PalArch's Journal of Archaeology of Egypt / Egyptology

CYBER SECURITY SITUATION IN PAKISTAN: A CRITICAL ANALYSIS

Zain Ul Abiden Malik[1], Huang Min Xing[2], Sundas Malik [3], Tayyab Shahzad[4], Min Zheng5, Hani Fatima [6]

[1] Postdoc Researcher, Institute of Middle Eastern Studies, Northwest University, Xian, China

[2] Professor, Institute of Middle Eastern Studies, Northwest University, Xian, China.

[3,4] Visiting Lecturer in Pakistan Studies, PMAS Arid Agriculture University, Rawalpindi, Pakistan.

[5] Ph. D Scholar, Institute of Middle Eastern Studies, Northwest University, Xian, China.

[6] Ph. D Scholar, School of Experimental Economic in Education, Shaanxi Normal University, Xia'n China.

Email: [1]Zainulabidenmalik786@gmail.com

Zain Ul Abiden Malik, Huang Min Xing, Sundas Malik, Tayyab Shahzad, Min Zheng, Hani Fatima. Cyber Security Situation in Pakistan: A Critical Analysis -- Palarch's Journal of Archaeology of Egypt/Egyptology 19(1), 23-32. ISSN 1567-214x

Keywords: War, Cyber Security, Pakistan

ABSTRACT:

The "art of war" is an ever-changing concept and a method how to engage the enemy, when and where. Not only for nations, but also for the private profit-driven society, a relatively new challenge is emerging globally. Billions of dollars are diverted or stolen illegally, privacies revealed; state secrets obtained, and hacked into vital public infrastructure. This is the cyber security domain. As the world becomes increasingly linked through the internet or digitized by information technology, cyber technology becomes increasingly connected. Threats to security are rising day by day. Pakistan is no exception to that theory. In the cyber domain, a nuclear state with a major geopolitical role is increasingly exposed to such challenges. Pakistan has a broad base of internet users, a growing digitized security apparatus, and a banking system that relies on internet

connectivity. Pakistan has also adopted legislation to counter cyber-attack risks that do not seem to cover threats in scope and wholeness.

INTRODUCTION:

Ever since the advent of computers Virus problems were there... The sanctity of data was never thought until the exponential growth of data. The Internet, the exposure on the Internet of too many computers offers a true sandbox for cybercrime committers to test their skills to shut down websites, steal data or commit fraud. Cybercrime is, therefore, a concept that defines any criminal activity committed as the primary means of commission and theft by using a device. The US Department of Justice is widening the scope of cybercrime to cover any criminal activity that stores evidence using a device. Invading and distributing computer viruses as well as new computer-based versions include crimes that can be committed by computers (such as the Internet). Crimes such as identity theft, stalking, intimidation and terrorism have become people and nation-based (Gade, 2014).

Type Of Threats:

Cybercrime comes in a range of ways, from website denial of service attacks to fraud, blackmail, extortion, exploitation, and destruction. These methods are varied and may include Malware, ransomware, spyware, social engineering, and even modification of physical systems (for example, ATM collectors). The fact is: almost anything that can be technically controlled will have a place to be in danger. In recent years, everything from cars (Greenberg, 2015) to medical equipment (Zetter, 2015) to toys (Gibbs, 2015) has been shown to be a victory for someone with little experience, from time-to-time Opportunity.

Russia And Georgia Cyber War:

During the military struggles in 2008 that culminated in the Russian invasion of Georgia. The Russian government was accused of targeting or promoting organized criminal assaults on official websites in Georgia. Russia has a broad definition of information warfare, including intelligence, counterintelligence, deception, misinformation, electronic warfare, communications weakening, navigation support deterioration, psychological coercion, information systems degradation, and propaganda(2014, Smith). The Russian invasion of Georgia was followed by an intense build-up of cyber-attacks aimed at disrupting and taking down vital Georgian governmental and civil online infrastructure. On the eve of the invasion, these attacks became a major assault that led to the capture of separate parts of Georgian cyberspace by blocking, re-routing of traffic and power. In the history of warfare, the attack marks a new point, being the first case in which a land invaded was coordinated with an online cyber offensive orchestrated. This provides strategists and planners with critical lessons while providing important details about how the Russian Federation is improving its Internet offensive capabilities.

Russia And Georgia Cyber War:

In 2009-2010, allegations emerged that in order to disable Iranian nuclear plant centrifuges that could be used to make weapons-grade enriched uranium, a sophisticated government-created computer worm named 'Stuxnet' was released. The worm was developed by the governments of the United States and Israel and a programming error allowed it to be propagated on the internet around the world (Broad, Markoff & Sanger 2011). The Stuxnet worm has targeted and penetrated over fifteen Iranian installations. This assault is believed to have been triggered by the USB drive of a random worker. The Natanz nuclear installation was one of the industrial installations affected. The first signs are that a problem occurred in the computer system of the nuclear facility in 2010. Visiting the Natanz site, inspectors from the International Atomic Energy Agency found that a strange number of uranium enriching centrifuges were breaking up (Kesler, 2011). At the time, the cause of these failures was unclear. Later in 2010, information security experts in Belarus were hired by Iranian technicians to test their computer systems. Eventually, this security firm found several malicious files on Iranian computer systems. These malicious files were eventually discovered to be the Stuxnet worm. While Iran has not yet released the impact of the attack, it is currently estimated that the Stuxnet worm destroyed the enrichment of 984 uranium. Only centrifuge. This decreases the productivity of concentration by 30 percent, according to current estimates (ibid).

Cyber-Attacks on NATO by Russian Hackers:

In Microsoft's Windows operating system, an undisclosed vulnerability exists that can be used to track NATO, the Ukrainian government, and a Russian hacker community that may work for the government. Researcher at American University and other priorities for national security (Nakashima, 2016). Western military officials said Russia did so by manipulating almost all of the Allied forces' weaknesses: their personal smartphones, opening up a new NATO front. Military cyber espionage experts say drone flight and cell phone data collection suggest that Russia is attempting to track the troop level of the new NATO base to see if more troops are present. Cybersecurity researcher Lonnie Benavides DocuSign says Russia has a favorable cybercrime environment-whether it's fraud, such as theft of credit cards or spying to steal state secrets, because there's a brilliant hacker who won't be prosecuted. Cases in other countries should be reduced, and some cyber-attacks/hacking incidents in Pakistan should be listed.

Warfare Cyber:

Cyber warfare, once the world of science fiction, is now quite plausible, and now the military cyber warfare division is committed to most superpowers. Many western nations now view cyberspace as another military area, in addition to land, air and sea. Although there were few identified, and organized, we don't need a crystal ball to foresee the future of cyber-attacks on physical targets, and they will

only increase. It informs us that we are now in an era of cyber-espionage, cyber-warfare, and cyber-terrorism in which states, political parties, criminals and companies will participate. Right now, we live in a world where war can be fought almost entirely-even if the results are almost always different in the real world. As nuclear weapons have changed the balance of power in many foreign affairs since the beginning of the 1950s, the electronic warfare of the nation-state would become an equalizer (MaAfee Lab, 2015).

Cyber-Attack Targets:

Cyber-attacks increased by 24 percent globally in the second quarter of 2017 compared to the first three months of the year the manufacturing industry is the most targeted. In addition to three recordings in the second quarter compared to the manufacturing sector, producers also appeared in the top target in five of the six regions of the world in 2016.) and health care (13 percent) as the most targeted sectors. Banks are also heavily targeted by cyber criminals. Ten years have passed. Cyber-crime pays huge sums of money to financial institutions as they fight fraud and direct theft. One report states that banks spend three times as much on cyber protection as non-financial institutions, and there is an agreement among banking regulators in the workplace that cyber-crime becomes a "legal threat" to financial stability. (Lewis, 2018) While the number of media attacks and entertainment has declined somewhat from last year (39 percent), it remains one of the most prominent targets. As audiences around the world increase their demands for faster access to quality content and the ability to view content anywhere on any device, the news and entertainment industry is becoming increasingly popular with hackers who want to steal anonymous personal information (PII). The news and entertainment industry also caters to hijackers seeking recognition or recognition. While the internet and telecom industry is one of the main targets of DoS attacks, research shows that a large percentage of these attacks were on the sports website, linking a portion of the highly targeted sports industry. These connections can easily lead to the internet and telecoms and quickly come up with a highly targeted list. Also, the internet and telecom rely heavily on the reputation of durability and overtime. Any levels of drop-in service can have a significant impact on the bottom line.

Where Is Pakistan Going to Stand?

The expansion of the cyber room, including the advanced use of information technology (IT) and telecommunications (Telecom), empowers hackers to misuse and disrupt cyber use. The risk of hacking has also increased to the point where they can voluntarily disable their networks. If the financial system, power grid, transport and military command and land management system were disabled, think about what would happen. Millions of cyber-attacks on infrastructure and services have occurred in recent years. Hackers have used ransom in many cases to clear a path for victims. Therefore, it is important that we find the strength to defend not only that attack, but also the power to initiate cyber-attacks. This is better said than

done, because it is difficult to determine who the perpetrator in most cases is. The online edition makes it possible for the entire infrastructure to hide its domain for free. This is particularly so when the government is funding cyber-attacks. And the hijackers are enjoying privacy because of the asymmetry of the assault. Efficient cyber protection initiatives should, however, be implemented by countries. Cyber security is characterized as a body of technology, processes and practices designed to prevent attack, harm or unauthorized access to networks, devices, systems, and data. Safety covers both cyber security and physical security, according to the computer. Cyber protection locks computer networks, facilities, applications, control systems and operating systems, tools for assistance, etc. Household objects may also be vulnerable to theft and destruction as technology progresses rapidly. Cyber protection is therefore a major area that will be the climbing assignment. The "era of knowledge" has come to be called this century, but it has not come without its adventures. The threat of cyber security breaches is growing and sometimes causes chaos, as the world relies heavily on the internet, communications and technology (Rasool, 2015). Similarly, Pakistan is facing cyber threats as well. Not surprisingly, Pakistan is also confronted with the cyber space problem. Cyberpace has expanded in the case of Pakistan to the areas of banks, education and communications, military institutions and government (Ibid).

Prevention Act for Cyber Crime, 2016:

Pakistan is aware of the threats to cyber nationality. The Electronic Crime Reduction Act was passed in 2016 in response to these risks and challenges, proposing to prosecute cyber criminals. Legally, any unauthorized access to information, as well as any unauthorized copying of any data, any sensitive infrastructure access, computer theft, communication obstruction, personal or public offences, malicious code or transmission, cyber piracy, hate speech, is a criminal offence. For these illegal actions, the statute recommends paying fines and imprisonment. In addition, a provision is made for Computer Emergency Response Teams, who will be specialist workers on cyber security problems on sensitive infrastructure or information data. Likewise, intellect Agency officials are also to be made part of these teams (Ibid). In this regard, the Act also proposes international collaboration to thwart or instigate cyber security risks. The act itself has been praised by some as a landmark and by some as a draconian legislation that would impede certain citizens' rights, such as freedom of speech, and grant government agencies and departments extra powers (Guranami, 2017). Several civil society groups and lawmakers have voiced concerns about the wording of the text, which leaves it accessible to agencies and departments for manipulation. Human rights professionals advocate for a balance between defence and human rights (Khan, 2016).

Pakistan's Most important IT services:

Countries and businesses alike are using digital technology in the 21st century to make information available to everyone, safe and confidential if necessary. When

keeping records of their people, countries have a very important role to play. The only organisation which registers and maintains personal information is the National Database and Registration Authority (NADRA) (Awan and Memon 2016). Awareness of their citizenship is important in Pakistan's efforts to combat terrorism. For similar purposes, NADRA also liaises with other state organs. This data is fragile and faces the possibility of theft or fraud. NADRA may be the latest target of cyber terrorism by blocking or damaging its valuable resources, infiltrating personal information from people and using it for illegal purposes. It is possible to obtain credit cards, account details and other financial information through theft or fraud. Banks are increasingly growing their users in Pakistan; threats are also rising. Such kinds of large markets help companies and governments spend their capital by shielding them from fraud (Awan and Memon 2016). Today, electronic trading platforms are inundating large markets. Such trading networks include share markets, investment banks, departments of finance and government departments (Ibid).

Computer Security Text (Cert) - Pakistan Institute System:

It is understood by the Electronic Crime Reduction Act that the Internet is the cornerstone of modern communication. The Act also notes that it is necessary to create an authority to battle cyber-attacks in order to improve the protection of sensitive information and sensitive infrastructure. To date, as a reaction to legal proceedings, the Act proposes CERT. The main purpose of CERTs will be to monitor and minimize any injuries, keep records, provide timely and adequate information, avoid such incidents and gain an understanding of threats to the organization. An implementation program called "CERT (Computer Emergency Response Team) - Pakistan Telecom Sector Operations Program" has been developed by the Pakistan Telecommunication Authority (PTA) to date (PTA, nd). The plan operates in the national communications sector and proposes steps for the formation of these groups to be taken by the PTA. The structure defines the functions and positions of CERT. Pakistan has 70% tele-density, a base of 140 million subscribers, and three to five million internet users are connected to the Internet every hour (Ibid). Given such numbers, in addition to violating the privacy and security of the telecommunications sector in Pakistan, disruption and damage could harm the country. CERTs will be at the forefront of protecting the telecommunications industry and their customers from cyber-attacks.

Pakistan has had its share of cyber-attacks in recent years. The websites of the Ministry of Defense, the Department of Water and Energy, the Department of Information, the Department of Environmental Change, and the Department of Food Security were hacked and attacked on the eve of the 70th Independence Day in Pakistan (Naseer and Amin 2018). In humiliating and exposing the shortcomings of the world, such dangers go a long way. There were comparable but significant attacks back in 2010, including the hacking of 36 government websites. Not only were government agencies targeted in 2018 for such attacks, but cyber-attacks also targeted Careem, an active passenger system. The attack has resulted in the

acquisition of 14 million user profiles from many countries, including Pakistan (Jahangir, 2018). Information indicates that information is compromised, such as email, customer ID, transit details and phone numbers. Similarly, in Pakistan, cyber-attacks on several banks have emerged and are on the rise. Nearly all Pakistani banks were compromised by cyber attackers in 2018, which led to financial losses in accounts, the Federal Investigation Agency (FIA) (Qarar, 2018) has announced. However, the State Bank of Pakistan, the regulator of all banks, advised further to ensure that only one bank that violates its cyber protection continues with any threat and how it will deal with the issue. The widespread view that banks operating in Pakistan are all at risk of cyber-attacks (Ali, 2018). These incidents raise questions about the cyber security situation in Pakistan when it comes to nuclear weapons and their distribution. Globally, Pakistan is under pressure to build nuclear weapons and ultimately maintain its security; attacks have exacerbated the situation in recent years of military deportation. In order to strengthen existing security agreements, new terms are proposed to define nuclear teachings (Naseer and Amin 2018).

CONCLUSION:

The state of cyber vulnerability extends beyond political, social and private boundaries. As the world becomes more technologically advanced and more economically dependent, our growth will take place in the cyber space. With the threat of escalating standards and technologies, countries are stepping up their review of cyber laws and policies. Pakistan has also extended the country's access to cybersecurity and its international ties. Pakistan is also faced with the same challenges that the world faces in cyberspace. Such risks are on the increase and are now pointing to more complicated schemes. Also not rescued from the attack were the military and other state agencies. There are stories of how to deal with these issues and challenges all over the world. Cyber threats will also continue to grow as Pakistan advances and increases access to cyber access. Over the years, Pakistan has made an official contribution to cyberspace and its growth. However, the question has not yet been properly resolved by such laws and regulations. In addition, when it comes to acquiring Pakistan’s cyber space, there is a need for law, policy making, concerted efforts and collective commitment.

REFERENCES:

Gibbs, S 2015, ‘Hackers can hijack Wi-Fi Hello Barbie to spy on your children’, The
Guardian, 26 November, viewed 26 Dec 2018,
www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spyon-your-children.

Zetter, K 2015, ‘Hackers can send fatal dose to hospital drug pumps’, Wired, 08 June 2015,
viewed 26 December 2018, www.wired.com/2015/06/hackers-can-send-fatal-doses-hospitaldrug-pumps.

Greenberg, A 2015, ‘Hackers remotely kill a jeep on the highway’, Wired, 21 July, viewed

26 December 2018, www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.

McAfee Labs 2015, 2016 Threats Predictions, October, viewed 26 December 2018, www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf.

American Chemical Society 2016, Cyber Security: Threats, Challenges and Opportunities,

ACS Publishing, viewed 26 December 2018, https://www.acs.org.au/content/dam/acs/acspublications/ACS_Cybersecurity_Guide.pdf.

Ali, K 2018, 'FIA takes up banking fraud, hacking with SBP', DAWN.com. 09 November,

viewed 25 December 2018, https://www.dawn.com/news/1444485.

Ashford, W 2017, Manufacturing a key target for cyber-attacks, TechTarget. 11August,

viewed 23 December 2018,

https://www.computerweekly.com/news/450424302/Manufacturing-a-key-target-for-cyberattacks.

Awan, J, Memon, S 2016, Threats of Cyber Security and Challenges for Pakistan, 11th International

Conference on Cyber Warfare and Security, At USA..

Kesler, B 2011, "The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights

Spring 2011, vol. 10, no. pp. 15-25, viewed 31 December 2018,

http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI-v10-I1_Kesler.pdf.

Cyber Attack Advantages 2013, thoughts on cyber politics, Nov. 28, UBC Blogs site, viewed

26 Dec 2018, http://blogs.ubc.ca/cyber/2013/11/28/cyber-attack-advantages/.

Smith, DJ 2014, Russian Cyber Strategy and the War Against Georgia, Atlantic Council ,

viewed 25 December 2018, http://www.atlanticcouncil.org/blogs/natosource/russian-cyberpolicy-and-the-war-against-georgia.

Grove, T, Barnes, JE & Hinshaw, D 2017, 'Russia Targets NATO Soldier Smartphones', The

Wall Street Journal, October 4, viewed 30 December 2018,

https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-

1507109402.

Guramani, N 2017, Senators term Prevention of Electronic Crimes Act, 2016 a 'black law',

Dawn, July 19, viewed 22 April 2018, https://www.dawn.com/news/1346310.

Internet Users by Country 2016, Internet Life Stats, July, viewed 30 December 2018,

www.internetlivestats.com/internet-users-by-country.

Jahangir, R 2018, 'Over 14m users' data compromised in Careem cyber attack', Dawn.com.,

April 24,viewed 27 August 2018, https://www.dawn.com/news/1403533.
Khan, R 2016, 'Cybercrime bill passed by NA:13 reasons Pakistani's should be worried',
Dawn.com, August 11, viewed 22 April 2018, https://www.dawn.com/news/1276662.

Lewis, J 2018, Economic Impact of Cybercrime—No Slowing Down, Report, Center for
Strategic and International Studies (CSIC), viewed 30 December 2018,
https://www.mcafee.com/us/resources/reports/restricted/economic-impactcybercrime.
pdf?utm_source=Press&utm_campaign=bb9303ae70 EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_ 7623d157bebb9303ae70-.
Nakashima, E 2014, Russian hackers use 'zero-day' to hack NATO, Ukraine in cyber-spy
campaign, National Security, The Washington Post, October 13, viewed 27 December 2018,
https://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-tohack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-
602188e70e9c_story.html?noredirect=on&utm_term=.1937fbac5efa.
Naseer, R & Amin, M 2018, Cyber-Threats to Strategic Networks: Challenges for Pakistan's
Security. A Research Journal of South Asian Studies, vol. 33, no. 1, pp. 35 -48.
Gade, NR & Reddy, UJG 2014, A study of cyber security challenges and its emerging trendson latest technologies, ResearchGate, viewed 31 December 2018,
https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Securi ty_Challen
ges_And_Its_Emerging_Trends_On_Latest_Technologies.
Qarar, S 2018, 'Almost all' Pakistani banks hacked in security breach, says FIA cybercrime
head', Dawn.com, November 6, viewed 28 December 2018,
https://www.dawn.com/news/1443970.
Rasool, S 2015, Cyber security threat in Pakistan: causes Challenges and way forward,
SocioBrains, Issue 12, August 2015, viewed 28 December 2018,
http://sociobrains.com/website/w1465/file/repository/21_34_Sadia_Rasool_Cyber _security_threat_in_Pakistan_causes_challenges_and_way_forward.pdf.
Shahani, A 2014, Microsoft Windows Flaw Let Russian Hackers Spy On NATO, Report

Says, National Public Radio, October 14, viewed 28 December 2018 https://www.npr.org/sections/alltechconsidered/2014/10/14/356167086/microsoft-windowsflaw-let-russian-hackers-spy-on-nato-report-says.

Broad, WJ, Markoff, J and Sanger, DE 2011, 'Israeli Test on Worm Called Crucial in Iran

Nuclear Delay', "The New York Times, Jan 15, viewed 28 December 2018, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.