available at: http://www.na.gov.pk/uploads/documents/1462252100_756.pdf

[53] "Personal Data Protection Bill 2020", Ministry of Information Technology and Telecommunication, Government of Pakistan, Available at: https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill %202020%20Updated.pdf

[54] Salim Hasham, Shoan Joshi and Daniel Mikkelsen, "Financial Crime and Fraud in the Age of Cybersecurity", McKinsey & Company, Oct 2019

[55] Joanne Kumire, "How are banks dealing with a rise in cyber attacks?", Jan 2020, Available at: https://11fs.com/article/how-are-banks-dealing-with-a-rise-in-cyber-attacks

[56] "Online Banking Security Risks and Threats Modeling", Diceus Business Forum, Nov 2019, Available at: https://diceus.com/risk-threat-models-banking/

[57] Adrian Nish, Saher Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System", Carnegie Endowment for International Peace, Mar 2019, https://carnegieendowment.org/2019/03/25/cyber-threat-landscape-confronting-challenges-to-financial-system-pub-78506

[58] Nida Tariq, "Impact of Cyberattacks on Financial Institutions", Journal of Internet Banking and Commerce, Jan 2019

[59] Richard Home, "The Cyber Threat to Banking, A global industry challenge", Cyber Report-2014, Available at: https://www.bba.org.uk/wp-content/uploads/2014/06/ BBAJ2110_Cyber_report_May_2014_WEB.pdf

[60] Prem Khatri, "Importance of Cyber Security in Today's Banking Environment", The Global Treasurer, Sep 2019, Available at:

https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/

[61] Propose Cyber Security Framework and List of Cyber Crimes in Pakistan, https://drive.google.com/file/d/1GiQ2mMOv9x-fnQbmONZZAUgvqt6o9aDJ/view?usp=sharing

[62] “How the Banking Sector can Combat Cyber-Attacks”, A scholarly article by Byte Academy, Aug 2020, https://www.byteacademy.co/blog/banking-cyber-security