Cyber Security: Where Does Pakistan Stand?

By

Rubab Syed, Ahmed Awais Khaver

& Muhammad Yasin
# Table of Contents

Abstract................................................................................................................................................... 1

1. Introduction..................................................................................................................................... 2

2. What is Cyber Security? ................................................................................................................. 2

3. Methodology ................................................................................................................................... 3

   3.1. Nature of the Threats............................................................................................................... 3

   3.2. Examples of Cyber Security Breaches .................................................................................... 3

      3.2.1. Russian Cyber war against Georgia ................................................................................ 3

      3.2.2. U.S. Cyber-attack against Iran ........................................................................................ 4

      3.2.3. Russian Hackers’ Cyber-attacks against NATO ............................................................. 4

4. Cyber Warfare.................................................................................................................................... 4

5. Advantages Enjoyed by the Cyber Attackers.................................................................................. 5

6. Cyber Attack Targets ...................................................................................................................... 6

7. Where Does PAKISTAN Stand? .................................................................................................... 6

   7.1.1. Prevention of Electronic Crimes Act, 2016 .................................................................... 7

   7.1.2. Essential IT services in Pakistan: .................................................................................... 7

8. Computer Emergency Response Team (CERT) – Pakistan Telecom Sector Implementation Plan 9

9. Conclusion .................................................................................................................................... 10

10. Recommendations........................................................................................................................ 10

References:............................................................................................................................................ 11
ABSTRACT

“The art of war” is an ever-changing phenomenon and a process as to how, when and where to engage the enemy. Globally a relatively newer threat is evolving not only for states but also for the private profit driven world. Billions of dollars are illegally transferred or stolen, privacies exposed, state secrets acquired and critical public infrastructure hacked. This is the realm of cyber security. As the world becomes more and more connected via internet or digitized through information technology, the cyber security threats are increasing day by day. Pakistan is no exception to it. A nuclear state with an important geopolitical position is increasingly exposed to such threats in the cyber realm. So are the business sector and the private work.

Pakistan has a large internet users’ base, an increasing digitized security apparatus as well as banking system, which depend on internet connectivity. Pakistan has also incorporated laws to tackle threat emanating from cyber-attacks, which do not seem to cover the threats in depth and wholeness. As threats evolve and come from varied foes and adversaries, we must continuously assess them and make necessary modification and rectifications in our strategy. In this perspective, the study assesses Pakistan’s cyber space, identify threats and make recommendations to eliminate those threats. It further discusses Pakistan’s legal development on the subject and the way forward.

Keywords: Art of war, Cyber security, Legal Development, Digitized, Information Technology, CERT (Computer Emergency Response Team)
1. **INTRODUCTION**

Virus threats have been here since the dawn of computing. However, they have never been on priority list in terms of security measures. Sanctity of data was never considered till the explosive growth of internet whereby the exposure of so many machines on the web provided a veritable playground for Cybercrime committees to test their skills bringing down websites, stealing data, or committing fraud. Cybercrime is, thus, a term that describes any illegal activity committed by using a computer as its primary means of commission and theft. The US Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism, which have become a major problem for people and nations. (Gade 2014)

Since the global penetration of internet by an estimated 3.4 billion users (internet users 2016), the opportunity for the cybercrime committees has exponentially increased. Thus, the practice of combating this multi-disciplinary problem, inclusive of hardware and software, and proactively preventing the occurrence of cybercrime at the first place and diminishing its impact when it does occur, is called Cyber Security.

2. **WHAT IS CYBER SECURITY?**

There is a wide range of currently acceptable definitions of cyber security:

a. The **International Organization for Standardization** defines cyber security or cyberspace security as:

   "The preservation of confidentiality, integrity and availability of information in the Cyberspace."

   In turn, the Cyberspace is defined as:

   "The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

b. The **Committee on National Security Systems (CNSS-4009)** defines cyber security as:

   "The ability to protect or defend an enterprise’s use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or, destroying the integrity of the data or stealing controlled information."

   

c. The **National Institute of Standards and Technology** defines cyber security as:

   The process of protecting information by preventing, detecting, and responding to attacks." Similar to financial and reputational risk, cyber security risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate, gain and maintain customers.

   Whenever there is technology advancement throughout the world and new opportunities are created, there will always be the ones who would exploit them for their own gains. So essentially,
cyber security seeks out protection of an enterprise from those who wish to do harm to a business, steal information or money, or use other’s system to target peers in the market.

The paper discusses both international and Pakistan’s cyber space dilemmas and responses. Besides it suggests a way forward for Pakistan’s cyber space, which is under threat at present.

3. **Methodology**

The study is based on qualitative approach. Data sources include Both primary and secondary sources of data have been used. Primary source includes focus group discussion where members from the academia, government and private sector were engaged. Recommendations and way forward were exclusively acquired from the FGD (Focus Group Discussion) exercise. Secondary sources include government reports, newspaper articles, research papers and journal articles on the subject which are readily available.

3.1. **Nature of the Threats**

Cybercrime comes in a variety of forms ranging from denial of service attacks on websites to theft, blackmailing, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransom-ware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers). The bottom line is: almost anything controllable by technology will have a weak spot. In recent years, it has been seen that everything from cars (Greenberg 2015) to medical devices (Zetter 2015) to toys (Gibbs 2015) succumb to anyone with a little knowledge, time, and opportunity.

3.2. **Examples of Cyber Security Breaches**

The Internet has become so integral to economic and national life that government, business, and individual users are targets for ever-more frequent and threatening attacks.

3.2.1. **Russian Cyber war against Georgia**

The Russian government was accused of attacking or encouraging organized crime assaults on official websites in the nation of Georgia during military struggles in 2008 that resulted in the Russian invasion of Georgia.

Russia holds a broad concept of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems and propaganda. (Smith, 2014) The Russian invasion of Georgia was preceded by an intensive buildup of cyber-attacks attempting to disrupt, deface and bring down critical Georgian governmental and civilian online infrastructure. These attacks became a massive assault on the eve of the invasion which resulted in the blocking, re-routing of traffic and control being seized of various sections of Georgian cyberspace. The attack marks a new phase in the history of warfare, being the first case in which a land invasion was coordinated with an orchestrated online cyber-offensive. This offers crucial lessons for strategists and planners whilst providing vital information about how the Russian Federation is developing its offensive capacities on the internet.
3.2.2. U.S. Cyber-attack against Iran

In 2009-2010, suspicions arose that a sophisticated government-created computer worm called “Stuxnet” was loosed in order to disable Iranian nuclear plant centrifuges that could be used for making weapons-grade enriched uranium. The governments of the United States and Israel designed the worm and that a programming error allowed it to be propagated around the world on the internet (Broad, Markoff & Sanger 2011).

Over 15 Iranian facilities were attacked and infiltrated by the Stuxnet worm. It is believed that this attack was initiated by a random workers’ USB drive. One of the affected industrial facilities was the Natanz nuclear facility. The first signs that an issue existed in the nuclear facility’s computer system in 2010. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of uranium enriching centrifuges were breaking. (Kesler, 2011) The cause of these failures was unknown at the time. Later in 2010, Iran technicians contracted computer security specialists in Belarus to examine their computer systems. This security firm eventually discovered multiple malicious files on the Iranian computer systems. It has subsequently revealed that these malicious files were the Stuxnet worm. Although Iran has not released specific details regarding the effects of the attack, it is currently estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges. By current estimations this constituted a 30% decrease in enrichment efficiency. (ibid)

3.2.3. Russian Hackers’ Cyber-attacks against NATO

A Russian hacking group probably working for the government has been exploiting a previously unknown flaw in Microsoft’s Windows operating system to spy on NATO, the Ukrainian government, a US university researcher and other national security targets (Nakashima 2016). By doing this Russia has opened a new battlefront with NATO, according to Western military officials, by exploiting a point of vulnerability for almost all allied soldiers: their personal smartphones (Grove, Barnes & Hinshaw 2017). Military cyber espionage experts said the drone flights and cellphone data collection show that Russia is trying to monitor troop levels at NATO’s new bases to see if there are more forces present there than the alliance has publicly disclosed. Lonnie Benavides, a researcher with the cyber security services firm DocuSign, says Russia provides an enabling environment for cyber offenses—whether it’s crime like stealing credit cards, or espionage to steal state secrets—because the country has some very talented hackers who do not get prosecuted.

We should reduce the number of examples on what happened in other countries and include a couple of cyber-attack/hacking incidents that Pakistan suffered.

4. **Cyber Warfare**

Once the domain of science fiction, cyber warfare is now very real, with most superpowers now having dedicated cyber warfare divisions of the military. Most modern countries are now treating cyberspace as another military domain, in addition to land, air and sea. While there have been few known, and co-ordinated cyber-attacks on physical targets, we need not to have a crystal ball to predict the future, and they will only increase. It’s telling that we are now in an age where governments, political groups, criminals and corporations can engage in cyber-espionage, cyber-warfare, and cyber-terrorism. We now live in a world where the entire warfare can be conducted virtually—though the consequences will almost
always have ramifications in the physical world. Nation-state cyber-warfare will become an equalizer, shifting the balance of power in many international relationships just as nuclear weapons did starting in the 1950s (MaAfee Lab 2015).

5. **ADVANTAGES ENJOYED BY THE CYBER ATTACKERS**

Wherever societal interaction occurs, criminals are sure to follow. The most striking example of this is in the realm of what is referred to generally as “computer crimes.” (Institute, 2002) As modern society becomes more intertwined with, and dependent upon, the computer through advancements in technology and increasing use of the Internet, the cyber-attacker is there to turn this beneficial development to his own advantage (the male pronoun is used purposefully as the vast majority of computer criminals have been males). Whether for financial gain or in pursuit of a social or political agenda, or even for the pure malicious challenge of it, cyber-attacks are committed by a number of perpetrators with varying degrees of ability and connections with each other. Thus, these cyber attackers enjoy the following benefits for the cyber-crimes they commit:

a. The first advantage is that a cyber-attack can be selective and the ramifications controlled. A cyber-attack could target a nation’s entire economy without necessarily destroying the critical underlying infrastructure or be used to target the nation’s infrastructure along with its economy. An economic attack may paralyze civilian life, weaken the state through loss of economic productivity and create public panic.

b. The second advantage is that a cyber-attack can be executed in a “completely painless form” for the terrorist because an attack can be launched at the press of a button, and does not need the deployment of several operatives, which would heighten the risk of being caught by security forces. This tactic has distinct advantages in terms of cost and visibility. The attack can be theoretically lethal with little warning and requires less effort to get past security barriers at places like airports, which may derail an operation.

c. Low cost is the third advantage, since “a 21 000-machine botnet can be acquired for just a few thousand dollars, and yet cause damage and disruption easily worth hundreds of times.” This eliminates the cost of conventional weapons and operational risk. (Nordleyb, 2013)

d. The computer criminal enjoys the advantage of picking the time, place, and tools of the crime. He can limit his endeavours to his particular specialty. Thus the attacker is often an expert in the means and nature of the crime. The defender, on the other hand, is often a generalist -- one with knowledge of a number of areas but with significant expertise in a limited number (especially relative to computer crimes).

e. The nature of the medium in which the crime is committed heavily favours the cyber criminals. Cyber criminals have no boundaries. The actions taken in the security of their residence can have affect hundreds or thousands of miles away, across interstate and international boundaries. Most law-enforcement agencies have geographical limits that comprise their jurisdiction. Exceeding such limits requires coordination with other agencies that may not share the same view regarding the seriousness of the crime or may, for any number of other reasons, not feel an urgency to cooperate.

These advantages are concrete, real and of vital attractions to cyber perpetrators, along with state and non-state actors alike, being especially solidified by the fact that governments cannot effectively coordinate amongst each other or often, even internally on the nature of cyberspace security. With exponential rise in technology, it is likely that more and more actors will see the benefits of cyber-attacks in the new cyber world to come.
6. **Cyber Attack Targets**

Cyber-attacks increased 24 per cent globally during the second quarter of 2017 compared with the first three months of the year with the manufacturing industry being the most heavily targeted. Just over a third of all documented attacks in the second quarter targeted the manufacturing industry, with manufacturers appearing in the top three targets in five of six geographic regions throughout 2016. Manufacturing (34 per cent) was followed by finance (25 per cent) and health care (13 per cent) as the most targeted sectors. Banks have also been the favourite target of skilled cyber criminals. This has been true for more than a decade. Cybercrime imposes a heavy cost on financial institutions as they struggle to combat fraud and outright theft. One report says that banks spend three times as much on cyber-security as non-financial institutions, and there is an agreement among bank regulators around the work that cybercrime poses a “systematic” risk to financial stability. (Lewis, 2018) While the number of attacks on media and entertainment decreased somewhat from last year (by 39 per cent), it remains one of the most prominent targets. As audiences around the world increase their demands for instantaneous access to quality content and the ability to view that content anywhere and on any device, the media and entertainment industry is becoming an increasingly favoured target for hackers looking to steal Personal Identifiable Information (PII). The media and entertainment industry also offer hackers looking for recognition or recruits higher visibility. While the internet and telecom industry are among the most targeted ones for DoS attacks, studies show that a large percentage of these attacks were on gaming websites, which links this particular category to the most-targeted industry of gaming. This connection could easily lead to internet and telecom quickly moving up the most-targeted list. Again, internet and telecom are highly reliant on a reputation for resiliency and uptime. Any drop-in service levels can have a dramatic effect on the bottom line.

7. **Where Does Pakistan Stand?**

The expanding cyber space, which involves the enhanced use of information technology (IT) and Telecommunications (Telecom), invites hackers to misuse and disrupt the use of cyber space. Attack space for hackers has also expanded to the extent that they can, at will, disable networks. Just imagine what will happen if the financial, electric grid system, transport and military command and control system of a country is paralyzed.

In recent years, there have been millions of cyber-attacks targeting infrastructure and services. In many cases, hackers used ransomware to make money from the victims. It is, therefore vital that we acquire the capability of not only defending against such attacks, but also the ability to launch counter cyber-attacks. This is easier said than done, because in most cases the attacker’s identity is difficult to establish. The nature of internet makes it possible to hide behind its free for all infrastructures. This is especially so when cyber-attacks are state sponsored. Also because of the asymmetry of attacks, the hackers enjoy anonymity.

Nevertheless, countries must adopt measures for effective cyber security. Cyber security has been defined as the body of technologies, processes and practices designed to protect networks, computers, programmes and data from attacks, damage or unauthorized access. In a computing context, security includes both cyber security and physical security. Cyber security envelops computer networks, infrastructure, software programmes, military command and control systems, utility services, etc. which must be protected from disruption, hacking and cyber-attacks. As the technology advances at a fast
rate, household devices will also be open to hacking and disruptions. Therefore, cyber security is a very vast field which will be an uphill task.

The last hundred years have brought much change to the ways states and non-state actors conduct the art of war. This century is increasingly being called the “information age”, but has not come without its downside. As the world relies more and more on internet, interconnectedness and technology, the threat of cyber security being breached increases manifold and has the tendency to impose serious damage (Rasool 2015). In the same way, Pakistan also faces threats from the cyber world. It’s not a surprise that Pakistan is also facing cyber space dilemma. In case of Pakistan, cyberspace has been spreading into the institutions of banking, education as well as, telecom sector, military and government sectors (Ibid).


Pakistan is cognizant of the threats it faces from cyber realm. In response to these threats and challenges, the Prevention of Electronic Crimes Act was passed in 2016, which proposes punishments for cyber offenders. According to the Act, any unauthorized access to information system constitutes a punishable offense, so does unauthorized copying of any data, access to any critical infrastructure, electronic fraud, tampering with communication information, offences against person modesty or decency, writing malicious codes or their transmission, cyber stalking, hate speech or glorification of an offence. The Act proposes both fines and jail terms for these offences. Additionally, a provision is made for Computer Emergency Response Teams, who would constitute personnel of expertise in issues pertaining to cyber security on critical infrastructure or information data. Similarly, intelligence agencies officials are to be made part of these teams as well (Ibid). The Act also proposes international cooperation in this regard to thwart or instigate threats of cyber security.

The act itself has been hailed by some as a milestone and by some as a draconian law which would hamper certain rights of citizens such as freedom of speech and give additional powers to the government agencies and departments (Guranami 2017). Many civil society organizations and politicians have raised concerns about the language of the document which leaves it open for exploitation for agencies and departments. Human rights experts call for balance between security and human rights (Khan 2016).

7.1.2. Essential IT services in Pakistan:

In 21st century, countries and business firms alike are employing latest innovative technologies to make information accessible to all, secure and confidential if need be. States have an especially significant role in his regard to keep record of their citizens. National Database and Registration Authority (NADRA) is the only organization which registers and stores the information about the population (Awan and Memon 2016). In Pakistan’s bid to fight terrorism, information about its citizen is essential. NADRA further relays the information to other government agencies for their related purposes. This information is sensitive and faces a threat of being stolen or fabricated. NADRA may be current target for cyber terrorism to block or sabotage its essential services, hack human confidential information and use them for their illegal purposes.
Similarly, other information technology-based services include financial services in Pakistan. Credit cards, accounts information and other financial information can also be acquired for theft or fabrication. In Pakistan, banking is increasing its user base at a brisk pace; the resulting threats are also multiplying. Capital markets, which are the buying and selling financial markets for long-term debt or investment purpose. This type of capital markets helps organization as well as government to invest their amount by protecting them from frauds (Awan and Memon 2016). Nowadays, capital markets are upgraded into computer-based electronic trading systems. These trading systems include stock exchanges, investment banks, treasury departments and government departments (Ibid). Figure 2 highlights offshoots of business and financial services,
8. **COMPUTER EMERGENCY RESPONSE TEAM (CERT) – PAKISTAN TELECOM SECTOR IMPLEMENTATION PLAN**

The Prevention of Electronic Crimes Act acknowledges internet as the core of modern day communication. The Act further claims that to strengthen the security of information and critical infrastructure, it is imperative to establish an authority against cyber-attacks. For this purpose, the Act proposes CERTs as a formal incident response capability. The main objective of the CERTs would be to control and minimize any damage, preserve evidence, provide quick and efficient recovery, prevent similar future events, and gain insight into threats against the organization. In order to achieve this, Pakistan Telecommunication Authority (PTA) has produced an implementation framework titled “CERT (Computer Emergency Response Team) – Pakistan Telecom Sector Implementation Plan” (PTA, n.d.). The framework is pertinent to the country’s telecom sector and recommends steps to be taken by the PTA in order to establish such teams. The framework delineates upon functions and roles of the CERT. The fact that Pakistan has a tele-density of 70 per cent, with 140 million mobile subscriber base and where three to five million users connect via the internet every hour (Ibid). Given such numbers the disruption and damage apart from privacy and security breach in Pakistan’s telecom sector could bring the nation to a standstill. To protect telecom industry and its user from cyber-attacks, the CERTs would be the vanguard.

Over the years, Pakistan has had its share of cyber-attacks. On the eve of Pakistan’s 70th Independence Day, the websites of the Ministry of Defense, Ministry of Water and Power, Ministry of Information, Ministry of Environment Change and Ministry of Food Security were hacked and defaced (Naseer and Amin 2018). Such incidences go a long way in embarrassing and exposing the weakness of the nation. Back in 2010, a similar but a larger attack was recorded, which included the hacking of 36 government websites. Not only government ministries were the target of such attacks in 2018, but also Careem, a ride-hailing app, was hit by a cyber-attack. The attack resulted in compromising information of 14 million users’ data from multiple countries, including Pakistan (Jahangir 2018). The details suggest that information such as email id, customer identity, trip details and phone numbers were compromised. Similarly, cyber-attacks on multiple banks have surfaced and are rising in occurrence in Pakistan. The Federal Investigation Agency (FIA) reported that almost all Pakistani banks were hacked by cyber attackers in 2018 resulting in loss of cash in accounts (Qarar 2018). However, the State Bank of Pakistan, the regulator of all banks, suggest otherwise and maintain that only one bank’s cyber security was breached. The confusion continues over what the nature of the threats are and how to deal with the issue. The ultimate consensus is that the banks operating in Pakistan are all vulnerable to cyber-attacks (Ali 2018)

Such incidences raise concerns about Pakistan’s cyber security capability when it comes to its nuclear weapons and installations. Globally, Pakistan faces pressure for having developed nuclear weapons and ultimately their security; the attacks in recent years on military installations have also aggravated the situation. New voices are being raised to establish a cyber-nuclear doctrine to strengthen the existing security protocols (Naseer and Amin 2018).
9. **CONCLUSION**

Globally the issue of cyber threats and responses has gained prominence both in literature, practice and government policies. The threats of the cyber realm transcend political, social and private boundaries. As the world become more and more digitized and the economy more interdependent, cyber space tends to be the medium through which our progress would unfold. Countries are increasing their scrutiny of cyber laws and policies as threats increase in occurrence and complexity. Pakistan is also expanding its cyber reach within the country and its international connectivity as well. The same threats that the world faces in cyber space are also faced by Pakistan. These threats are increasing and targeting more complex systems now. The military and other state institutions are also not spared from these attacks. Examples as how best to tackle such issues and threats are available across the globe. As Pakistan moves forward and increases in cyber reach, the cyber threats would also continue to increase. Over the years, Pakistan has done its share of legislation and progress regarding cyber space. But, those mechanisms and legislations have not adequately addressed the issue. Further there is a need for legislation, policymaking, coordinated efforts and collective responsibility when it comes to securing Pakistan’s cyber space. This study is a step in that direction.

10. **RECOMMENDATIONS**

- With the increasing use of internet and its free for all availability, the cyber space is expanding making it easier for attackers to target infrastructure and services. In order to ward off attacks from cyber space, CERT (Computer Emergency Response Team) implementation plans annexation to the PEC (Prevention of Electronic Crimes) Act is a must. Organizations should aim at resilient and “Intrusion Tolerant” computer networks. Intra-agency and inter-agency intelligence sharing and coordination must be ensured.
- Around 30 to 35 per cent of bandwidth is lost due to data packets not going directly to the source of information. On the contrary they do so via reaching varying nodes present at different locations and hence take additional time and bandwidth. To counter this, a classical Internet Exchange Point (IXP) is essential for Pakistan.
- Deliberation on a policy for cyber security was underway at the ministry. The role of academia, experts and military in fighting off cyber threats is imperative. There is a need of having a joint structure for civil and military coordination for cyber security assessment and response.
- The issue of cyber security resides at national, sectoral and institutional levels and the response must also be multi sectoral and multi layered. The need of a national level strategy to face challenges arising from cyber space must be evolved, which should be enforced and implemented through national and sectoral CERTs.
- The first and foremost priority is a national policy or a framework which delineates the mission, aims and goals of the state for ensuring cyber security. The draft for cyber security policy resides with the Ministry of Information Technology, the finalization and its promulgation must be made a priority.
- Whereas the need of action and policy for cyber security is essential, there must a balance between security and legal rights of citizens. Any cyber security policy will fail if it impinges upon legal rights.
- The role of academia and education in cyber security is integral for effectively facing challenges. Awareness from school levels must be prioritized. Even on bachelors and masters level education the quality is not optimal to produce cyber security leaders and experts. Quality of curricula and syllabus must be enhanced to meet latest challenges. Even the Pakistan Telecommunication Authority lacks the necessary human resource for cyber security positions.
REFERENCES:


Piper, T 2002, An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement-and Some Practical, 10 September, SANS Institute Reading Room site


Awan, J, Memon, S 2016, Threats of Cyber Security and Challenges for Pakistan, 11th International Conference on Cyber Warfare and Security, At USA.


