Journal of Development Policy, Research & Practice
Vol. 2, No.1 (January – December 2018)
pp. 59-77

Cyber Security Imperatives and Pakistan's Readiness: A Brief Overview

Brig. (Retd.) Mohammad Yasin[*]

ABSTRACT

With increasing use of the Internet and its free for all availability, the cyber space is expanding making it easier for hackers to target infrastructure and services. The next war between adversaries will be a cyber war. The country stronger in cyber warfare will win without even taking to the battlefield. This paper describes the types of cyber threats; advantages cyber-attackers have; categories of cyber-attacks; threats to data; and information confidentiality, integrity, and availability (CIA). It also highlights the possible targets of cyber-attacks; and the type of leadership needed in the cyber security and cyber war environment. The study aims at creating awareness in Pakistan's policymakers and other stakeholders about prevailing cyber threats and making recommendations to mitigate the dangers. Finally, some Pakistan-specific recommendations are included to mitigate the threats to the country's cyber security.

Key words: Cyber space, cyber security, cyber war, espionage, asymmetry, cyber leadership, Computer Emergency Response Team (CERT).

[*] Brig. (Retd.) Mohammad Yasin is Senior Advisor, Sustainable Development Policy Institute (SDPI) for Capacity Building in Islamabad, Pakistan. He has been with SDPI for over 17 years. He has previously worked in the Prime Minister's Committee for Research and Analysis where he coordinated a number of research projects on district administration, police systems, dispensation of justice, Information Technology, and education.

1. INTRODUCTION

The expanding cyber space, increasing prevalence and severity of cyber-attacks are posing a serious threat to the global economy and national security. According to the Hiscox Cyber Readiness Report 2017, the annual loss to the global economy in 2017 was around USD 450 billion due to lack of stringent security measures; and it is likely to increase to USD 2 trillion by 2019. In 2007, Syrian air defence was reportedly disabled by a cyber-attack moments before the Israeli Air Force demolished an alleged Syrian nuclear reactor (Tyaki 2013). The asymmetry and anonymity of cyber-attackers calls for coordinated international efforts to respond to this threat. While declaring a national emergency to deal with the threat of cyber-attacks, former United States (US) President Barack Obama (2016) said:

> The increasing prevalence and severity of malicious cyber-enabled activities constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States.

The expanding cyber space which involves the enhanced use of Information Technology (IT) and Telecommunications (Telecom) enables 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 (C2) system of a country is paralysed?

In recent years, there have been thousands of cyber-attacks targeting infrastructure and services. In many cases, hackers used ransomware to mint money from victims. It is, therefore, vital that countries, especially developing ones like Pakistan, 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 the Internet makes it possible to hide behind its free-for-all infrastructure. This is especially so when cyber-attacks are state-sponsored. Nevertheless, countries must adopt measures for effective cyber security. There are several definitions of Cyber Security, of which the most oft quoted one is:

> The body of technologies, processes and practices designed to protect networks, computers, programs and data from attacks, damage or unauthorized access. In a computing context, security includes both cyber security and physical security.

It is also called the CIA Triad (confidentiality, integrity and availability), and not to be confused with the Central Intelligence Agency of the US. Cyber security includes computer networks, infrastructure, software programmes, military C2 systems and utility services which must be protected from disruption, hacking and cyber-attacks. As technology advances at a fast rate, household devices will also be vulnerable to hacking and disruptions. This paper explains various categories of cyber-attacks, cyber threats and their objectives, the advantages cyber-attackers have, possible targets, type of leadership needed to cope with threats and mitigation strategies recommended by various cyber professionals. The paper provides a brief overview of Pakistan's current 'readiness' to cope with cyber threats. Finally, it makes specific recommendations for policymakers and other stakeholders to meet the prevailing threats to the country's cyber security.

2. CYBER-ATTACK CATEGORIES

This section focuses on the CIA Triad or categories which cyber-attackers focus on during an attack. Rouse (2014) discusses the following components of cyber-attacks:

2.1. Confidentiality

Extensive connectivity of the Internet and its inadequate security, makes it is possible for hackers to steal information. Confidentiality implies that unauthorised elements will not have access to information that is exchanged between those who should have such access. The information will not be intercepted and codes will not be broken. Civil and military organisations stand to lose a great deal if confidentiality is compromised. Challenges will become serious if information is stolen at a massive scale, like design of combat aircrafts, missiles, industrial patents and intellectual property (Ibid.).

2.2. Integrity

'This is the unauthorized modification of information… Integrity attacks can involve sabotage of data for criminal, political and military purposes' (Geers 2011, p.137). Official websites can be attacked by installing wrong information. In military C2, wrong instructions and data can be passed vertically and horizontally. Weapon systems can be given wrong commands. Security barriers may open up for criminals and terrorists.

2.3. Availability

'Cyber-attackers prevent the authorized users from gaining access to the systems they require to perform certain tasks. This is also referred to as denial of service (DoS)' (Ibid.: 21). Any DoS of banking system, power or transport system can have serious repercussions, especially if it is done for prolonged periods.

3. CYBER THREATS

According to Geers (2011), a hacker will seek the following objectives in a cyber-attack:

1.1. Espionage

Objective: to steel data and information of highly sensitive political and military communications. This can be done remotely from anywhere in the world. Adversaries continually collect intelligence to destabilise a victim's economy and keep an eye on military preparedness. This can have devastating consequences for the victim.

1.2. Propaganda

Objective: to intercept the Internet and communicate tailored information behind enemy lines. This can create confusion and spread false and fabricated news which could affect morale. Well-planned propaganda can create great uncertainty resulting in depression and fear. Lin and Kerr (2017, pp. 9-10) quote Randal Marlin's famous definition of propaganda:

> The organized attempt through communication to affect belief or action or inculcate attitudes in a large audience in ways that circumvent or suppress an individual's adequately informed, rational, reflective judgment.

In any future conflict, cyber space will be used as an effective platform for propaganda by the adversary. This can be done by spreading false rumours. Internally, even a terrorist and extremist can use this tool to brainwash a large audience. Such actions can create chaos, confusion and uncertainty. It is said that Hitler was an expert in propaganda warfare by spreading big lies. Obviously, the victims will have to devote significant effort to neutralise such propaganda and this may not always be possible.

1.3. Denial of Service (DoS)

Objective: to deny the use of required information, data or computing resources. This is done with electromagnetic interference, creating current/voltage surges or physical destruction of equipment. Any disruption in banking services, power and transport system will bring life to a standstill. Denial in the use weapon systems will result in enemy's walkover without a fight.

1.4. Data Modification

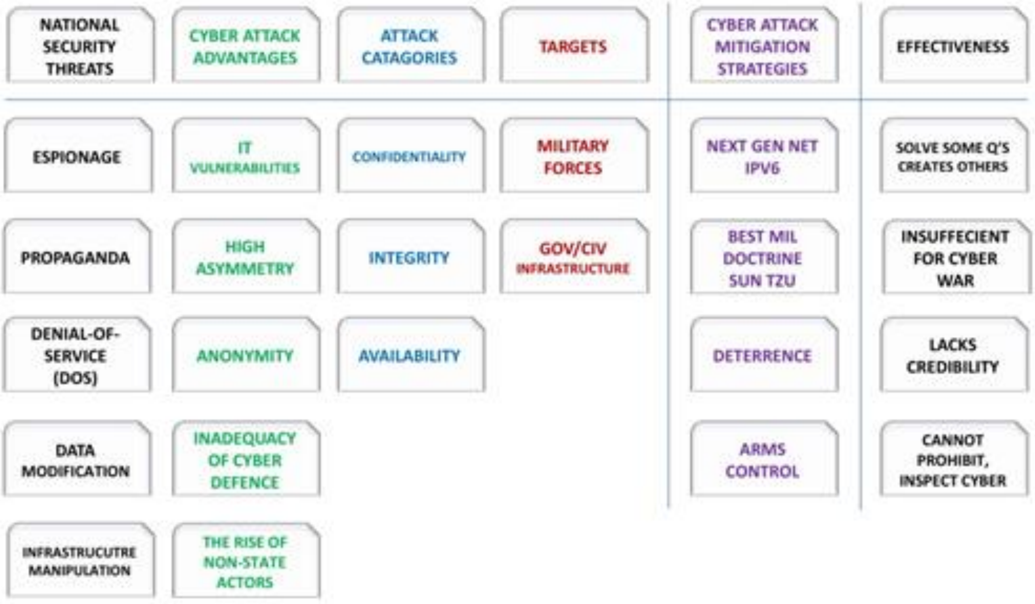
Objective: to compromise the integrity of important and sensitive data through website defacement or by introducing fictitious data in the victim's database. This is done with a high level of anonymity. In such situations, data analysis will give wrong findings/results. This could seriously affect planning and consequent implementation.

1.5. Infrastructure Manipulation

Objective: to degrade vital infrastructures like electric grids or available bandwidths and computer networks. This can also be done by the service providers. Any unauthorised modification in civil/military infrastructures/use will have devastating effects on their working. Considerable effort will be needed to recover and restore the systems. According to ASC (2016, p. 29):

> Not all attacks are about theft or destruction. A more sinister course is the manipulation of data in places such that machines can be controlled or wrong information reported to human operators without their knowledge.

Figure 1: Influencing Factors related to Cyber Security



NATIONAL SECURITY THREATS	CYBER ATTACK ADVANTAGES	ATTACK CATAGORIES	TARGETS	CYBER ATTACK MITIGATION STRATEGIES	EFFECTIVENESS
ESPIONAGE	IT VULNERABILITIES	CONFIDENTIALITY	MILITARY FORCES	NEXT GEN NET IPV6	SOLVE SOME Q'S CREATES OTHERS
PROPAGANDA	HIGH ASYMMETRY	INTEGRITY	GOV/CIV INFRASTRUCTURE	BEST MIL DOCTRINE SUN TZU	INSUFFECIENT FOR CYBER WAR
DENIAL-OF-SERVICE (DOS)	ANONYMITY	AVAILABILITY		DETERRENCE	LACKS CREDIBILITY
DATA MODIFICATION	INADEQUACY OF CYBER DEFENCE			ARMS CONTROL	CANNOT PROHIBIT, INSPECT CYBER
INFRASTRUCUTRE MANIPULATION	THE RISE OF NON-STATE ACTORS				

Source: Geers (2011), p. 133.

2. ADVANTAGES TO CYBER-ATTACKERS

Given nature of the Internet and the medium through which information passes, potential cyber-attackers enjoy various advantages. Geers (2011) lists the following ones:

2.1. Vulnerability

Because of the maize-like design of the Internet, hackers are able to find paths to enter sensitive sites. Proliferation of communication technologies facilitates such attacks. This advantage will continue till such time the Internet is made completely safe which does not seem possible, because it is available to all. No one gets any privilege or priority for its use.

2.2. Asymmetry

Cyber-attacks vary in nature. No two attacks are similar. It is difficult to foresee the nature of the next attack since it is very challenging to find a pattern. Hackers and cyber-attackers' habits based on previous practices are also hard to predict.

2.3. Anonymity

Spread and nature of the Internet enables hackers to route their attacks via countries other than the origin. For example, they can route their attack through a country with which the victim has poor relations. Thus, it is difficult to ascertain the identity of hackers. Anyone with the required expertise can be a hacker and remain safe from identification. In 2010, the US and Israel launched a cyber-attack on Iranian nuclear sites using a sophisticated and maliciously developed malware called Stuxnet. The Iranians remained under the impression that the operation of their equipment and machines was erratic. Some revolving machines would run slow, and then suddenly pick up speed, go out-of-control and burn out.

2.4. Inadequacy of Cyber Defence

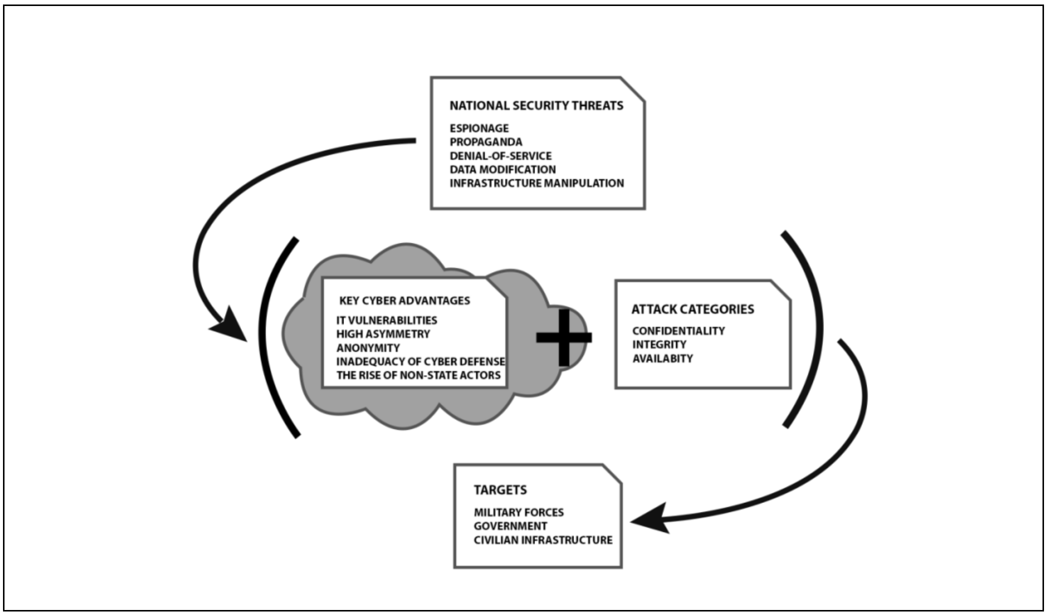
Given such advantages available to cyber-attackers and the absence of any binding international treaty, states are at a great disadvantage. Organisations are finding it very difficult to acquire cyber defence capabilities. Technical experts in cyber security are difficult to find and even more difficult to retain because of their circulation value. Although some universities in advanced countries train cyber leaders and managers, there is still a dearth of cyber defence experts.

2.5. Rise of Non-State Actors (NSAs)

The Internet is available to all. The asymmetry and anonymity enjoyed by hackers and cyber-attackers facilitate its use for espionage, propaganda, crime and military aggression. There is no international law to control the illegal and wrongful use of the Internet. Non-State Actors (NSAs) like civil society, economic/social entities and terrorists can use the Internet for their ulterior motives. NSAs are not under any obligation to respect laws. They can hack computers and important information at will. Terrorists and extremists can be a big problem in cyber security. Terrorist organisations are now well-equipped for such attacks and they are not under any legitimate control.

Terrorists or state-sponsored and non-state sponsored actors engaged in cyber-attacks to pursue their objectives can also use cyber space to deny essential services like banking, transport and power grids. Cyber terrorists, in the garb of cyber spies, can steal sensitive and vital information (Theohary and Rollins 2015). There are cyber thieves and cyber warriors who may be agents of other nations on their payrolls. Figure 2 shows how cyber space offers attackers numerous advantages that facilitate and amplify the three traditional attack categories of confidentiality, integrity and availability:

Figure 2: Key Cyber-attack Advantages



Source: Geers (2011), p. 135.

3. CYBER-ATTACK TARGETS

According to Geers (2011), cyber-attacks of strategic significance do not occur every day. In fact, it is likely that the most powerful cyber weapons may be saved by militaries and intelligence agencies for times of international conflict and war. In any future war or conflict, the element of cyber-attack will certainly be introduced. Some of the institutions that may use this tactic or could become potential targets include the following:

3.1. Military Forces

Their goal would be to disable the adversary's weapon system and C2. DoS would target the victim's communication system. The aim would be to destroy, disrupt, deny, degrade and deceive. Also, a military would aim to defend its own system from such attacks. Most militaries collect information on their adversary's deployment, readiness, supplies, logistics and reinforcements etc. The US Department of Defence (US DoD) has been conducting result-oriented exercises and games in cyber-attacks and defence. In 2008, the US DoD was a victim of a cyber-attack on its sensitive systems. The US now has a good organisation on ground to deal with cyber-attacks. Lin and Kerr (2017) write:

> From the standpoint of traditional military conflict, The United States is unmatched by any other nation. Other nations have taken note of US conventional military prowess and some other asymmetric methods of confronting the United States…Cyber warfare is one asymmetric counter.

It appears that the concept of nuclear deterrence has now gone in the background. Besides, nuclear weapons can be destroyed, but cyber weapons because of their asymmetry, anonymity and nature of cyber space cannot be destroyed. Therefore, in any future conflict military communications, C2 systems and logistics would be very vulnerable targets. Even the US and the other advanced countries have taken full stock of this situation and put necessary counter measures in place.

3.2. Government/Civilian Infrastructure

The targets could be an adversary's financial sector, industry, transport and power supply. Government functioning could be seriously hampered. Decision-making would become extremely difficult, and disable the defender from engaging in a longer conflict. This could also impact and destroy national morale.

4. CYBER LEADERSHIP

According to Francesca Spidalieri:

> Cyber defense requires not only information technology experts with computer science, electrical engineering, and software security skills, but also professionals with an understanding of political theory, institutional theory, behavioral psychology, ethics, international law, international relations, and additional social sciences…the pillars of our society… are often led by individuals with extremely limited exposure to cyber issues and the existential threats they pose…(CSFI n.d., p.6).

In the same report by CSFI (n.d., p. 8), the Committee on professionalising the US' cyber security workforce, highlights that:

> Because, cyber security is not solely a technical endeavour, a wide range of backgrounds and skills will be needed in an effective national cyber security work force.

The report recommends the following four aspects that senior cyber leaders should master - Knowledge, Skill, Abilities (KSAs):

- A senior cyber leader should possess soft skills as well as come up to technical expectations required in cyberspace.

- He / She should master the ‘executive management competencies to interact with the board of directors and other stakeholders.’
- Interdisciplinary competencies are needed for making timely and sound decisions affecting the mission, business functions and processes.
- ‘Cyber-centred competencies are needed to provide the greatest technical insight and decision-making support to the organisation’ (Ibid.).

Academic institutions and universities have to play their part in grooming / producing cyber leaders. In advanced countries like the US, some universities are already implementing programmes in cyber leadership. This is being done with the aim of producing cyber leaders who would be able to ‘effectively communicate complex technical matters in a manner that other senior leaders can understand.’ Such programmes train future cyber leaders ‘to take initiative, motivate, exhibit creativity and innovation and provide sound, seasoned judgment.’ However, a large number of interdisciplinary competencies should be included in the curricula. These programmes also include cyber-centred competencies.

5. MILITARY LEADERSHIP IN CYBER WAR

Sun Tzu’s doctrine of war appears to cover a cyber war. The concept is applicable even after 2,500 years:

> [He] advised military commanders to avoid unnecessary destruction of an adversary’s infrastructure. The best leaders can attain victory before combat is even necessary. Hence, to fight and conquer in all our battles is not a supervene excellence. Supervene excellence is breaking the enemy’s resistance without fighting (Geers 2011).

Commanders in cyber war will need a mix of leadership qualities and traits required for conventional war and working knowledge of Information Technology (IT), computer networking and data security. Cyber warfare requires timely and sound decisions. The commander must be able to think on his feet and make quick decisions. He must be able to understand the technical language and be able to communicate in that language. A commander who would be able to seize the initiative would be in a better position to influence the conflict in his/her favour.

Some advanced countries foresaw the need to raise cyber commands many years ago. The US commenced this exercise in the late nineties. Following are some of the important features of the US Military Cyber Command (USCYBERCOM):

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to direct the operations and defense of specified Department of Defense information networks; and prepare to, and

> when directed, conduct full spectrum military cyber space operations in order to enable actions in all domains, ensure US / Allied freedom of action in cyber space and deny the same to our adversaries (US DoD 2010, p.1).

The US Army, Navy and Air Force have their own cyber commands. The USCYBERCOM brings together all components of the three forces that work on cyber issues. In 2014, it employed 60,000 personnel. Its headquarters is co-located with the US National Security Agency (NSA) for better planning and coordination. ‘This allows the two agencies to share resources at the field level’, such as the ‘hundreds of PhDs in Mathematics, Computer Science, Engineering, and other fields who work there’ (Singer and Friedman 2014, p. 134). Cyber command works on three fronts, ‘cyber protection forces that will defend the military’s own computer networks; combat mission forces that will support the mission of forces in the field; and national mission forces that will aid in the protection of important infrastructure’ (Singer and Friedman 2014). According to *The Strait Times* (2017):

> The Us Army will soon send teams of cyber warriors to the battle field as the military looks to take the offensive against computer networks. While the Army’s mission is ‘attack and destroy’, the cyber troops have a slightly different goal. Not everything is ‘destroy’. The cyber soldiers have been integrated in infantry units and will tailor operations according to commander’s needs. The Army has for the past three years conducted training for such operations at a huge center in Southern California.

6. CYBER-ATTACK MITIGATION STRATEGIES

Singer and Friedman (2014) enunciate the following principles for cyber-attack mitigation:

- Build capacity to work under degraded conditions.
- Build resilience to adapt to adverse conditions. The system must recover quickly.
- Learn lessons for safe guard against future cyber-attacks.

Some actions that can be taken when attacked:

- Quickly lock down valuable information.
- Outward facing Internet services should / could be shut down.
- Organise to ‘fail gracefully’.

> Resilience is about understanding that different pieces fit together and then how can they be kept together or brought back together when under attack. The best solution is not only a matter of attitude or

> organization; it’s about people and practices (Singer and Friedman 2014).

Geers (2011, p. 140) suggests the following mitigation strategies:

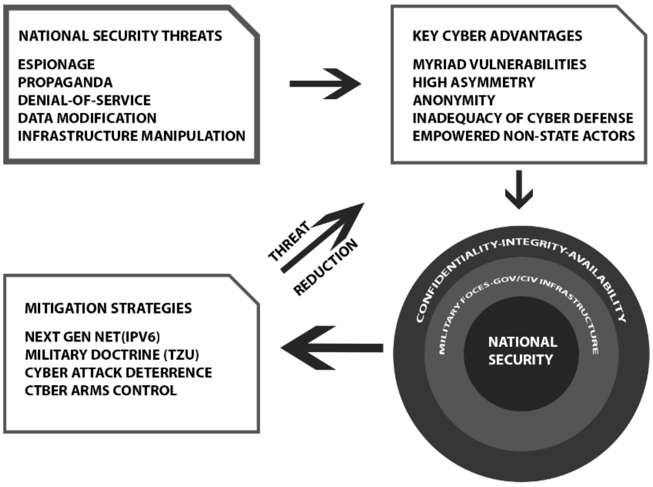
6.1. Internet Protocol Version 6 (IPv6)

This version has replaced the IPv4 version as the language of the Internet. It not only solves the world’s shortage of computer addresses, it has enhanced security. However, the security feature is optional which most organisations may find inconvenient to adopt. Despite its security features, the attackers would be able to exploit its vulnerabilities because of the expanded ‘attack surface’ as a result of increased computer addresses.

6.2. Military Doctrine

No matter how much a military doctrine builds in flexibility and adaptability, cyber-attackers can launch attacks on military infrastructure. According to Geers (2011, p.140) even ‘Sun Tzu’s Art of War which is renowned for its flexibility and adaptability to new means and methods of war has great difficulty subsuming many aspects of cyber warfare.’ Figure 3 is a causal loop diagram that shows how cyber-attack mitigation strategies are designed to reduce the impact of cyber-attack advantages with the ultimate goal of reducing the threats to national security via cyber space:

Figure 3: Causal Loop Showing Mitigation Strategies, Cyber Advantages and Threats



Source: Geers (2011), p. 139.

6.3. Computer Emergency Response Team (CERTs)

ENISA (n.d.) recommends the establishment of a national/governmental Computer Emergency Response Teams (CERTs) which should be involved in risk management. A national CERT can play a leading role in safeguarding critical infrastructure. It can coordinate the working and activities of organisations and various sector CERTs. It can also act as a point of contact during cyber-attacks. It can provide early warning to countrywide CERTs. The key to success of this mitigation strategy is full cooperation between the government, private sector, Internet service providers and mobile operators.

6.4. Readiness Pillars

According to the ACS (2016) given below are important readiness pillars:

6.4.1. Education and Awareness

Education in cyber security should start from schools. To prepare cyber security professionals is a long process especially when the technology is fast changing and the cyber space is quickly expanding. So far, there is lack of awareness among the public and private sector in Pakistan. For awareness, the government should take the lead and manage strong awareness programmes.

6.4.2. Planning and Preparation

There should be a strong understanding of the cyber threats and risks involved. A good management system should be in place. All stakeholders should have proper Standing Operating Procedures (SOPs) in place.

6.4.3. Detection and Recovery

Critical and vital infrastructures should be intrusion-tolerant and resilient. Breaches should be quickly detected and timely corrective actions taken. Detection and recovery should be the responsibility of CERTs trained and ready to meet any exigency.

6.4.4. Access Control in Network Security (NAC)

NAC approach should be adopted in computer security that attempts to unify end-point security technology such as anti-virus, host intrusion protection, and vulnerability assessment, user or system authentication and network security enforcement.

7. SUN TZU’S ART OF WAR AND CYBER SECURITY

Sun Tzu’s 5th Century military strategy known as *The Art of War* is so flexible that it is even applicable to cyber security. Madsen (2017) highlights its following principles which are relevant to cyber security:

7.1. Know the Enemy and Know Yourself.

This is an important principle of military leadership. Even during peace time, intelligence gathering about the enemy's military preparations and his war plans are gathered. At the same time, one's own strengths and weaknesses are analysed and preparations are made to counter enemy threats/attacks. In cyber security, this means understanding how a hacker is likely to operate. What are his/her strengths and resources? How are one's own systems and infrastructures protected? Does one have trained professionals and resilient infrastructures? How can one overcome weaknesses?

7.2. All Warfare is based on Deception.

In military strategy and tactics, deception is an effective weapon of war. Deception gives one an edge because the enemy would not know where the attack will be and with what strength. Cyber-attackers use methods that are based on deception. To gain sensitive information, hackers may pose themselves as heads of organisations. Untrained and unsuspecting staff members will be tricked into divulging secrets and sensitive information. Thus, cyber-attackers and hackers may achieve their objective through stalking and phishing. Intrusion deception is a new approach to cyber security built on the classic philosophy from the *Art of War*. Sun Tzu said that 'you should appear weak when you are strong and strong when you are weak.' A website can appear weaker, and yet actually be stronger.

7.3. Attack Him Where He is Weak, Appear Where You are Unexpected.

This is the principle that the attacker will follow. Untrained employees would be the weak link. Attackers will also search other paths to enter organisational systems and infrastructures. This again boils down to the strategy of training employees in cyber security. Organisations should have competent security experts. There should be full intra-agency and inter-agency coordination; and post-attack learning exercises from hacking experiences.

8. WHERE DOES PAKISTAN STAND IN CYBER SECURITY AND CYBER WARFARE?

In relation to offences committed by any person or service providers and punishments for various crimes, the Parliament of Pakistan on 22 August enacted the Prevention of Electronic Crimes Act, 2016 legislation which also covers cyber terrorism, cyber stalking, spamming and spoofing, etc. Most importantly, it lays down preventive measures which include constituting CERTs with the following functions:

- 'The Federal Government may constitute one or more Computer Emergency Response Teams (CERTs) to respond to any threat against or attack on any critical infrastructure, information systems or critical infrastructure data or widespread attack on information systems in Pakistan.

- A Computer Emergency Response Team constituted under the above sub-section may comprise of technical experts of known expertise, officers of any intelligence agency or any sub-set thereof.
- A computer emergency response team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data as may be prescribed' (GoP 2016).

Following up on the Prevention of Electronic Crimes Act, 2016, a comprehensive implementation plan was prepared by the CERT of Pakistan Telecom Authority (PTA).Typical services offered by a CERT include:

- **Reactive:** This is the core component of CERT designed to respond to threats and attacks.
- **Proactive:** Designed to avoid incidents and to reduce their impact and scope when they do occur.
- **Security Quality Management:** Designed to improve the overall security of an organisation. Other organisational entities such as IT or technical audit can provide these services, but participation of CERT in these services improves their effectiveness.

The PTA CERT framework is about what needs to be done to protect critical information and infrastructures. The plan lists responsibilities of PTA licensees, and defines the critical information assets and the critical information infrastructure that must be protected. The licensees are required to set up an internal CERT which will immediately come into action in the event of a cyber-attack. The CERT will also enforce protective measures. In fact, this is required by all organisations, not only by the licensees.

8.1. PTA Responsibilities

PTA CERT is supposed to be a dedicated team with its own budget to coordinate with all licensees and keep itself updated on information security situations and provide support. It is also meant to coordinate with other organisations; and provide the following care services:

- Incident analysis
- Incident response support
- Incident response coordination
- Coordination with global CERTS
- Coordination with academia
- Vulnerability and artifact response coordination
- Alerts and warnings

- Announcements
- Security-related information dissemination
- Awareness building, education and training.

The plan lays down resource requirements of CERT including human resources, equipment and other related infrastructure. It comprehensively lays down duties and actions to be taken by a CERT. A comprehensive set-up has been planned ranging from Information Security Analysis Centre to Country Wide Cyber Security Operations Centres. The PTA has done solid work in devising an elaborate plan to cope with the ever increasing incidents of cyber threats and cyber-attacks. The plan is open to revision and updates as the cyber situation evolves globally. However, it is not known how far the plan has been implemented and whether or not the proposed organisation is on ground. Whether or not PTA licensees have CERTs, whether the proposed infrastructure like Information Security Analysis Centre and Country Wide Cyber Security Operations Centres have been established are unknown variables. Also, what is being done to train/groom cyber security leaders and managers?

8.2. Pakistan Military Cyber Command

Pakistan military functions are network-centric. Due to hostile regional neighbours, other NSAs and forces which are bent on destabilising, weakening and even breaking up Pakistan, the military is vulnerable to cyber-attacks. Any future war is likely to be a cyber war. An adversary rich in cyber warfare technology will win without even taking to the battlefield.

9. WAY FORWARD

Before anything else, the world needs an international arms control treaty for cyber space. This can be done along the lines of the Chemical Weapons Convention (CWC) of 1997. Such a treaty may, at least deter state-sponsored hacking and cyber-attacks. The International Telecommunication Union (ITU) should be mandated by the United Nations (UN) to regulate the Internet. Previous such moves were opposed by powerful countries like the US. These measures are difficult to implement because of the nature of the Internet. However, given political will of world powers a beginning can be made.

The Internet should be made more secure. Although, IPv6 is an improvement over IPv4, it is still not the answer to hacking and cyber-attacks. The telecommunication technology is advancing very fast and additional security features can be added to make it more secure. Building firewalls by countries is not the answer to the problem of cyber security as this would restrict the use of the Internet. Advancing technology can make computer infrastructure designs more resilient. This would enable systems to endure security threats and recover quickly after a cyber-attack. This would mean intrusion-tolerant infrastructures. Coordination and information sharing among the government and civil agencies and Internet service providers will help in taking joint measures to recover quickly and learn lessons from such attacks.

Another important trend is Cloud Computing where individuals and organisations instead of using their own infrastructures/resources purchase outside services. The organisations do not run their own servers. Even militaries of some countries are using it. The providers of cloud computing take care of cyber security. Organisations and individuals lack cyber security expertise and hiring and retaining them is expensive. Cloud Computing service providers have trained cyber security engineers to limit hacking and attacks.

The threats of cyber security and cyber war will continue to hover. To become cyber-resilient, countries are enhancing their talent pool of professionals in cyber security. This requires a national level approach. Colleges and universities will have to produce cyber leaders and managers. For Pakistan, the government, the private sector and the military must collaborate and coordinate in this endeavour.

10. POLICY RECOMMENDATIONS FOR PAKISTAN

This paper makes the following recommendations based on Yasin (2017):

- Develop comprehensive legislation covering individual and state sponsored cyber-attacks/cyber warfare. Although there are laws on cyber crimes, they do not cover organised cyber-attacks and state-sponsored attacks.
- A draft Cyber Policy exists, but a revamped Cyber Security Policy is needed. This should include goals, objectives, systems, organisations and responsibilities.
- A full-time, combined workforce, involving all stakeholders from the Armed Forces and civil organisations, needs to be raised and trained. Currently, due to lack of collaboration, a holistic pattern of cyber-readiness has not evolved. Above all, Pakistan needs a collaborative mechanism. The National Security Division (NSD) should quickly take on this responsibility.
- The CERT (Computer Emergency Response Team) – Pakistan Telecom Sector Implementation Plan should be annexed with Prevention of Electronic Crimes Act, 2016 through legislation (if considered appropriate).
- A military cyber command should be established. A suitable existing model of an advanced country can be adopted.
- Universities should start programmes to prepare cyber security leaders and managers. Here again, curricula followed by some international universities can be adopted. A future generation of technically proficient cyber security specialists should be prepared.
- Security audits carried out by PTA CERT, weaknesses observed and guidance for corrective actions should be shared with all users of IT.
- Organisations should aim at resilient and ‘intrusion tolerant’ computer networks.

- Inter-agency and intra-agency intelligence sharing must be ensured. The key advantage of information is that it allows more holistic view of emerging threats and patterns and lessons learned from experience.
- There should be an international agreement on the fair and lawful use of cyberspace on the lines of Geneva agreements, and agreements on telecommunications that are facilitated by the ITU.

11. CONCLUSION

The need to acquire requisite capability to neutralise cyber-attacks is now the most urgent and vital requirement. But, growing dependence on the Internet has simplified the work of cyber-attackers. Effective steps against hovering threats are difficult because of the advantages of asymmetry and anonymity which hackers have. However, this does not mean acceptance of this dimension as *fate accompli*. Effective and realistic SOPs, to include organising trained CERTs, effective coordination among the public (including the defence establishment) and the private agencies (including Internet Service Providers) and preparing future cyber leaders and managers can make the difference because any future war will be fought in cyber space not the battlefield.

REFERENCES

ACS 2016, ‘Cybersecurity: Threats, Challenges, Opportunities’, [Online], November, Australian Computer Society, <https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf>.

CSFI n.d., ‘Senior Cyber Leadership: Why a Technology Competent Workforce Is Not Enough’ [Online], Omaha and Washington, D.C.: Cyber Security Forum Initiative (CSFI).

ENISA n.d., ‘Baseline Capabilities of National/Governmental CERTs (Policy Recommendations)’, [Online], European Network and Security Agency, Greece.

Geers, K. 2011, *Strategic Cybersecurity*, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (*CCDCOE*), <http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF>.

GoP 2016, ‘Prevention of Electronic Crimes Act, 2016, Act No XI of 2016’, *The Gazette of Pakistan* , 22 August, Government of Pakistan, Islamabad, <http://www.na.gov.pk/uploads/documents/1472635250_246.pdf>.

Hiscox Insurance 2017, ‘The Hiscox Cyber Readiness Report 2017’, <https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf>.

Madsen, T. 2017, ‘Sun Tzu’s “The Art of War” for Cyber Security’, *Infosecurity Magazine*, 29 May, <https://www.infosecurity-magazine.com/opinions/sun-tzus-art-of-war-cybersecurity/>, accessed 10 November 2018.

Obama, B. 2016, ‘Executive Order--Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities’, [Online], Executive Order, December 29, The White House, <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency>, accessed 9 November 2018.

Rouse, M. 2014, ‘Confidentiality, Integrity, and Availability (CIA Triad)’, [Online], *TechTarget.WhatIs.com*, <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>, accessed 8 November 2018.

Singer, P.W. and Friedman, A. 2014, *Cybersecurity and Cyberwar*, New York: Oxford University Press.

Theohary, C.A. and Rollins, J.W. 2015, ‘Cyberwarfare and Cyberterrorism In Brief’ [Online], Congressional Research Service, 27 March, <https://fas.org/sgp/crs/natsec/R43955.pdf>.

The Straits Times 2017, ‘US Military to Send Cyber Soldiers to the Battlefield’, 14 December, <https://www.straitstimes.com/world/united-states/us-military-to-send-cyber-soldiers-to-the-battlefield>, accessed 8 November 2018.

Tyagi, R.K. 2013, ‘Understanding Cyber Warfare and Its Implications for Indian Armed Forces’, New Delhi: Vij Books India Pvt. Ltd.

US DoD 2010, ‘U.S. Cyber Command Fact Sheet’, 25 May, United States Department of Defence, U.S. Strategic Command, <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf>.

Yasin, M. 2017 ‘Cyber Warfare’, *Research and News Bulletin*, vol. 24, no. 3, Sustainable Development Policy Institute, Islamabad, Pakistan.