P-ISSN: 2709-6254	Journal of Development and Social Sciences	Oct-Dec 2022, Vol. 3, No. 4
O-ISSN:2709-6262	http://dx.doi.org/10.47205/jdss.2022(3-IV)58	[631-640]

Journal of Development and Social Sciences
www.jdss.org.pk

RESEARCH PAPER

The Rise of Cyber Crime in Pakistan: A Threat to National Security

[1]Dr. Muhammad Imran [2]Dr. Ghulam Murtiza*
[3]Muhammad Sulyman Akbar

1. Assistant Professor, College of Law, Government College University Faisalabad, Punjab, Pakistan
2. Assistant Professor, College of Law, Government College University Faisalabad, Punjab, Pakistan
3. Lecturer, College of Law, Government College University Faisalabad, Punjab, Pakistan

***Corresponding Author:** ghulammurtiza@gcuf.edu.pk

ABSTRACT

This research paper investigates the unprecedented and rapidly growing threat of cyber space and cyber warfare to Pakistan's national security in the context of non-traditional dangers. Utilizing a descriptive approach and qualitative data collection method, the study analyzes various secondary sources, including books, articles, and internet search engines, to understand the current state of cyber security in Pakistan. The findings reveal that Pakistan faces multiple cyber threats from nations such as India, Russia, Israel, the United States, and China, and lacks advanced information technology (IT), effective policy implementation, and adequate educational progress in IT. The paper concludes that Pakistan must prioritize the development of cyber space technology, enhance advanced technology, educate its population in advanced IT, and learn from first world nations' cyber security strategies to protect its government, financial system, military locations, and citizens' personal information from cyber threats. Proper implementation of existing laws, policies, and penalties is also crucial to mitigate hacking and other forms of cyber-crime, ensuring a more secure digital future for the nation.

KEYWORDS Cyber Dilemma, Cyber Security, Cyber Terrorist, Cyber-Attack, Cyber-Crime, Hacking-Aggression

Introduction

Non-traditional dangers are less of a concern as we approach the new century compared to those that are already well-established. The danger presented by cyberspace is unprecedented and unheard of, despite the fact that it is rapidly spreading across the globe. In the 1980s, British science fiction books first introduced the concept of cyberspace (Betz & Stevens, 2021). However, in 1992, the term “cyber usage” referred to activities carried out with the use of computers and computer networks such as the internet. The so-called “information age” has only just begun, yet there is already the potential for theft of data and information in both digital and physical forms. There is very little respect for national borders, and data theft seldom gets reported. To put it more simply, it is something that cannot be seen directly. After waiting for thirty years, cyberspace is now being included in military plans. We can no longer continue the farce of pretending that the computer, global network, and software applications that we use to access the internet are restricted to the exclusively digital environment. However, the internet is a hybrid of the personal computer, the television, and the telephone. Everything has its own air signals and weirs to regulate traffic. The proliferation of cyberwarfare in today's world may be directly attributed to the current information and communication technologies that have emerged in recent decades, which move fights away from the conventional battlefields of air, land, and sea and into the domain of the virtual world that is the Internet. According to John Perry Barlow, in order to enter (cyber)space, one must “forsake both body and location and become a creature of words alone.”

After dealing with traditional threats, Pakistan is now confronted with an innovative and non-traditional one in the form of the internet (land, sea, and air). When it comes to the

internet, Pakistan and India in Asia have some disagreements with each other. All facets of Pakistani society, including the country's armed forces, government, financial system, and digital economy, are ramping up their usage of cyberspace. In recent years, Pakistan has not made any significant strides in either education or technology. It is generally known that Pakistan has recently placed a higher priority on the fight against terrorism compared to the growth of its information technology (IT). Cyber warfare, also known as fifth generation warfare, poses a significant threat to Pakistan's national security. Pakistan is among the most susceptible countries in the world to this kind of conflict. Pakistan continues to feel the effects of a lack of information security, as well as the effects of minor cyberattacks and expanding cyber-crime. Pakistan's laws and regulations regarding cyber-crime are not being adequately enforced, despite the fact that the country has in place effective policies, norms, and decision-making processes, as well as legislation. In this regard, Pakistan must exert a great deal of effort.

Literature Review

According to Hussain (2022), the first individuals to create cyberspace did so to increase worldwide communication and make it simpler for diverse building systems to collaborate. Almost half of the world's population could connect to the network and utilize it to send and receive data. New cyber threats make it more difficult for governments throughout the world to execute their tasks and may endanger people's lives (Hussain, 2022). Cyber security has been discussed since the late 1980s. It gained popularity in the 1990s, and the concept has now expanded too many other nations. Around the middle of the 1990s, several nations realized how a worldwide networked software system may impact their national security and industrialized economies, and cyber security became a major political priority. The growth in online threats that has resulted is a huge danger to people's safety, prosperity, and feeling of community. It has also been demonstrated that any system linked to the internet may initiate cyber assaults. No one knew who this unexpected foe was or if it belonged to a country at the time. Nowadays, it is simple to obtain a complicated hacking tool that is equally simple to use. According to Cavelty (2010), this manner of thinking about dangers can easily turn minor issues into major security issues. People frequently use the terms “cyberspace” and “internet” interchangeably, despite the fact that “cyberspace” refers to “the internet” and “the internet” refers to "a part of cyberspace" (Cavelty, 2015). However, Yamin (2014) refers to the globe as a “virtual global village” since so many individuals have internet connection. According to him, the term “cyberspace” refers to the electronic environment enabled by computer command and control. This includes, but is not limited to, Internet use and electronic mail.

According to Tariq, Aslam, Rashid, and Waqar (2013), the National Cyber Security Division would be located in the Prime Minister's Secretariat. This section would be in charge of coming up with computer security strategies, policies, and laws. The Computer Emergency Response Team (CERT) will be part of the Ministry of Information Technology. Its job will be to deal with and handle cyber security incidents. Scholars agree that the area of cyber security has not yet reached a level of full understanding and safety that is good enough.

This talk goes into detail about the many threats to cybersecurity in Pakistan and the steps that have been taken to reduce these risks. The National Cyber Security Policy of 2021 could threaten the safety and well-being of the Pakistani people as a whole. Because they aren't being used, computer security standards aren't good enough as they are now. Tariq, Aslam, Rashid, and Waqar (2013) made a top-down organizational system to make it easier to start well-known cyber security businesses at different levels of the hierarchy. Two government organizations would be in charge of keeping the digital assets of the country safe. It is part of the PM Secretariat and is in charge of making cyber security strategies, policies, and laws. The Ministry of Information Technology is in charge of the second organization, the Computer Emergency Response Team, which is in charge of reporting on

computer incidents. The evaluation of Pakistan's 30 most recent cyber defense measures poses a danger to both national and personal security. However, researcher like Khan (2019) has pointed out that the current cyber security guidelines aren't very useful and can only be used in limited ways. Because of this, Pakistan needs to set up a thorough response system to protect itself from such risks (Tariq, Aslam, Rashid, and Waqar, 2013). There is also an urgent need for training programs to teach people about cyber risks and the possible effects of using technology without any rules.

Research Methodology

Material and Methods

This research paper design adopts a descriptive approach, as it seeks to investigate and elucidate a specific topic, simultaneously offering supplementary information pertaining to the subject matter. Utilizing a qualitative data collection method, the research paper relies exclusively on non-numerical data derived from various literary sources. In order to gather pertinent information and insights, this study employs a range of secondary sources, including books, articles, and internet search engines, thus enabling a comprehensive understanding and analysis of the topic under investigation.

Theoretical Framework

The three primary ideas covered during the course of this article are securitization, offensive realism, and defensive realism. When it comes to the concept of offensive realism, John Mearsheimer is the one who came up with the term for the very first time. In addition, when it comes to defensive realism, Kenneth Waltz is in a league of his own. According to these hypotheses, having access to sophisticated and cutting-edge weaponry makes it less likely that one state would engage in an arms race with another or be attacked by a third nation (both conventional and non-conventional). However, offensive and defensive realists agree that there is a significant chasm in the realm of international affairs. The use of defense and attack principles in national foreign policy can be beneficial. There are instances when countries choose to use aggressive strategies to further their own goals (deployment, proxy conflicts, and economic downfall of any nation).

People who subscribe to the aggressive realist point of view believe that the national security of other nations is being put in jeopardy on purpose. There would not be a worldwide war if nations did not coerce their populations into going to war for their own self-interests, but they do (Shiping, 2018). The doctrine of defensive realism holds that there is no deliberate attempt to undermine the safety of the state. One should not assume that resorting to force is the only option to resolve international disagreements; nonetheless, strengthening military and defense capabilities makes a country better prepared for any future conflicts that may arise. It is worth considering that alternate options, such as company structures and alliances, are available instead.

In light of the fact that cyberattacks are still a relatively new concern for Pakistan and the rest of the globe, it is important that this study includes both offensive and defensive measures. Therefore, it is essential for a nation to possess the tools necessary to protect the cyber infrastructure of the nation. The second kind of weapon is one that is used in an assault over the internet. The defense of their country's economy, population, private information, and data is one of their highest priorities. This objective can be accomplished with the use of cutting-edge, protective IT and a cyber defense system force (i.e., educate, select, and hire skilled hackers and give them government jobs so they can contribute to national stability). At that point, Pakistan's position towards its cyber security is seen as defensive. After a government has built up its cyber defense capabilities, it should be granted permission to utilize offensive cyber systems and the authority to destroy other countries' defensive cyber capabilities. The private information of people should then be gathered and used for the sake of national security as well as other governmental objectives. In light of the adage that “the

best defense is a good offense," Pakistan needs to place a high priority on the development of both offensive and defensive cyber systems to guarantee the protection of its population.

The third conceptual framework used here is the securitization theory, which was conceived at the Copenhagen School and relies on the collaborative efforts of academics such as Barry Buzan and Ole Waever. The origins of the idea of securitization in the realm of creative activity can be traced back to this ideology (Hadi, February 2, 2018). This idea presents a somewhat uneasy feeling. The Securitization Act can be broken down into four primary portions: 1) A person or organization that securitizes a security is referred to as a securitizing actor. (2) An existential risk in the form of a potentially hazardous item has been uncovered and is being investigated. Thirdly, a referent object is anything that must be protected since it is in jeopardy. Fourthly, a group that must be educated about possible dangers to their safety and should be the focus ofthe campaign.

As a direct consequence of implementing this strategy pertaining to the fifth dimension of fighting (cyber warfare), the Pakistani state has determined that cyberspace poses a threat to national security, identified the threat as existential in nature (an attack from cyberspace), and targeted the referent object (the critical infrastructure of cyberspace). As a result, the Pakistani government decides that it is necessary to take precautionary measures to protect against the threat. Finally, the audience that is supposed to receive this message (Pakistan) begins to take action to strengthen its cybersecurity and better protect itself against harmful actors (civilian-military bureaucracy).

Cyber Space Warfare Globally

Cyberspace significantly alters many facets of human existence, including culture, economics, and military forces, to name just a few areas. The protection of global security is susceptible to threats posed by commercial or digital economic activity. For example, if a country is subjected to a military assault, another nation can respond in kind by launching an attack of its own. It is challenging to establish a consistent response regardless of the objective of a cyberattack, whether that goal is online banking, online shopping, military data, or government websites.

As computers do not have free will, this becomes common knowledge over time. A single individual is in charge of everything and uses a computer to carry out their instructions. This person is human. However, a danger to national security may be posed by governments and their cyberforces (people) when they use this technology for unethical purposes and adhere to contrasting political views. Cyberwarfare capabilities, data storage infrastructures, and security protocols are standard components of a modern industrialized nation's military arsenal.

Thus, the relationship between armed conflict and technology, guided systems, command and control, and other related concepts is crystal clear. Cyberattacks were used for the first time as early as the "Gulf War" in 1991. During the conflict in the Gulf of Oman, the United States disabled Iraq's air defense system with the use of a computer virus known as AF/91. Using Jordan as cover, spies from the United States of America transported a virus concealed in a printer chip into Iraq. The Iraqi air defenses were rendered ineffective as a result of this malware.

A cyberattack known as "Titan Rain" was launched against the United States of America by Chinese hackers in 2005. According to Hadi (2018-02-02) page 65, this had a significant impact on Lockheed Martin in Florida, which specializes in aircraft technology. This attack was classified as an "Advanced Persistent Threat" (APTs). The People's Liberation Army sanctioned the strike as an act of espionage (PLA). In 2009, the technology that would later become known as GhostNet was discovered. This, too, was manufactured in China. The hack resulted in attacks on the media, the economy, and the government. Targets included diplomatic missions from several countries and nonprofit groups. The United

States often has private business agreement papers stolen by China, and China then exploits such materials in cyberattacks, which is harmful to the American economy.

A range of attacks occurred very recently, the first of which came from Russia in 2007 when it began assaulting Estonia online. Throughout the month, Russia carried out several cyberattacks on institutions located in Estonia. As a direct consequence, Estonia could not perform any domestic or international internet transactions, which had a cataclysmic impact on the country's economy.

On July 20, 2018, Russia began an invasion into Georgia that had been planned for some time. The origins of this assault can be traced back to Estonia. The attack was launched by a computer infected by a virus and turned into a zombie. As a direct consequence, several websites, including those belonging to the Georgian president and television stations, were rendered inaccessible for an entire day.

The most recent and severe attack, which took place in 2010, was known as Stuxnet. It was the culmination of a new wave of cyberattacks that had been building up for years. The dangerous computer worm, known as Stuxnet, targeted Iran's supervisory control and data acquisition (SCADA) system, causing damage to the country's nuclear program. After Iran achieved nuclear capability, a photograph was released showing the country's president seeing the facility that houses the nation's nuclear arsenal. The United States of America learned the secret code for the SCADA box located behind the president as a resultof this image. The United States government used this code to introduce a virus into Iran's nuclear program. This attack had direct government support. Both the United States of America and Israel have since come clean and admitted to cooperating on the development of the worm.

India, which has more advanced IT than Pakistan, has conducted cyberattacks against Pakistan. Pakistan's attack on Pakistani government and military institutions in 2010 was given the codename “Operation Hangover.” India targeted Pakistani government and military institutions in 2010 (Chandio, August 13, 2020). The second attack, attributed to the “Black Dragon Indian Hacker Squad,” targeted Pakistani websites of the Pakistan Peoples Party (PPP), Pakistan Railway, National University of Modern Languages (NUML), Quaid-e-Azam College Gujranwala, Pakistan Electric Power Company, and the National Manpower Bureau.

Threat To Pakistan National Security

According to our research, nations across the globe such as Russia, China, India, and the United States (which also have an impact in south Asian countries such as Iran and Iraq) are more advanced in cyber space technology (Nevill, 2016). Therefore, the progress that these nations have made in IT poses a significant risk to the national security of Pakistan. Pakistan is now dealing with a crisis in terms of its cyber security. It is common knowledge that the government of Pakistan is concentrating its efforts, under the National Action Plan(NAP), on combating terrorism and extremism. Pakistan did not give the growing non-traditional danger known as “cyber warfare” any consideration. In Pakistan, the number of cases of cyber-crime is continuously increasing. There are 15 million people using mobile phones and 30 million people using the internet in Pakistan. According to the statistics provided by the CyberCrime Unit (CCU) of the Federal Investigation Agency (FIA) the year wise inquires conducted for Cyber-crimes are as follows (Akhlaq, 2021).

Table 1
The year wise inquires conducted and No. of Cases Registered for Cyber-crimes in Pakistan

Year	No. of Inquires	No. of Cases Registered
2016	514	47
2017	1290	207

2018	20295	255
2019	11389	1071

Akhlaq, M. (2021). Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan. *PCL Student Journal of Law*, *5(1)*, 17.

It was also revealed that overall only 14 convictions were made in 5 years (2015-19), (shehzad, 2020) this raises a question markon the effectiveness of Prevention of Electronic Crimes Act (PECA) of 2016, as a law and also on the efficiency of Cyber-crime wing of FIA toproperly prove the crimes on the accused. PECA grants punishment of sentences in jail and fines also (Akhlaq, 2021).

Causes and Challenges To The Security Of Pakistan

Causes

The majority of Pakistan's banking and other financial institutions are in the process of migrating their customer-facing operations away from analog hardware and toward digital networks and web-based services. However, there is not yet a reliable mechanism in place at financial institutions to detect when accounts have been hacked. Because of this, hacking ATMs has become the most significant and pervasive problem. Skimmers are a kind of gadget that may be covertly inserted in automated teller machines (ATMs) by hackers in order to steal bank card information. Hackers posted a message saying "your system is insecure" on the website of a Pakistani bank that had been hacked, similar to Allied Bank. According to the banks, since they are covered by insurance, they are not worried about the introduction of new data security instruments. The people of Pakistan, on the other hand, are the ones who are feeling the repercussions of these cyber-attacks.

Sadly, the government of Pakistan does little to encourage its population to become more knowledgeable about IT or to assist the expansion of the country's IT industry. In light of the fact that Pakistan only spends 1% of its Gross Domestic Product (GDP) on research and development, the nation's information technology sector is in desperate need of attention.

Cyberwarfare between India and Pakistan is a more perilous and challenging kind of combat than the conventional form of confrontation between the two countries. Pakistan devotes far less attention to scientific research and development in comparison to India, which makes a significant investment in cutting-edge technology. When compared to Pakistan, India's level of technological advancement is far higher. Both nations have their own cyber armies and often hack one other's websites. However, when contrasted with India's military might and technological prowess, Pakistan's military might and technology come up short.

A Pakistani organizationnamed Information Security Association (PISA)is leading the way in the promotion of a cyber effort. Meetings and training sessions are planned and run independently by PISA. The government, on the other hand, gives such information very little consideration.

In Pakistan, the government has established an agency known as the "National Response Center for Cyber-Crime," which investigates and prosecutes incidents of cyber-crime. Despite the fact that this group is working to battle terrorism, financial problems, and information delays, the general public is unfortunately ignorant of its existence. Even though the Federal Bureau of Investigation (FIA) is working to reduce instances of cyber-crime on many platforms (including Facebook, Google, Twitter, and Skype), its success is impeded by a lack of legislation and enforcement.

Challenges

The deterioration of Pakistan's cyber security situation represents an increasingly serious danger to the country's overall safety. The growing reliance that Pakistan has on the internet puts the country in jeopardy and gives rise to a number of problems.

The Pakistani government has limited access to certain of these websites, such as YouTube and Torrents, because they include content that the government deems to be offensive. Users were still able to access these sites by using virtual private networks (VPNs) and other programs. As a direct consequence of this, the predicament facing the state is very precarious.

The Pakistan Telecommunication Agency (PTA) was founded by the Pakistani government with the intention of ensuring the country's continued connectivity PTA. This agency banned 15,380 websites or links in 2022 or 2013 for containing some undesirable content, however it did not include YouTube on its list; as a result, the situation for the state is concerning and not particularly effective.

More precisely, the 13.5 billion communications that were transmitted and received by email, phone, and fax when the NSA was undertaking cyber and hacking operations to monitor Pakistani communication infrastructure. These messages were sent and received during the time period in question. Pakistan is in second place on this organization's priority list, behind Iran. This is a terrible possibility that puts Pakistan's independence at jeopardy.

The internet and banking done over the internet are becoming an increasingly important component of Pakistan's financial sector. However, they do not have an adequate security mechanism, which leads to a regular occurrence of data breaches. The internet banking system is losing users' confidence at an alarming rate. As a direct consequence of this, there is a significant threat to Pakistan's digital economy.

It is not uncommon for terrorist groups to possess both highly skilled IT personnel as well as cutting-edge gear at their disposal. After that, they began conducting cyber bombings, also known as attacks on computers over the internet.

The National Database Registration Authority (NADRA) is also in danger due to the fact that certain Pakistani hackers have said that this website's security is lacking in various areas. This website needs to have a higher level of security implemented immediately. Taking into account the political difficulties that exist in that region of Pakistan.

Hackers in Pakistan are increasingly engaging in malevolent behavior, and this is becoming more normal. The websites that the Pakistani government maintains are often hacked and defaced, which makes it impossible for the government to access the websites. The only element that may be considered a contributor is the fact that Pakistan does not have access to any sophisticated cyber technology. These dangers come from both the interior and the exterior of the building.

Cyber Warfare Against Pakistan And Other Muslim Countries

Propaganda against Muslim countries, especially Pakistan and other Muslim nations, has already started to be spread by Western states. The West would prefer that no Muslim country ever acquires nuclear weapons since this is something they see as very dangerous. This is an idea that Israel vehemently opposes, which is why it is making preparations to fight a cyberwar against Islam and Muslims. According to a video produced by Vice News, Israeli Prime Minister Benjamin Netanyahu is reported as claiming that his country is "spending a lot of money on cyber defense and offensive effort." And when it comes to the top five countries in terms of cyber technology, we come in first. Israel spent a total of 1,500,000 dollars in order to obtain information about the military plans and actions of Pakistan. Additionally, the Washington Post and the New York Times should join the BBC

and FOX News in disseminating falsehoods regarding Pakistan's efforts to build nuclear weapons. There is a lot of misinformation going around online that claims the Pakistani nuclear program is under the direction of Al Qaeda and the Taliban rather than the Pakistani military. This propaganda can be found here. In addition, they spread misleading information regarding Pakistan's nuclear development. Following the events of September 11, 2001, Western nations pointed the finger of blame at Pakistan for acts of terrorism and said that Pakistan was the only nation that harbored terrorist organizations. Therefore, cyberwarfare is a significant danger for Pakistan. Pakistan is addressing the issue because it is aware that, after an assault, it cannot credibly accuse the other countries of having launched an unseen strike on Pakistan. As a result, Pakistan is aware that it cannot credibly accuse the other countries of having launched an unseen strike on Pakistan. As a result, we have to give our defensive strategy some fine-tuning. Alter our defensive approach so that it becomes an offensive one.

Cyber Laws In Pakistan

In Pakistan, having rules and regulations in place is not very noteworthy. And the people of Pakistan are not aware of the rules and regulations that govern their country. The Electronic Transaction Ordinance 2002 was the first measure to be passed in Pakistan. This ordinance deals with the banking system. But the first prospective measure to pass in 2007 was called the "Pakistan Cyber-crime Bill." It focuses on electronic crimes like as cyber terrorism, illicit access to electronic systems, electronic forgery, electronic system fraud, and abuse of encryption, among other things. subsequently, with the introduction of the "Prevention of Electronic Crime Bill 2020" in 2020, which was the first comprehensive legislation of its kind ever, some adjustments were made to this measure in 2016 as Prevention of Electronic Crimes Act (PECA) of 2016. Therefore, Pakistan has appropriate laws on cyber-crime and penalties that are addressed in legislation; nevertheless, Pakistan does not have appropriate execution on these laws. In addition, they do not possess advanced technology, a cyber force, or awareness.

Findings

- Pakistan is facing a multitude of dangers on a global scale, including those posed by cyber space and cyber warfare from India, Russia, Israel, the United States, and china.
- There is a lack of cutting-edge IT in Pakistan. Pakistan needs to be obligated to make progress on it.
- The Pakistani administration takes little notice of the dangers posed by cyber or space warfare from a political standpoint.
- Pakistan is not making progress in the technology battle because its educational establishments are not advancing in IT.
- Economic risks associated with hacking on the internet carried out by other nations. Because Pakistan lacks both institutions and an adequate cyber force, the country now struggles with a cyber security crisis.
- Prior to this point, there has been a very low amount of research conducted on the subject of the cyber danger to Pakistan's national security.
- There is a very limited amount of information accessible on the internet system of Pakistan due to the fact that Pakistan does not have advanced technology.
- No institutions that are responsible for cyber-related issues are mentioned anywhere in this article. The cyber space realm is something that Pakistan has to focus a lot of attention on.

Conclusion

In the event that Pakistan experiences new obstacles regarding its cyber security, it will be necessary to develop robust plans and policies in order to protect the nation's safety. It is common knowledge that Pakistan is now suffering a problem with its cyber security. Because of Pakistan's advanced technological capabilities, a number of nations, including India, Russia, and the United States, are interested in bringing the country to its knees. In order to develop its cyber space army, Pakistan should focus more on offense than defense and adopt a more aggressive strategy. Develop the appropriate guidelines and techniques to defend against the onslaught from cyberspace. The ability to assist oneself is also highly significant and may resolve very modest issues. In order to protect its government, financial system, military locations, and citizens' personal information from cyber thieves, Pakistan has to strengthen its cybersecurity.

Although Pakistan has laws, enacted bills, policies, and penalties, these laws and policies are not being properly implemented in Pakistan. Although Pakistan has laws, passed bills, policies, and punishments. Therefore, hacking and other forms of cyber-crime are becoming more common. The Indian cyber army, armed with more sophisticated technologies, often breaches Pakistani websites.

It is imperative that Pakistan prioritize the development of cyber space technology, as well as the enhancement of advanced technology and the education of their population in advanced IT. Pakistan must to be required to learn from first world nations how they handle challenges of cyber security and implement such lessons locally. Observe the measures they take to protect their digital economic system. And model your own policies after theirs.

Recommendations

- Pakistan must become a party to both international and bilateral conventions concerning the protection of cyber space. Since they will assist Pakistan in making its digital system more effective and safe, and because Pakistan has acquired more advanced cyber technologies from foreign states.

- Many skilled individuals in the art of hacking and hijacking may be found in Pakistan. However, they put their skills to bad use by engaging in illegal activities such as theft and cyber-crime. However, if the government were to choose such individuals and put them to productive use, such as in the field of development, research, or a safe and sound cyber security system, the situation would be different.

- Education in IT is something that is much required here. Therefore, studying computer science need to be a requirement both in high schools and in colleges. In this way, our future generation will be able to understand computers and know how to combat crimes committed online.

- The government has established legislative committees in order to ensure compliance with cyber legislation.

- Each and every public and commercial company and institution should also have expert teams to deal with the increasing number of cyber-attacks. In addition to this, they should have cooperation with the institutions of the government.

- The government ought to put effort into the study and development of cutting-edge technologies in the sphere of cyber space.

- Pakistan also has to build its cyber force in order to improve its first- and second-strike capabilities.

References

Akhlaq, M. (2021). Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan. *PCL Student Journal of Law*, *5(1)*, 1-37

Betz, D. J., & Stevens, T. (2021). Cyberspace and the State: Toward a Strategy for Cyber-power. *Adelphi Series*, *51(424)*, 9-34.

Cavelty, M.D. (2010). *Cyber-threats*. In M.D. Cavelty, & Victor Mauer, *The Routledge Hand book of Security Studies* (pp. 180-188). London: Routledge.

Cavelty, M.D. (2015). *Cyber security.* In *A. Collins, Contemporary Security Studies* (4th ed., pp. 400-415). Oxford: Oxford University Press.

Chandio, K. (2020). Cyber Security / Warfare and Pakistan. *Islamabad Policy Research Institute*. 1-6

Ehsan M. K. (2018, Feb 01). Hybrid Warfare: A Conceptual Perspective. *Hilal magazine*,

Hussain, A. (2022, January 16). Should Pakistan have a cyber army? *The Express Tribune.*

Khan, U. P., & Anwar, M. W. (2020). Cyber security in Pakistan: Regulations, Gaps and A Way Forward. *Cyber politik Journal,* 5(10), 205-218

Lodhi, M. 2021. *Pak beyond crises state. london: oxfored.*Oxford University Press Karachi.

Nevill, L. (2016). *Challenging Opportunities for the Asia-Pacific's Digital Economy*. In C. Samuel, & M. Sharma, Securing Cyberspace: International and Asian perspectives (pp. 221-231). New Delhi: Pentagon press.

P.Liff, A. (2022). Cyber war: A new absolute weapon? The Profliferation of Cyber Warfare and Interstate War. *Strategic Studies* (35), 401-428.

Rasool, S. (2020). Cyber Security threat in Pakistan: causes challenges and way forward. *International Scientific Online* (12), 21-34.

Rizwan S. (2020, July 20). Only 14 cyber-crime convictions in five years. *Tribune Pk.*

Shiping, T. (2018). *From Offensive to Defensive Realism: A social Evolutionary Interpretation of China's Security Strategy*. In R. S. Ross, & Z. Feng, *China's Ascent Power Security and the Future of International Politics* (pp. 141-162). New York: Cornell University Press.

Syed A. H. (2018, Feb 01). Securitization of Cyberspace: the debateable contours of cyber warefare. *Hilal Magazine*

Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013, December). Cyber threats and incident response capability-a case study of Pakistan. In *2013 2nd National Conference on Information Assurance (NCIA)* (pp. 15-20). IEEE.

Yamin, T. (2014). *Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan (No. SAND2014-4934)*. Sandia National Lab. (SNL-NM), Albuquerque, NM (United States).