Mairaj
Vol 2, Issue 1
https://www.mairaj.pk editor.mairaj@gmail.com
ISSN Online 2959-2089 ISSN Print 2959-2070

Muhammad Umar Farooq Baloch
Research Scholar, National Defence University, Islamabad

Cyber Security Governance; Implications For Pakistan's National Security

Abstract

Networks for information and communication technologies form the backbone of the global cyberspace. These networks operate across physical borders and hold vital data and information that is essential to the national security of any nation. In the modern digital sphere, these networks are frequently vulnerable to cyber threats and attacks. One of the most important security concerns in the modern world is cyber warfare, which is a term coined to describe this conundrum. In response, the nations are making significant investments to fortify the security of their cyber frontiers and to assemble a formidable cyber force to defend their cyberspace. Similarly, Pakistan's national security is under grave threat from the ongoing cyberwarfare. This article seeks to elucidate Pakistan's current cyber challenges as well as the steps that country should take to counteract sophisticated cyber security threats. In order to protect Pakistan's national security, this article will also highlight the creation of a framework and governance mechanism for cyber security along with suggested courses of action that are in line with the country's cyber policy.

Introduction

In the past ten years, information and communication technologies, or ICTs, have been instrumental in transforming the world and turning it into a true global village. The world's socioeconomic development is being redefined by ICT innovation, which is giving users of cyberspace new commercial, economic, cultural, and social opportunities. A new era characterized by simple and affordable access to globally interconnected networks has been brought about by this unparalleled growth. Because of advancements in ICTs and our increased reliance on broadband infrastructure, the Internet has become indispensable in today's modern society.[1]

People today have unparalleled access to information and knowledge due to the world's increasing interconnectedness. Pakistan has also chosen the route of digital transformation in order to capitalize on the advantages of ICTs and the Fourth Industrial Revolution (4IR). The growing use of ICTs has improved digital services global connectivity, mobility, and versatility. However, it has also exposed information assets to a variety of new and developing Cyber Security threats. These assets have become extremely valuable due to the Fourth Industrial Revolution, nevertheless as the Internet has naturally expanded and grown, some concerning patterns in the usage of cyberspace have also surfaced.[2]

Significance of Study

As the world is increasingly connected day by day through digital and IT platforms, the cyber security is under huge threats. The threats are evolving globally while captivating the entire world under its effects. The states and individuals possessing critical information and their IT based infrastructure, both are under the peril of Cyber threat. Pakistan is a country with colossal base of internet users. The systems are becoming digitalized in significant institutions of the country. Therefore, the cyber risk is increasing with the digitalization of the world. As the threat unfold, it is important to assess the risk and enhance the governance system to tackle the issue. Therefore, this study would assess the cyber security system of Pakistan, the gaps and risk and implications of governance system to protect the state against likely cyber threats and attacks.

Pakistan falls in the run-down of developing states as far as the promise to cyber security while considering the gravity of the threats and the security at stake, it is imperative that a comprehensive use of information technology solutions are to be inculcated. In order to address the previously mentioned peculiarities, Pakistan needs an incorporated institutional structure which interconnects the frameworks and administrations of pertinent offices and makes coordination and participation among them to ensure the national security of a country. At long last, Pakistan ought to embrace the pursuit of ‘techni-fication’ regarding its cyber security realm.

The creation of effective mechanisms, the implementation of security standards and regulations within legislative and legal contexts, and the establishment of a cyber-governance framework that is in line with the national cyber vision can all be done to strengthen national cyber security capabilities and reduce cyber threats and the outlook for cyber security.

Pakistan’s Cyber Landscape

The story of Pakistan's cyber revolution is one of unparalleled transformation. ICTs have grown rapidly in Pakistan over the past ten years, and this has had a revolutionary effect on society. Pakistan had the third-fastest growing information technology market in the world in 2008. Overseas and inland investments in fixed-line and mobile networks were contributing significantly to the significant improvement of Pakistan's telecommunications infrastructure. Nationwide, fiber systems are being built to support network expansion.

However, in order to protect Pakistani citizen’s online safety and guarantee the security of digital systems, a number of federal, provincial, and sectoral regulators have already put in place a number of initiatives. These include the Electronic Transaction Ordinance, 2002 (which only covers electronic financial transactions and records), the Investigation for Fair Trial Act (IFTA) of 2013, the Pakistan Telecommunication (Re-Organization) Act of 1996, and the Prevention of Electronic Crime Act (PECA) of 2016, which address some but not all aspects of information and cyber security. Furthermore, the PTA has notified the Telecom Computer Emergency Response Team (CERT), and the State Bank of Pakistan (SBP) has released guidelines on cyber security for the financial industry.

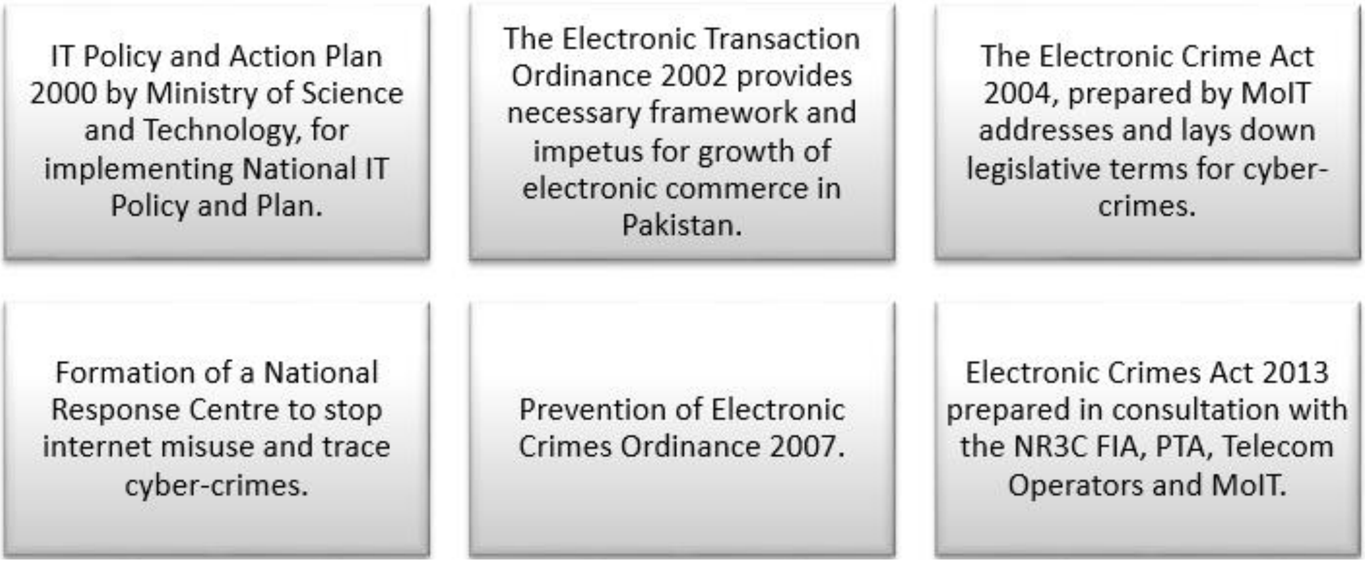
Nonetheless, a particular focus at the national level is necessary for the interdepartmental coordination and comprehensive approach to address the cyber security challenges and their emerging trends. This section attempts to analyze Pakistan's current cyber landscape by looking at the initiatives and governance structures that are in place as well as the current weaknesses in our cyber systems.

Existing Governance Processes/Parameters

1. **Ministry of Information and Technology (MoIT)**: The Federal MoIT is in charge of developing the infrastructure, rules, and legal framework for ICTs, as well as designing and implementing IT and telecom initiatives throughout Pakistan. In order to assess online content and requests for website blocking, the MoIT established the Inter-Ministerial Committee for the Evaluation of Websites (IMCEW) in 2006. The committee's recommendations for the issuance of filtering and blocking orders are then forwarded to the ministry. The MoIT Secretary is in charge of the committee, which is made up of representatives from the cabinet, interior, information and broadcasting, and security agencies. Generally, the MoIT and the PTA receive directives to block content from the government or the Supreme Court through the IMCEW, and then forward those orders to specific Internet service providers (ISPs).
2. **Federal Investigation Agency (FIA)**: The Federal Bureau of Investigations (FIA) is an independent federal agency that was founded in 1974 and is responsible for conducting investigations and carrying out operations against copyright infringement, federal crimes, terrorism, and smuggling. The National Response Centre for Cyber Crimes (NRC3) was founded by the Federal Bureau of Investigations (FIA) and has been operational in Pakistan since 2002. However, the Agency did not have greater legislative authority to investigate, prosecute, and regulate electronic crime until the Prevention of Electronic Crimes Ordinance (PECO) was passed. Enforcing cyber laws and addressing financial crimes such as email threats, plastic money fraud, and Internet fraud was the primary goal of NRC3.
3. **Pakistan Telecommunication Authority (PTA)**: The PTA is the primary licensing and regulatory authority for Pakistan's internet and telecommunications sector. It was founded in January 1997 in accordance with the Telecom Reorganization Act of 1996. It also serves to recommend policies and encourage the expansion of telecommunication and internet services. PTA is effectively a government body because the MoIT is the organization's reporting partner and the Federal Government appoints the organization's chairman and members. Under the guidance of the government, the Supreme Court, and the MoIT, the authority regulates online activities in close collaboration with PTCL and the FIA.
4. **Framework for Regulating Cyber Activities in Pakistan**

There are various frameworks that facilitated inclusion of Pakistan in the cyber domain are as under: -

Cyber Security Initiatives in Pakistan



IT Policy and Action Plan 2000 by Ministry of Science and Technology, for implementing National IT Policy and Plan.

The Electronic Transaction Ordinance 2002 provides necessary framework and impetus for growth of electronic commerce in Pakistan.

The Electronic Crime Act 2004, prepared by MoIT addresses and lays down legislative terms for cyber-crimes.

Formation of a National Response Centre to stop internet misuse and trace cyber-crimes.

Prevention of Electronic Crimes Ordinance 2007.

Electronic Crimes Act 2013 prepared in consultation with the NR3C FIA, PTA, Telecom Operators and MoIT.

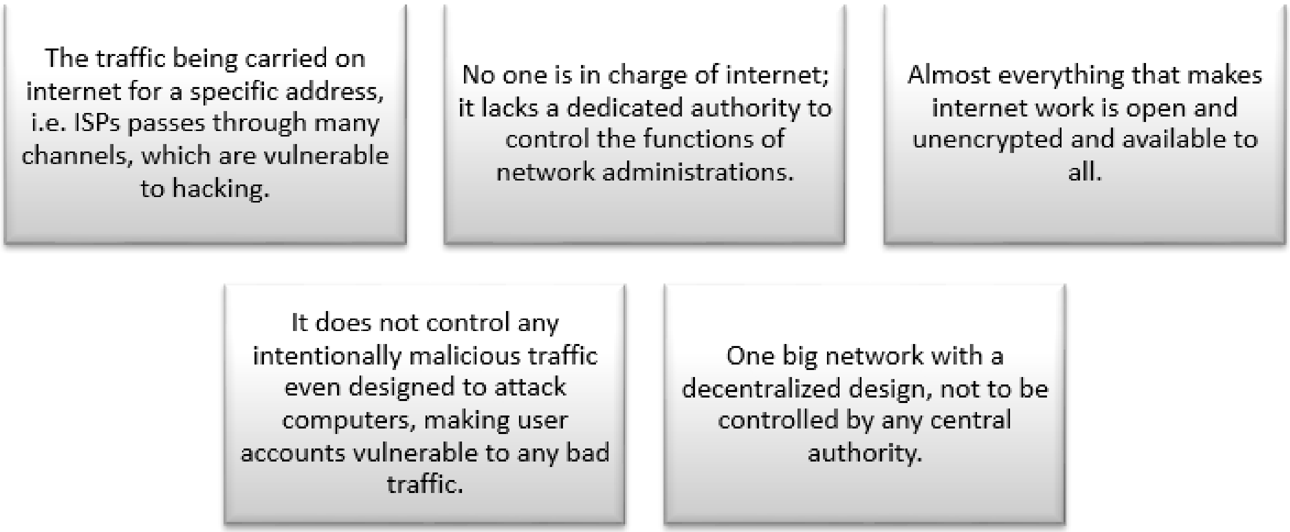
While various ministries and organizations including the Armed Forces are working on Cyber Warfare. The following initiatives highlight the current state of cyber threat and crime mitigation at the national level:-

1. **Prevention of Electronic Crime Act-2009**: Pakistan passed the Prevention of Electronic Crime Act in 2009 to criminalize malicious computer activities. Two entities were established to carry out the legislation. The Federal Investigation Agency's (FIA) National Response Centre for Cybercrimes is in charge of stopping and looking into cybercrimes, protecting information resources, and informing departments and owners of critical infrastructure about cyber threats. The government receives advice from the National Telecommunications and Information Technology Security Board (NTISB), which also supervises IT equipment purchases. [3]
2. **Cyber Security Manual for Journalists-2013**: In collaboration with the Pakistan Information Security Association (PISA), the Senate’s Committee on Defence launched the first-ever Cyber Security seminar on July 8, 2013, to begin work on the topic. As a result, the Senate Defence Committee created training manual to inform both laypeople and media professionals about their online and digital device vulnerabilities and to provide them with the tools to create their own security protocols to counteract evolving threats. [4]
3. **Cyber Security Council Bill-2015:** Pakistan's first cyber Security Council Bill - 2015 was introduced in the Senate by Senator Mushahid Hussain Syed. The bill proposed a National Cyber Security Council and outlines the council's responsibilities, including creating policy guidelines and governance models in response to new and evolving cyber security threats. The Bill also grants the Council the authority and responsibility to create strategic plans. In addition to developing a 10-year and 20-year vision, it places a strong emphasis on facilitating communications between government and private sector entities, academia, civil society, and cyber security experts.[5]
4. **Prevention of Electronic Crimes Bill 2015**: The Prevention of Electronics Crime Bill, 2015 was approved by the National Assembly Standing Committee on Information Technology on April 16, 2015. The Ministry of IT claims that the law guards against hackers accessing vital government infrastructure and addresses hate speech and terrorist activity on the internet.
5. **National Cyber Security Policy 2021:** The National Cyber Security Policy of Pakistan, which was first released as a consultation draft in January 2021, has undergone substantial improvements. The approved version of the policy, which was unveiled in July 2021, presents a more expansive vision than the previous consultation draft. It emphasizes resilience establishment through a strong and ever-improving digital ecosystem, rather than just asset security. The goal is to promote cyber security while highlighting and completing initiatives to enhance the socioeconomic development of society as a whole. [6]

Shortfalls in Pakistan’s Cyber System

Pakistan’s cyber/computer systems are mainly vulnerable due to the following deficiencies:-

1. **Lack of Implementation of National Cyber Security Policy 2021**: Pakistan is faced with multifaceted cyber threats in the absence of cyber security laws or policies, especially from a neighbouring hostile state that wants to control this domain regionally in particular and globally in general. Thus, developing a cyber-security culture and awareness as well as securing our computer and electronic systems calls for a focused and well-coordinated national policy on cyber security in order to prevent such cyber-crimes and cyber terrorism like activities.
2. **Lack of Committed National Cyber Authority**: The National Cyber Security Council was founded to create and draft governance models and policy guidelines pertaining to the threats to cyber security that the public and private sectors face. Cyber security is also under the purview of the Cabinet Division, which oversees another national organization called NTISB. The Ministry of Interior (MoI) oversees the National Response Centre for Cybercrimes, which is a division of FIA. The Ministry of Technology (MoIT) is in charge of IT advancement. These hierarchical organisations don't have a single, cohesive command structure or synchronization.
3. **Lack of Laws against Cyber Threats**: In addition to the lack of proper legislative frameworks, there is also a problem with the public's limited understanding and awareness of the laws. Although the first relevant law, "Pakistan's Cyber Crime Bill 2007," is in place and addresses electronic crimes such as cyberterrorism, illegal access, electronic system fraud, electronic forgery, and encryption misuse, its low implementation rates are evident from the statistics.
4. **Insufficient Cyber Security Awareness**: Cyber security awareness is low because even important government employees access the internet through unprotected commercial ISPs and national practitioners exchange information routed through US and UK servers.
5. **Internet Vulnerabilities:** Pakistan's cyber system is susceptible to the five major vulnerabilities found in the internet:



The traffic being carried on internet for a specific address, i.e. ISPs passes through many channels, which are vulnerable to hacking.

No one is in charge of internet; it lacks a dedicated authority to control the functions of network administrations.

Almost everything that makes internet work is open and unencrypted and available to all.

It does not control any intentionally malicious traffic even designed to attack computers, making user accounts vulnerable to any bad traffic.

One big network with a decentralized design, not to be controlled by any central authority.

6. **Sense of National Information systems:** The majority of modern communication and electronic systems produced by foreign firms are vulnerable to cyber-attacks and lack the technical muscle to counteract them. Other factors include the use of foreign low-grade security codes that are easily compromised and likely to have back door entry, a lack of an indigenous production base and reliance on foreign equipment and experts for modifications, poor computer system management, and inadequate security to prevent unauthorized access and intrusion.

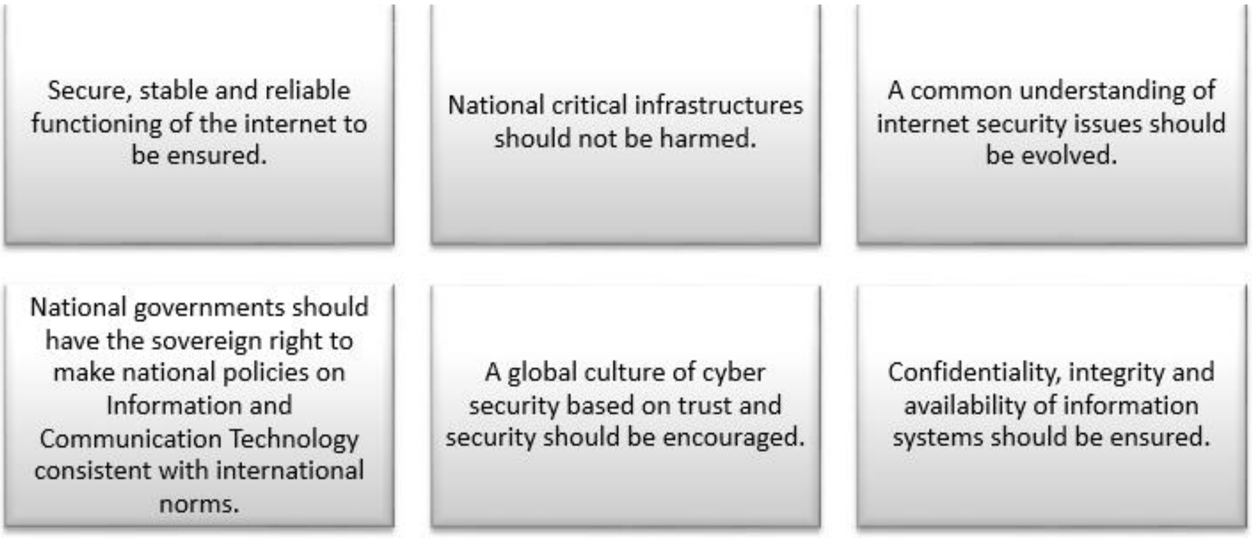
Recommended course of Action to Strengthen Cyber Security Governance in Pakistan

The confidentiality, availability, and integrity of data are increasingly important to us in the modern cyber world. In the absence of significant investments in the field of cyber security, data systems remain vulnerable to both dangerous and rudimentary forms of exploitation and attack. Our ability to combat new and emerging cyber threats will be greatly streamlined and improved by focussing on and making progress in the following areas.

1. **Convention on Cyber Warfare**: Pakistan needs to follow an aggressive approach to engage the global community through meaningful international legal instruments to counter cyber warfare threats. Several

international conventions (chemical weapons convention, biological toxins and weapons convention, NPT etc) and a body of international humanitarian law (Geneva and Hague conventions) exist, which are equally applicable to cyber domain. A cyber warfare convention can be promulgated in the light of existing international legal structures.

The following should be the main points of discussion for any potential cyberspace convention:



Secure, stable and reliable functioning of the internet to be ensured.

National critical infrastructures should not be harmed.

A common understanding of internet security issues should be evolved.

National governments should have the sovereign right to make national policies on Information and Communication Technology consistent with international norms.

A global culture of cyber security based on trust and security should be encouraged.

Confidentiality, integrity and availability of information systems should be ensured.

2. **Internet Access from sensitive routes:** The heightened concerns over cyber security, national security, and data privacy have led to an increased scrutiny of internet access from sensitive routes, such as those in conflict zones or critical infrastructure areas. The risk of unapproved data interception, cyber espionage, and the possible interruption of essential services has increased as the world's connectivity has grown.
3. **National Level Measures:** There are some important measure required at national level, stated as below;

a. **National Information Security Policy**: Pakistan does not have a national information security policy that is founded on uniform guidelines for the whole nation. In consultation with the corporate sector, the Information Technology Division, and military authorities, the government must develop a comprehensive National Information Security standard.

b. **Establishment of Lead Cyber Security Organization**: The MoIT should establish a National Information/Cyber Security Division, tasked with overseeing governance models and policy guidelines pertaining to information and cyber security threats faced by both the public and private sectors. There ought to be representatives from the public, commercial, and military sectors in this division.

c. **Comprehensive Legislation to Combat Cyber Crime**: It is necessary to implement comprehensive legislation to combat cybercrime and cyber terrorism. Any future information technology policy must be strengthened with features that make it simple to implement across international borders and must be refined in a dynamic cyber environment. Several issues have been brought up by the government's draft cybercrime bill. Priority work must be given to this bill, and it needs to be amended before it can become law. In addition, when national security is in jeopardy, a clear procedure involving input from the private sector must be created for obtaining communications data.

d. **Isolation and Protection of all Critical Systems:** Government and military computers and networks ought to be equipped with a network intrusion detection system that keeps an eye on traffic and notifies authorities of any misuse or unusual activity.

e. **Cyber Warfare Capacity Building**: There are very few advanced studies, mostly theoretical, in the fields of cyber warfare and cyber security. By leveraging the widespread awareness of computers across the nation, new and targeted educational initiatives can be launched to develop the next wave of cyber warriors.

f. **Evaluation of System Software**: All system software must be made sure to carry out only the functions for which it was intended and must not include any intentionally added features that could lead to malfunctions after the system is put into use. When assessing the system software of combat equipment, the most recent viruses should be considered.

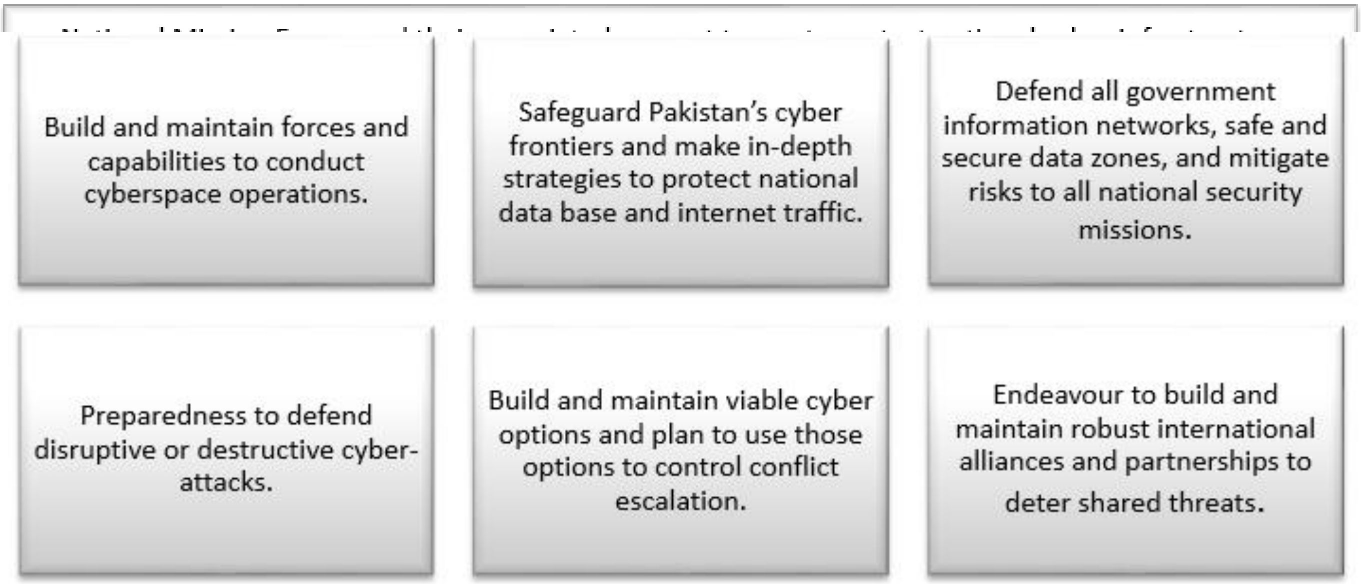
g. **Indigenous Production**: Efforts should be made to increase the basis of domestic production and development of computer hardware and software systems for offensive cyber capabilities.

h. **Formulation of Cyber Warfare Strategy**: Our critical systems susceptibility to cyber war raises the likelihood of instability, which can be lessened by developing a "Cyber Warfare Strategy." The following components should be included in the cyber warfare plan:-

- Prevention: Preventing enemies from obtaining, utilizing, or effectively employing cyber warfare tools and tactics against Pakistan.
- Deterrence: Must impede assaults and protect Pakistan's cyberspace from any foe attempting to undermine national interests.
- Protection: To lessen cyber domain vulnerabilities by strengthening potential targets against assault, thereby reducing the potential harm that such attacks can cause and enhancing the capacity for swift recovery.

The Development Strategy for Cyber Security Governance
Establishment of Cyber Force: The Cyber Force should be made up of cyber warriors arranged in the following hierarchy:

1. **Strategic Tasks of Cyber Force:** The strategic tasks of cyber forces Includes:



Build and maintain forces and capabilities to conduct cyberspace operations.

Safeguard Pakistan's cyber frontiers and make in-depth strategies to protect national data base and internet traffic.

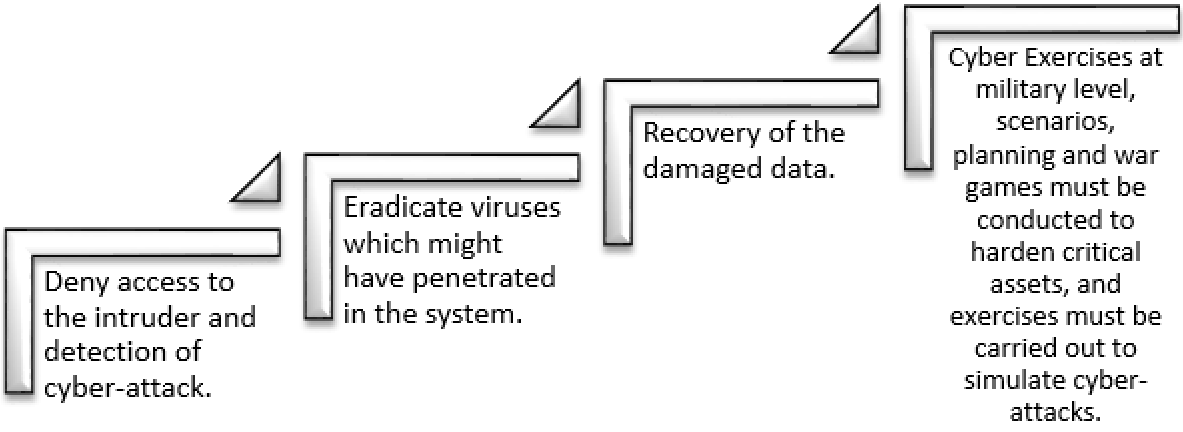
Defend all government information networks, safe and secure data zones, and mitigate risks to all national security missions.

Preparedness to defend disruptive or destructive cyber-attacks.

Build and maintain viable cyber options and plan to use those options to control conflict escalation.

Endeavour to build and maintain robust international alliances and partnerships to deter shared threats.

2. **Network Security:** To protect military communication systems, security precautions have been implemented. Nonetheless, hostile cyber agencies or internal sources may pose a threat to the nation's network and the armed forces. To ensure sufficient safeguard, the following can be the strategy:-

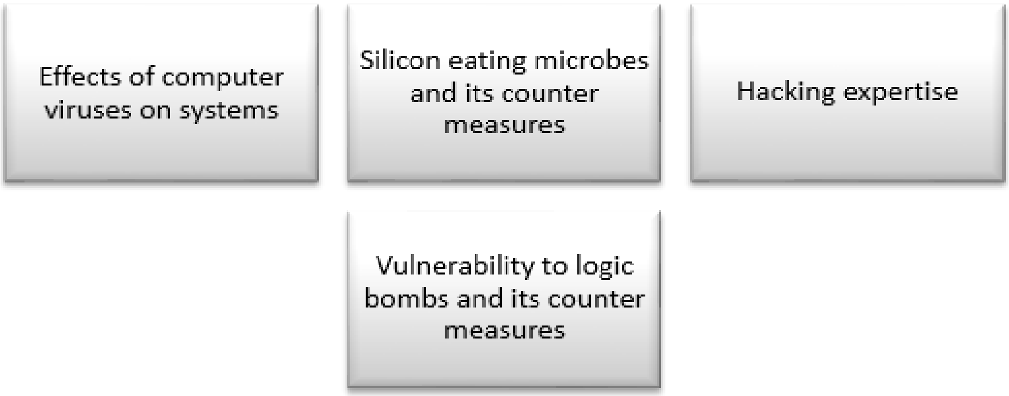


Deny access to the intruder and detection of cyber-attack.

Eradicate viruses which might have penetrated in the system.

Recovery of the damaged data.

Cyber Exercises at military level, scenarios, planning and war games must be conducted to harden critical assets, and exercises must be carried out to simulate cyber-attacks.


Effects of computer viruses on systems
Silicon eating microbes and its counter measures
Hacking expertise
Vulnerability to logic bombs and its counter measures

3. **Research and Development of Cyber Domain:** Research and development facilities must be established in order to conduct studies in the following areas:

Way Forward for Pakistan

The following recommendations are made at the national and international levels to counteract the threats found in the field of cyber warfare.

At International Level

One of the biggest security issues facing the world today is information and communications technology (ICT). Risk assessments indicate that the state or a group of companies could use ICT to destroy military coordination systems or the fundamental framework, thus causing fear and possibly causing a real and universal emergency. The emergence of asymmetric warfare, characterized by conflicts between states or groups possessing varying military capabilities, has led to a greater utilization of ICTs by the states. Consequently, there is a need to promote a digital lead code globally. Interstate cooperation is desperately needed to reduce the risks associated with cybercrime, basic cyber-attacks, electronic surreptitious work, mass information interventions, and proposed hostile actions that would use the Internet's power to expand control.

The emergence of digital risks has the potential to hasten the catastrophic financial and social harm, so efforts must be refocused globally to convey this new reality. To prevent conflicts between states, multinational organisations and regional partners like the UN, BRICS, SAARC, and many more can collaborate to address the problem of cyber-security. These organisations in particular can collaborate to create a system to halt the spread of cyber terrorism. A good example of such a cooperative mechanism is the EU Parliament's 2016 Directive on Network and Information Security Systems, which addressed cyber threats to critical and sensitive infrastructure and improved online services like e-commerce by strengthening safeguards against them. However, data systems against these digital infrastructures could have dire consequences and result in significant operational costs. [7]

At National level

The recommendations are separated into two categories at the national level: the Future Strategy Category and the Critical Category.

Critical Recommendations: This emphasizes the pressing actions needed to safeguard cyberspace, including:

- **Broad National cyber Security Policy:** Enacting a broad and comprehensive national cyber-security policy that lays out precise procedures for addressing cyber-security issues is a crucial first step for the government. The National Cyber Security policy must incorporate the cybercrime bill and its broaden scope. One possible model for developing a comprehensive policy is the National Cyber-security Policy of India, which was implemented in 2013. [8]
- **Establishment of National Cyber-Command:** The issue of cyber warfare, which is regarded as a component of fifth-generation warfare, requires the creation of a national cyber command. The USSTRATCOM serves as an excellent model for how Pakistan's National Cyber-Command, operating under the National Security Council, can be established to include all relevant leaders and develop offensive

and defensive cyber war capabilities. The FIA's present NR3C is limited to addressing small-scale cybercrime.

- **Regulation of Pakistan's Cyber-Space:** Pakistan's national security depends heavily on the regulation of the current cyberspace, since the PTA has failed to enforce state authority in this domain for example, by outlawing social media in the past due to blasphemy concerns. This can be accomplished by working with the IT industry and LEA to develop a comprehensive system that complies with ICAN standards for worldwide cyberspace regulation. Records pertaining to computer users and mobile subscribers should all be kept up to date. It should be illegal to use VPNs, untraceable IP addresses, and pirated software. [9]
- **Capacity Building:** To handle new developments in cybercrimes, Pakistan's Law Enforcement Agencies (LEA) should be better equipped. In light of the concerning state of cybercrime, law enforcement officers ought to possess the necessary training and tools to effectively tackle cybercrimes. Regarding terrorism, financial embezzlement, harassment, and many other cyberspaces, the forces ought to be split up into distinct operational zones.
- **Public Awareness Campaign: I**nternet users in Pakistan are susceptible to foreign propaganda because they can't even tell the difference between the advantages and disadvantages of using the internet. Every day, hundreds of people fall victim to online fraud. Campaigns for special promotion and advertising should be started for this reason in order to educate the public on how to keep themselves safe using the advice provided. It is important to organize seminars and workshops to increase the general public's knowledge of cyber law. One more way to raise awareness of the value of cyber-security is to plan a National Cyber-Security Awareness Day.

Future Recommendations: This emphasizes the actions needed to safeguard cyberspace going forward:

- **Regulation of Imported Computer Hardware:** Aside from smartphones, the majority of computer hardware, including CPUs, hard drives, network switches, routers, and many other pieces, enters the nation uninspected and is utilized by several significant institutions. It is not hard to insert viruses and factory-built codes into these devices. Hardware-level firmware malware subversion is the most dangerous and challenging to identify threat to critical infrastructures. Pakistan and the majority of the states rely on foreign vendors to provide computer systems like SCADA and ICS. Chaos may result from the production-phase malware that was incorporated into the system. One glaring example of this level is the European ban on Chinese cell phones due to claims that they contain hardware spying equipment. Therefore, before incoming hardware equipment enters public or government systems, it should be inspected by a different division of the PTA or FIA for viruses and spying software.
- **Incorporating Cyber-Warfare into Secondary & Higher Secondary Curriculum:** Cyber-security is not covered in Pakistani primary and secondary computer textbooks. Not even at the university level is the subject particularly covered. The university curriculum ought to be changed in this way to prevent our children from being dependent on imports.
- **Indigenous Development of Software:** Cyber-attacks are primarily caused by software. Since computer software is created in the same languages and on the same platforms, it is simple to learn its codes and strategies and use them to take advantage of the weaknesses in other platforms-developed systems, including Microsoft Windows, Java, Android, Linux, Unix, and many more. It is risky for significant institutions to rely on foreign software, particularly in uncontrolled cyberspace like Pakistan. Hackers are familiar with these operating systems, and they take advantage of zero-day vulnerabilities by using APT. Therefore, before being implemented, these operating systems must be customized. On the other hand, local operating system development will thwart any cyber-attack aimed at these objectives.
- **Narrative Building:** The state's encouragement of opportunities and scholarships to encourage students to conduct cyber-security research is part of the narrative building. Pakistan's higher education institutions publish very little written or researched content related to cyber-security and cyber warfare. Think tanks should be established in a similar manner to expand and broaden the research. As of right now, the National Centre for Cyber-Security (NCCS), a think tank devoted to cyber security, is the only one located at Air University Islamabad. This is concerning, and in order to increase the scope of cyber-security research, the government needs to take action and push other institutions to follow suit.

Conclusion

In conclusion, every technology has both positive and negative effects on society. How policymakers, governments, and social researchers respond to and mitigate the negative effects of new technologies on various societal segments is up to them. Similarly, information technology has brought the entire world within the reach of a single digital device. Cyber security has become a hot topic in recent years for reasons including international cooperation, human rights security, privacy, safety, harmony within the country, and peace. According to the research, the best way to combat the rising number of security lapses and cybercrimes is to prevent them. But until a suitable cyber security system, knowledge, expertise are created, it might not be possible to prevent the cyber frontiers. There is a need of time that citizens, media, politicians, and civil society organisations play a crucial role in the development of cyber security governance system.

Pakistan is among the countries that are often the subject of covert operations. Cybercriminals who operate methodically regularly target the important websites of the Pakistani government. The financial sector in Pakistan has recently struggled with the rise in cybercrime. Pakistan must recognise the grave threat to its IT infrastructure, and the government must act rapidly to ensure the security of the country's cyber borders. The government formally unveiled its national cyber security policy in July 2021, but it is crucial to start building the country's cyber security capabilities by creating necessary and well-coordinated mechanisms, putting security standards and laws into place under a framework of laws and policies, and so on. To do this, it is necessary to acknowledge the public foundation that is still necessary for Pakistan's public and financial security. In the end, it is also critical that cyber security experts and professionals identify the current and emerging digital threats and develop a cyber-security governance framework according to the contemporary global trends in order to safeguard the cyber frontiers of Pakistan.

References

[1] Ministry of Information Technology and Telecommunication, National Cyber Security Policy 2021, Pakistan, July 2021 (Accessed: 3 January 2024)

[2] DIGITALISATION - Pakistan’s Vision 2025, “One Nation One Vision” (Accessed: 13 January 2024) https://ciltinternational.org/wp-content/uploads/2021/11/Digitalization-Pakistans-Vision-2025.pdf

[3] Prevention of Electronic Crime Act – 2009, https://na.gov.pk/uploads/documents/1470910659_707.pdf. (Accessed: 8 February 2024)

[4] Senate Defence Committee launches Cyber Security Manual for Journalists.” (Accessed: 15 February 2024) https://www.thefreelibrary.com/Senate+Defence+Committee+launches+Cyber+Security+Manual+for...-a0349547736.

[5] Cyber Security Council Bill – 2015, https://senate.gov.pk/uploads/documents/1448429639_654.pdf. (Accessed: 18 February 2024)

[6] Ministry of Information Technology and Telecommunication, National Cyber Security Policy 2021, Pakistan, July 2021. (Accessed: 22 February 2024)

[7] “The Directive on Security of Network and Information Systems (NIS Directive)” (2019), https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. (Accessed: 12 March 2024)

[8] “National Cyber Security Policy 2013” (2013). (Accessed: 26 March 2024)

[9] Anwar, Waqar. (PDF) cyber security in Pakistan: Regulations, gaps and way forward. (Accessed 28 March, 2024) https://www.researchgate.net/publication/349097228_Cyber_Security_in_Pakistan_Regulations_Gaps_and_Way_Forward.