CYBER-WARFARE: IMPLICATIONS FOR THE NATIONAL SECURITY OF PAKISTAN

Muhammad Imad Ayub Khan[*]

Abstract

Computer networks serve as the backbone of modern-day information and communications technologies. These networks have no physical boundaries that contain important data and information critical to any state's national security, which is vulnerable to cyber-attacks in the digital domain. This dilemma gives birth to the term cyber-warfare and it is one of the most critical security issues in present-day world. Huge investments are being done by the countries to use it as an offensive tool vis-à-vis they are also trying to build a steady force for the protection of their cyber-space. Cyber-Warfare poses a much complex and dangerous threat to the National security of Pakistan in the era of hybrid-warfare. This paper aimed to explain, what kind of threat does Pakistan faces in the domain of cyber-warfare and what effective measures Pakistan should take against such threats. This paper is based on deductive reasoning from the experiences of other nations to chart out a way forward for the National cyber policy of Pakistan as Pakistan is indeed developing with an effective speed in the field of information and communication technology, but the security aspects are not focused upon, which exposes a major unregulated domain of cyber-space to cyber-attacks, which can undermine the national security of Pakistan.

Keywords: Cyber warfare, National Security of Pakistan, Cyberspace, Information and communication, technology, Security Dilemma.

Introduction

Pakistan has witnessed the impact of cyber-warfare in the shape of minor cyber-attacks and violent use of its cyber-space in the last five years in the form of hate speech and exploitation of religious sentiment of its population. We as a nation have witnessed the use of social media, such as Facebook, Twitter, YouTube etc. for different religious and political movements. The threat of religious violence and propaganda of extremist views through the social media is, at the moment, on an insignificant level and not so powerful in shaping the anti-state propaganda. However, this might escalate to a significant level in the future if left untapped. The Government of Pakistan has been involved in the development of a policy against

[*]Muhammad Imad Ayub Khan is a Software Engineer and MPhil Scholar at Department of Strategic Studies, National Defence University Islamabad, Pakistan.

cyber-attacks since 2003, but so far, no real implementation has been put in practice. With the passage of time, the domain of cyber-space is not only abused by cyber-criminals, but has also become the strongest safe-heavens for cyber-terrorists to recruit and use the networks for communication, data collection, psychological warfare and mobilization.[1]

Cyber warfare domain can be identified from the technical history of cyber development. Cyber warfare is traced backed to the start of the electronic warfare era, where the use of electric and radio communication came to the battlefield. The rapid evolution of computer technology since the dawn of the 21st century, have led most security thinkers to define cyber-warfare as part of military strategy and tactics. Sometimes these attacks are organized to weaken a state's fighting capacity in hostility, but the main problem still exists in terms of the purpose for which the attack was launched and the nature and desire of attackers. In both cases, cyber-attacks are not merely military instruments. The increasing use of information technology, especially in military and logistical operations, has made the militaries and other critical national security infrastructures vulnerable to cyber-attacks; thus leading to the creation of new military institutions, such as "Cyber-Commands" by various countries, whose primary purpose is not to prevent these attacks but rather to prevent, protect and counter-attack. There are many aspects of attribution-related cyber-attacks, as these attacks are not fully defined in international law, and more importantly, it is very difficult to investigate and gather evidence to prosecute when it comes to litigation.

Although cyber-space is a recent phenomenon, and even the basic definitions have not yet been agreed upon. However, the influence of cyber-space is widespread and immense. The rapid development of Information and Computer technologies (ICT) affects all aspects of human society, including the international political system. Cyber-space is an area of strategic importance and nation-states seek to use Cyber-space to promote their national interests. "Nation-states use all possible options to ensure their survival".[2]

Concept of Cyber-warfare

Cyber-warfare means the use of cyber-space for political aggression against the enemy for sabotaging its digital capacity. It involves the use of digital battle space for attacking enemy's computers and networks in which one can be either the offender or the defender involving operations pertaining to cyber-threats such as espionage, sabotage. The ongoing debate on cyber-warfare to define it as an act of war still resultless in its definition but still, this developing area in information technology has raised the alarms and nations have started taking countermeasures

by developing capabilities and has technically involved with the term cyber-warfare either as an aggressor, defendant or even both. The terms cyber-security, cyber-warfare and cyber-space are as interrelated as in the practical arena the terms security, battlefield and warfare.

Cyber-security-in general is a term used for the protection and regulations of cyber-space that is all the digital information. It includes transmission networks, which are used for the transmission of digital information across different organizations and institutions across the country through the internet. These networks are also used for the transmission of data, which can be classified as sensitive to the national security of a country.

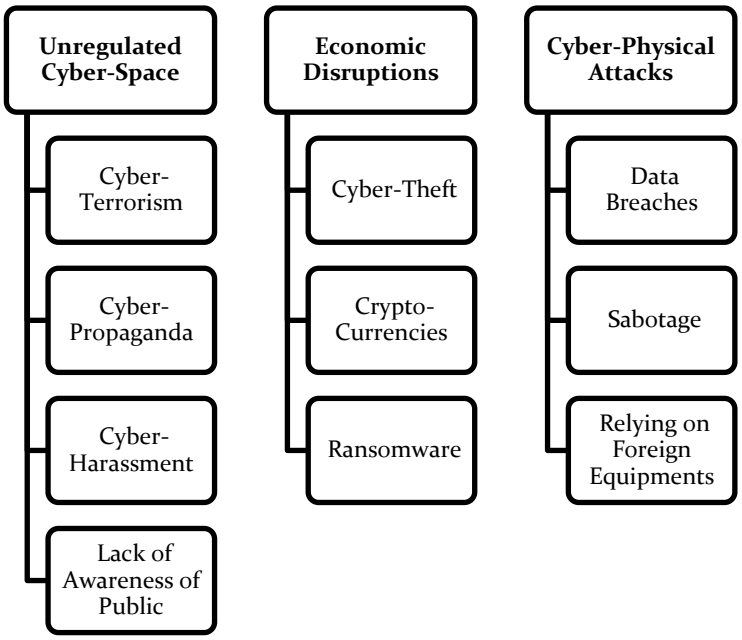
National Security of Pakistan: The Role of Cyber-warfare and Cyber-security

Pakistan's rivalry with India and its engagement in the war against terror enhance the necessity of effective cyber-defense in order to prevent hacking, online incitement and even digital surveillance. In Pakistan's recent history, some of the incidents indicate violence induced through cyber-channels like Cyber-Jihad, digital surveillance and Hacktivism falls under the umbrella of cyber-warfare, which have all the potentials to undermine the national security of Pakistan.

Pakistan has even lagged behind its neighboring countries, such as India and Iran, in vision, leadership, infrastructure, appropriate legislation and thoughtful policies to respond to any cyber-attack.[3] Our traditional rival, India, which has invested a lot on this front in the previous two to three years and has also activated the Defence Cyber Agency (DCA), which a tri-services command of the Indian army responsible for cyber-defence and led by Rear Admiral Mohit Gupta.[4] Researchers and lawmakers have already on many occasions pointed out that cyber-threats pose threats to the national security of Pakistan. Senator Mushahid Hussain, Chairman Senate Committee on Defense and Defense Production in 2013, said that;

> *"The cyber-security threat can affect Pakistan's national defense, security, intelligence, diplomacy, nuclear and missile program, economy, energy, education, civil aviation as well as industrial and manufacturing units both in the private and public sector. Cyber-security is an issue of paramount importance for Pakistan's stability and progress."*[5]

Similarly, former National Security Advisor, Naser Khan Janjua also said, "Cyber-attacks pose an enormous threat to the national economy, defense and security."[6]



Cyber-Threats to the National Security of Pakistan

Three broad categories of cyber-threats can be analyzed from the last two decades of cyber-attacks in the entire world, which further comprises the number of cyber attacks such as;

Unregulated Cyber-space

The laws regulating the Pakistani cyber-space are very minimal and can be easily evaded by someone with a little knowledge of the computer systems.[7] For Instance, we go back to 2008, when the first time Pakistani authorities ordered to block anti-Islamic content on the internet but due to the lack of an effective URL filtering system small free available softwares were used, which easily bypassed the Pakistan Telecommunication Authority blocking system.[8] Similar the Pakistani government on numerous occasions has banned access to many website contain blasphemous, pornographic and anti-state content, which has been termed almost totally in-effective because of poor blocking mechanisms. This is because Pakistan has been on the very low rating of ICAN (The Internet Corporation for Assigned Names and Numbers) where there is a very poor system to maintain the records of internet data flow. Freeware software can easily hide the real identities and location of a user using the internet in Pakistan which is very alarming indeed. The unregulated cyber-space has given birth to the following threatening concepts in Pakistan.

- **Cyber-Terrorism:** Unregulated cyber-space has fueled the impact of terrorism, where terrorist organizations use the digital information medium to spread violence, terror and extremism with quite ease. Pakistan has already suffered a lot in the last two decades due to terrorism. Pakistani armed forces have achieved significant success by eradicating the conventional terror attacks. However, the threat of cyber- terrorism is now posing a more potent threat due to its stealth nature. Attack on Bacha Khan University, Mardan in 2016 was planned and executed by terrorists using Afghan soil and the Afghan telecommunication network.[9] Similarly the famous Safoora bus attack in Karachi was claimed by Janduallah based in Afghanistan[10] the individuals like Saad Aziz, Tahir Hussain Minhas and Asad-ur-Rehman, who all were university students were basically inspired by ISIS.[11] These kinds of attacks are very dangerous because of its surprising nature and pose a serious threat to the national security. The case of Naureen Leghari who was a 2nd year student in medical college and joined the IS through extensive use of Facebook and was later apprehended by Pakistani security forces also merit mentioning.[12]
- **Cyber-Propaganda:** Cyber-Propaganda is the use of cyber-space to spread violence, anti-state agenda and narrative of extremism by individuals, political and religious groups. This kind of propaganda can put any government under immense pressure. The effect of cyber-propaganda can be witnessed from international events such as the alleged manipulation of the 2016 US presidential elections by Russia. In this case fake news and stats are used to engineer the minds of the voters using social media. This kind of act undermines the fairness of any elections. Pakistan has also been suffered by such events in the last two to three years. We have witnessed the use of social media by different religious and political movements. The rise of Tehreek Labaik Pakistan (TLP) to promote religious violence has twice put Pakistan in difficult times both in 2017 and 2018.[13]TLP used social media to spread its agenda in which the government was helpless to maintain law and order in the country and the common people suffered a lot in the form of physical and mental loss.[14]
- Another pertinent case is that of Pashtun Tahafuz Movement (PTM) which emerged in the last two years exploiting the sentiments of Pashtuns in the Federally Administered Tribal Area of Khyber Pakhtunkha and spreading it to the whole of Pakistan. The movement anti-state slogans made a soft power platform to instigate hatred in the critical phase of the ongoing war against terrorism.[15] The scale of the

event can easily make it a platform for anti-state elements to exploit the weakness of participants to promote anti-state agenda. Similarly, the internet and social media have been flooded many times by fake news to create panic within the public.

- **Cyber-Harassment:** Also known as cyber-bullying, this is the individual use of cyber-domain to bully people across many social media platforms. Most of the times the victims are general users of social media, who are blackmailed and used for different purposes. The effects of cyber-bullying are different, but research shows that cyber-bullying has a disproportionate impact on young people than adolescents and adults. Young people are more likely to suffer as they continue to grow physically and mentally. Children who are harassed are likely to experience anxiety, depression, loneliness and depression.[16]
- **Lack of Awareness of Public:** The most critical problem that Pakistan faces in cyber-domain is the lack of understanding of the public on how to use the internet/social media platforms. Lack of knowledge convinces mostly under-educated class to believe fake news rather than even now understanding what they are seeing on their devices. Lack of understanding of cyber-ethics often leads to cyber-bullying, harassment, theft or being terrorized. This category fuels the above-defined categories to act as a catalyst to broaden the spectrum of cyber-attacks. The major cause of this is the lack of the subjects from the Pakistani educational curriculum from primary to university levels. No Computer subject books cover the subject of Computer Ethics and cyber-warfare. Even today only one University in Pakistan i.e. National Defence University (NDU) offers the course of cyber-Security as an elective subject but the lack of interest of students often leads the course to be dropped due to less number of students. This issue has created concern in Pakistani cyber-experts as the public can hardly understand the threat posed by the spectrum of cyber-space. This is not only important on the academic level but rather at the national level to make the public aware of how to surf and use the cyber-domain safely to secure them from being a soft target for the outside world.

Economic Disruptions

The modern era has become dependent on ICT based economic facilities such as e-trade, e-commerce and e-banking. Such terms have made life extremely fast and brought tremendous changes in the existing patterns of life, at the same time such practices have become vulnerable to cyber-attacks. Economic disruption

in the cyber-domain is considered as the most critical because the purpose of such cyber-attacks is to target the economic system of any country, which can create panic among the public. Such attacks are either to inflict damage or maybe even led to direct stealing of money. The target can be banking systems, which are directly linked to the economies of nation consequently economy is one of the most important pillars of any nation's national security. Pakistan has most recently been the target of such attacks at minor levels targeting many bank account holders in 2018 but coordinated attacks in this domain can have a catastrophic impact. Following terms have cautioned the life of an individual and brought a huge impact on national security;

- **Cyber-Theft:** Cyber-theft is the stealing of money targeting internet-based trading and banking companies. Pakistan witnessed such kinds of attacks most recently in November 2018, when people were deprived of millions of rupees using unauthorized online transfers.[17] Pakistani authorities were helpless to explain the incidents. Until now no criminal is identified and has created a dilemma, where people are losing trust in using internet banking systems, which again will put Pakistan on backbenches in this domain. Internet scammers and hackers have led many online payment companies to put a ban on Pakistan from using its services such as PayPal, Google AdSense, Skill and many others. The misuses of Pakistani credit cards and debit cards have compromised people's trust. In this regard, the latest report claimed that card data of almost 20,000 users was stolen and sold to hackers on the dark web.[18] This kind of attack holds the potential to inflict major damage to the economy of any country in general and Pakistan in particular in the coming future and will ultimately compromise the national security.
- **Crypto-Currencies:** The mysterious rise of crypto-currencies in the last few years has attracted investments from major investors because of its secure and stealthy nature. Crypto-currencies are forecasted to be used extensively in terror financing because of its complex transaction systems, for a country like Pakistan with less efficient e-payments systems it is difficult to avert and track the financial activities of terrorist and anti-state organizations, which are directly linked to its national security. There are many registered crypto-currencies in the world, while some are unregistered. In any case, the stealth transactions have attracted terrorist organizations to use unregulated currencies. Money Laundering is also common, using unregistered crypto currencies. According to statistics, there is almost 2073 crypto-

currencies in operation with an approximately market capacity of 1.4 trillion US dollars.[19] The Legalization of crypto currencies varies from country to country. There is an "absolute ban" on the use of crypto-currencies trading in countries such as Algeria, Lesotho, Bolivia, Egypt, Bahrain, Iraq, Pakistan, Morocco, Nepal, Lithuania, and the UAE. Whereas an "implicit ban" applies to another 15 countries.[20] Pakistan, however announced a ban on crypto currencies and the State Bank of Pakistan strongly warned financial institutions against its use in Pakistan. But the lack of an effective system against the use of crypto currencies led to 60% increase in the value of Pakistan's first and only crypto currency, PakCoin. The use of crypto currencies in terrorism, tax evasion and money laundering is becoming a major threat not only to the economy, but also to the national security in larger framework.[21]

- **Ransomwares:** Ransomwares are virus softwares that are used to infect target computers and encrypting its data unusable until a specified ransom is paid-off to the unidentified attackers to decrypt the data for using again. Most of the time the attackers demand the money in crypto-currencies which makes then difficult almost impossible to track down the attackers. These kinds of attacks got famous in mid-2017 when the UK's NHS computer systems were attacked. Hackers gained access to the UK medical system. A computer virus is known as "WannaCry" is distributed via email as an attachment, because as the computer user clicks on it, all his data is blocked by the spreading virus in the computer system and will require online money transactions to the attackers to gain access to those files again. Around 300,000 connected computers were infected with WannaCry due to which the National Health Services (NHS) of the U.K remained inactive for several days when a 22-year-old Devon security researcher managed to find a kill switch and restore access to the system.[22]The same kind of attack dubbed was used to hack computer systems in Ukraine during its conflict with Russia by using a virus named "Petya".[23]

Cyber-Physical Attacks

These attacks are also known as "cyber-to-physical effect," when the hacker/attacker reaches the real world from his virtual computer world results in a catastrophic consequences. The use of "Stuxnet" computer virus by the Americans and Israelis, which infected the computers of the Iranian nuclear program and caused disruption in thousands of programmable logic controllers (PLCs) controlling the centrifuges used for the uranium enrichment process.[24] Such attacks are

identified as top-level attacks by countries such as the US; which considers these attacks as critical to their automated SCADA systems (Supervisory control and data acquisition) and Information Control Systems (ICS) which is used in many of their systems such as Water Management, Electrical Power grids and other critical infrastructure. The following cyber practices fall in physical cyber attacks.

- **Sabotages:** Sabotage in the domain of cyber-warfare is considered as the attack, where the target of attackers is the computer systems controlling critical infrastructures, such as Nuclear Weapons, Nuclear Power Grids, Electric Distribution Systems, Automated Production Systems, Transportation Systems and many others. Pakistan luckily has not faced such kind of attacks because of two reasons. First, Pakistan has developed both its nuclear program and appropriate defense mechanism which on many occasions has been termed satisfactory by International Atomic Energy Agency (IAEA). Secondly, Pakistan remains underdeveloped in Industrial control systems, which will change in the future and the probability will increase with the introduction and development of modern technologies. This kind of development in technology makes any country of the world a target for sabotages as was the case of Iran when its nuclear program was hit by the Stuxnet virus.[25]
- **Data Breaches:** Data breaches have emerged as critical failures in information and communication systems. For example, in the last three years on many occasions, the personal data of individuals using social media on the internet have been breached and accessed illegally, which is then sold illegally on the internet, which in turn is then used in cyber-harassment. These kinds of breaches have been termed as critical by many researchers as this data can be critical in shaping the ideology of the public using fake news according to pre-defined agenda. Data breaches have been reported since 2005 but the most critical data breaches happened in 2017 and 2018. In 2018 a Cambridge Analytica whistleblower reveled that data of more than 50 million Facebook users were exposed to Cambridge Analytica, which was used to target American voters.[26] Data breaches have been allegedly termed as a major factors leading to events such as Arab Spring, the US presidential election (2016) and the Brazilian presidential elections(2018). Keeping these in mind it is important to explain here that according to Pakistan Telecommunication Authority, 60 million users of Pakistan has access to the internet out of which 40% have registered user profiles on social

media. This can lead to an unwanted situation in the future if such data is breached illegally.

- **Relying on Foreign Equipments:** The use of foreign equipment in the domain of information and communication technology is one of the most ill researched areas in cyber-space. Most of the computer systems used around the world is developed by major powers and used in the critical infrastructure of many countries. The use of such systems can be exploited if the manufacturers leave a back door, backchannel, RAT (Remote Access Trojan), etc. in computer equipment. Pakistan like most of the countries around the world relies on foreign computer equipment's from small microprocessors, embedded systems to heavy-duty industrial computer system, which can at some time in the future pose a threat to the national security.

Pakistan and Cyber Warfare; An Analysis

Pakistan currently has a very low level of cybercrime laws, which are supposed to combat low-level cyber-crime. There is nothing as such to combat cyber-warfare at a broad and effective national or international level and neither there is any such strategy. Moreover, the current laws are ineffective rather public hardly knows about these laws. The first "Electronic Transactions Ordinance 2002" was drafted only to deal with banking issues, whereas, "Pakistan's Cyber-Crime Bill 2007" covers cyber-terrorism, misuse of electronic encryption, electronic system fraud and electronic forgery. The current and only first-level response to any cyber-crime in Pakistan has been adopted in the form of "*Prevention of Cyber-crime Act 2015"* which is the only drafted law in the constitution of Pakistan to combat cyber-crime. It explains the specified areas of cyber-crime and punishments for committing cyber-crimes in Pakistan. Moreover, the bill also highlights different types of crimes that come under the umbrella of cyber-crimes in the Pakistan Cyber-Space.[27]

The National Response Center for Cyber-crime (NR3C) was set up in 2007 and mandated to the Federal Investigation Agency (FIA) to primarily combat technological crime in Pakistan. It is the only unit of its kind in the country and, in addition, to directly receive complaints, it also helps other law enforcement agencies in their own affairs.[28]But since the inception of NR3C, if one compares it on the technological analysis to the modern innovations in cyber-crimes, the statistics of NR3C reports about its implementation are poor. Neither it is up to the standard neither it is properly regulated. Even the basic setup of the agency is not up to the marks when compared with other agencies of the world.

Way Forward for Pakistan

The following international and national level recommendations are suggested against the threats identified in the cyber warfare domain.

International Level

Information and Communications Technology (ICT) is one of the main security challenges around the world. Risk assessments suggest that the real and universal emergency may be caused by the fact that the state or group of companies may create fear by using ICT to destroy the basic framework or military coordination systems. The proliferation of asymmetric warfare (i.e., conflicts between nations or groups that have disparate military capabilities) has expanded the use of ICTs by the states, which requires the promotion of a digital lead code throughout the world.[29]There is an urgent need for interstate participation to mitigate the dangers of Cyber-Crime, Basic Cyber-Attacks, Electronic Secret Work, Mass Information Interventions and Proposed Hostile Actions to expand control through the power of the Internet. The development of digital hazards can accelerate the monstrous social and financial damage, and it is necessary to re-calibrate worldwide efforts to present this new reality. Multinational organizations or regional partners such as UN, SCO, BRICS, SAARC and many others like these can work together to jointly tackle the issue of cyber-security to avoid confrontations between states. Especially these organizations can work jointly to make a mechanism to stop the spread of cyber-terrorism. The 2016 EU Parliament Directive on the Network and Information Security Systems, is a good example for such joint mechanisms in which the EU Parliament initiative focused on cyber-threats to sensitive and critical infrastructure with the aim to improve its countermeasures and enhances safeguarding mechanisms of its online services such as e-commerce, data systems against such digital infrastructures could have severe consequences and can inflict huge operational costs[30]and other services vital to the businesses of its governments and citizens. Any coordinated cyber-attacks

National level

At the national level the recommendations are divided into two categories; the Critical Category and the Future Strategy Category.

- **Critical / Emergency Recommendations:** This highlights the urgent steps required to secure the cyber-space such as;
    - **Broad National Security Policy:** The first critical step for the government is to legislate a broad and comprehensive national

cyber-security policy which must lay down well-defined procedures to tackle the issues of cyber-security. The scope of the cyber-crime bill should be expanded and be part of the national cybersecurity policy. The example of India's National cyber-security policy 2013 can be considered as a guideline model to devise a comprehensive policy.[31]

- **Establishment of National Cyber-Command:** The establishment of a national level cyber-command is very important to handle the issue of cyber-warfare which is considered as part of fifth-generation warfare. The USSTRATCOM is a good example wherein Pakistan the National cyber-command can be established to work under the National Security Council to take all concerned leaders onboard while preparing offensive and defensive cyber-war capabilities. The current NR3C of FIA can continue only to tackle minor cyber-crime.
- **Regulation of Pakistan's Cyber-Space:** Regulation of the current cyber-space is also very critical for the national security of Pakistan as PTA has failed to implement the writ of the state in cyber-space, such as the ban of social media in the past due to the issue of blasphemy. This can be done by devising a comprehensive mechanism with IT industry and LEA to regulate the cyber-space with the standards of ICAN internationally. All the computer and mobile subscriber's records should be properly maintained. The illegal use of untraced IP's, VPN's, Pirated Softwares should be banned.[32]
- **Capacity Building:** The capacity of Pakistan's Law Enforcement Agencies (LEA) should be enhanced in order to deal with new innovation in cyber-crimes. LEA workers should be properly trained and equipped to combat cyber-crimes as the current situation of cyber-crime are very alarming. The forces should be divided into a different areas of operation with regard to harassment, economic embezzlement, terrorism and many other cyber-spheres.
- **Public Awareness Campaigns:** The public should be educated with campaigns and promotions to help them understand their rights and ethics in the domain of cyber-space. Many of the internet users in Pakistan are literally unable to distinguish between the pros and cons of the internet, hence are vulnerable to international propaganda. Daily hundreds of people are scammed through the internet. For this purpose, special promotion and

advertisement campaigns should be launched to help the general public aware, how to keep themselves secure with provided tips and tricks. Seminar and workshops should be arranged to build the capacity of the general public about cyber law. "National Cyber-Security Awareness Day" can be also organized to make people aware of the importance of cyber-security.

- **Future Strategy**
  - **Regulation of Imported Computer Hardware:** Apart from mobile phones most of the computer equipment such as CPUs, hard drives, network switches, routers and many other computer equipment are coming in the country without proper checks and are being used in different important institutions. Factory-built codes and viruses is not a difficult task to implant in these devices. The subversion due to firmware malware at the hardware level is the most difficult to detect and the most dangerous for critical infrastructures. Most of the states, including Pakistan, depend on foreign suppliers to supply computer systems, such as SCADA and ICS. The built-in malware created during the production phase can lead to chaos. The incidents of ban on Chinese mobile phones in Europe with respect to the allegation of hardware spying equipment is a clear example of such level. Consequently, a separate wing of PTA or FIA should be trained to check incoming hardware equipment for spying and viruses before making its way to public or government systems. As an intermediate option, it is necessary to configure the equipment purchased before buying it in operation.
  - **Indigenous Manufacturing of Computer Hardware:** Pakistan must strive to achieve the capacity of producing all components of computer hardware, which are used in different industries particularly in power plants along with network routers, Switches etc.
  - **Broad introduction of Cyber-Warfare in the Curriculum at Secondary and Higher Secondary level:** In Pakistan, primary and secondary level computer books do not have any material on cyber-security. Even at universities level the topic is not specifically discussed. In this regard, the university curriculum should be amended so that our future generations are not dependent on foreign products.

- **Indigenous Development of Software:** Softwares are the main drivers for cyber-attacks. As the computer software is developed in the same languages and platforms, it is easy to master its codes and techniques by using it to exploit the flaws of the other systems developed in the same platform such as Microsoft Windows, Java, Android, Linux, Unix and many others. Relying on foreign software in important institutions especially in unregulated cyber-space like that of Pakistan is dangerous. Hackers are well conversant with these operating systems and by using APT these hackers exploit zero-day exploits. Hence it is imperative these Operating Systems should be customized before inducting. However indigenous development of Operating Systems will prevent any cyber-attack directed against these targets.
- **Narrative Building:** The narrative building includes the encouragement of the state to provide opportunities and scholarships to motivate students to research on cyber-security. There is very little material printed or researched in the field of cyber-security and cyber warfare in Pakistan's higher education institutes. Similarly think tanks should setup to widen and broaden up the research. Currently, there is only one think tank dedicated to cyber security setup in Air University Islamabad in 2017 i.e. National Center for Cyber-Security (NCCS). This is alarming, and the government must tend and encourage other institutes to do so to broaden up the base for cyber-security research.
- **Research and Development:** Technology is constantly changing. Today's decision may be futile tomorrow. In the same way, the threats, their consequences and the capabilities of the attackers are changing rapidly. This requires constant investigation into the most recent threats, the capabilities of the attackers, countermeasures and technical progress. Without R&D, it is almost impossible for any organization to keep up with the ever-changing threat environment. This will require funding and guidance for the implementation of cyber-security R&D requirements.

Conclusion

The world has witnessed a phenomenal growth in cyber-space. The impact of ICT extends to all business areas. Cyber-space is an activator for all other domains and unprotected cyber-space can pose a threat to the economy and safety of any country's national security in the modern era.[33] Many kinds of cyber-threats are

emerging which needs to be dealt at a national level rather at a department level. In the worst-case scenario, Cyber-attacks could affect the territorial sovereignty of the country by interfering with government decision-making systems, causing panic or inadvertent war. The Government of Pakistanis still in inertia for the development of a policy against cyber-attacks. Since 2003, only paperwork is done to build a comprehensive cyber policy and so far, no real implementation has been carried out. Currently, cyber-space is not only abused by cyber-criminals but also becoming a safe and strongest heaven for cyber-terrorists to recruit and use the networks for communication, data collection, psychological warfare and mobilization.[34]

The research highlight that Pakistan is becoming more and more vulnerable day by day to the current and newly developing cyber-threats. The unserious attitude of the governments towards cyber-security is making Pakistan a soft target for cyber-attacks and even at many times the issue is being raised as recently by the DG ISPR in a seminar he urged media workers and journalists to counter the anti-state narrative being spread out on the internet platform which is known as fifth generation and hybrid war that is already being imposed against Pakistan.[35] This clearly points out that the war bells have already rung, and it is critical for Pakistan to start and secure the cyber-space as soon as possible.

NOTES

[1] Zaheema Iqbal, "Cyber Security in Pakistan: Myth or Reality," Eurasia Review, January 12, 2018, https://www.eurasiareview.com/12012018-cyber-security-in-pakistan-myth-or-reality-oped/.
[2] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton, 2003), 29–54.
[3] "Cyber Threats: Implication on National Security," Seminar Report (Islamabad: Institute of Policy Studies, December 18, 2015), http://www.ips.org.pk/pakistan-lags-behind-in-cyber-security-preparedness/.
[4] Sudhi Ranjan Sen, "Centre May Create Single Agency for Cyber Defence," Hindustan Times, November 11, 2019, https://www.hindustantimes.com/india-news/centre-may-create-single-agency-for-cyber-defence/story-pD3QUcNvU2a9THFCF01SMO.html.
[5] Mehwish Khan, "7-Point Action Plan Proposed for Cyber Secure Pakistan," ProPakistani, 2013, https://propakistani.pk/2013/07/09/7-point-action-plan-proposed-for-cyber-secure-pakistan/.
[6] Sana Jamal, "Pakistan's First-Ever Cyber Security Centre Launched," Gulf News, May 22, 2018, https://gulfnews.com/world/asia/pakistan/pakistans-first-ever-cyber-security-centre-launched-1.2225435.
[7] "Cyber Threats."
[8] "Pakistan Blocks Access to YouTube in Internet Crackdown," BBC News, May 20, 2010, https://www.bbc.com/news/10130195.
[9] "Afghan Soil Used for BKU Attack, Envoy Told," DAWN, January 26, 2016, http://www.dawn.com/news/1235516.
[10] "TTP's Support for IS Disturbing for Pakistan," The News, October 6, 2014, https://www.thenews.com.pk/archive/print/640902-ttp%E2%80%99s-support-for-is-disturbing-for-pakistan.
[11] "TTP's Support for IS Disturbing for Pakistan."
[12] "'Terrorist' Killed, Wife Held in Lahore Encounter," DAWN, April 16, 2017, https://www.dawn.com/news/1327252.
[13] Asad Hashim, "Pakistan: Thousands Protest Blasphemy Acquittal, Ignore PM's Call," Al Jazeera, January 11, 2018, https://www.aljazeera.com/news/2018/11/pakistan-thousands-protest-blasphemy-acquittal-ignore-pm-call-181101140852399.html.
[14] "Pakistan Army Called on to Stop 'blasphemy' Clashes in Islamabad," BBC News, November 25, 2017, https://www.bbc.com/news/world-asia-42124446.
[15] Raza Rumi, "Young Pashtuns Have Shown the Mirror to 'Mainstream' Pakistan," Daily Times, November 2, 2018, https://dailytimes.com.pk/199383/young-pashtuns-shown-mirror-mainstream-Pakistan/.
[16] "Online Bullying: Tips for Prevention," American Osteopathic Association, 2015, https://osteopathic.org/what-is-osteopathic-medicine/online-bullying-tips-for-prevention/.
[17] Senator Rehman Malik, "Pak Cyber Security and Cyber Crime," The News, November 19, 2018, https://www.thenews.com.pk/print/395551-pak-cyber-security-and-cyber-crime.
[18] "Card Data of 20,000 Pakistani Bank Users Sold on Dark Web: Report," Dunya News, November 6, 2018, https://dunyanews.tv/en/Crime/465384-Card-data-Pakistani-bank-users-sold-dark-web-report.
[19] "All Cryptocurrencies," CoinMarketCap, accessed December 15, 2019, https://coinmarketcap.com/all/views/all/.
[20] Hanibal Goitom, "Regulation of Cryptocurrency in Selected Jurisdictions" (The Law Library of Congress, Global Legal Research Center, June 2018).
[21] Goitom.
[22] Malik, "Pak Cyber Security and Cyber Crime."
[23] Conner Forrest, "NotPetya Ransomware Outbreak Cost Merck More than $300M per Quarter," TechRepublic, October 30, 2017, https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/.
[24] Robert McMillan, "Siemens: Stuxnet Worm Hit Industrial Systems," Computerworld, September 14, 2010, https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html.
[25] McMillan.
[26] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," The Guardian, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[27] "Prevention of Cybercrime Act 2015" (2016).
[28] National Response Center for Cybercrime (NR3C), is a wing of the Federal Investigation Agency to counter cybercrime according to the constitution of Pakistan.
[29] Elena Chernenko, "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms," Council on Foreign Relations, February 23, 2018, https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.
[30] "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.
[31] "National Cyber Security Policy 2013" (2013).
[32] IP address means Internet protocol address which identifies a specific user on internet. VPN is Virtual proxy network which is intended to route data through a proxy server.
[33] Nasir Jamal, "Cyber Challenges to Nuclear Infrastructures" (National Defence University, 2017).
[34] Iqbal, "Cyber Security In Pakistan."
[35] "DG ISPR Urges Media to Show Progress, Potential of Pakistan," Geo.tv, December 6, 2018, https://www.geo.tv/latest/220948-dg-ispr-holds-press-conference.