Journal of Positive School Psychology http://journalppw.com
2023, Vol. 7, No. 6, 82-94

Dimension Of Cyber-Warfare In Pakistan's Context

Muhammad Shahzad Akram[1] , Moneeb Jaffar Mir[2] , Abdul Rehman[3]

[1]Research Officer at Center for Strategic Studies-AJK and he holds an M.Phil. degree in IR from Quaid-e-Azam University Islamabad.
[2]Assistant Research Officer at Center for Strategic Studies-AJK and he holds an Master degree in DSS from Quaid-e-Azam University Islamabad.
[3]Assistant Research Officer at Center for Strategic Studies-AJK and he is pursuing his M.Phil. degree in IR from National Defense University Islamabad.

Abstract

Cyber warfare has evolved as a crucial part of modern combat, comprising many sorts of harmful activities carried out in cyberspace. This research investigates the topic of cyber warfare in the context of Pakistan. The paper begins with a comprehensive analysis of cyber warfare, its definition, and its importance in today's national security scene. It emphasizes rapid technological breakthroughs and the rising reliance on the internet for essential infrastructure, communication, and economic activities, making nations exposed to cyber-attacks. This study examines Pakistan's cyber landscape, including its cyber capabilities, infrastructure, and policy framework. It investigates Pakistan's growing threat landscape, which includes state-sponsored attacks, terrorist activities, espionage, and cybercrime. The investigation delves into notable Cyber incidents that have occurred in the country, their impact, and the response procedures that have been implemented. Furthermore, the report explores the Pakistani government's strategies and activities to improve cybersecurity and build resilience against cyber threats. It evaluates the legal and regulatory frameworks, institutional arrangements, and capacity-building efforts in the fight against cyber warfare. The research also emphasizes the importance of international cooperation and collaboration in countering cyber threats in Pakistan. This study gives a thorough examination of the cyber warfare issue in the Pakistani context. It provides insights into the growing cyber threat landscape, the country's readiness to counter cyber threats, and potential future problems and possibilities. The findings help to improve understanding of the complicated nature of cyber warfare and give recommendations for Pakistan's authorities and stakeholders to improve their cybersecurity posture.

Key Words: Cyber-warfare, Cyber-Espionage, National Security, Cyber Security, Revolution in military affairs.

Introduction

In contemporary times with the advancement of technology, war has been revolutionized. Cyber is rapidly contributing the modern warfare. Pakistan is a developing country and its reliance on the internet has been increasing rapidly for e-governance which increases its vulnerability to cyber-attack, because of poor understanding of cyberspace, lack of preparedness, and hostile regional situation. Pakistan was ranked among the top 10 countries that booming digitally in UN Trade and development in the information economy and 365 million Pakistani have access to the internet most of them the 3G and 4G users

who are more vulnerable to cyber-attacks.[4] Pakistan passed its first law related to online crime in 2016 Electronic crime prevention act. However despite this still Pakistan lacks full-spectrum legislation on how to deal with this new nature of the threat. Technological advancement has revolutionized the life of the public and they start becoming more dependent on the Internet. Technological advancement poses a security threat to individual privacy and the national security of the state. National security can be defined by Arnold Wealfare in his words as an "Ambiguous symbol" [5]

National security is different concerning countries' interests and capabilities, for example, the United States national security threat from World War II to the fall of the Soviet Union was Russian and from 1990 it regard China as a potential threat. In contemporary times, cyber warfare has been very serious on the national security of Pakistan because of having nuclear weapons and poor national security preparedness.[6] The state must take effective measures to protect individual privacy, critical infrastructure, and military infrastructure because of extreme dependency on the internet and technology.

National Security

National security refers to the absence of any potential threat to the state's survival. It is a very broad concept over some time states have taken several measures to ensure their survival. National security notion develops during the 17th century. [7] When Europe was heavily indulged in wars and conflicts to give peace a chance and to promote peace harmony and mutual interdependence. A peace treaty was signed in 1648 named as Westphalia peace treaty. After this treaty not only conflicts ended in Europe but also led to the creation of nation-states along with that comes the concept of sovereignty where a state has full control over its boundaries. The pre-Westphalia concept of security is mostly associated with the universal principle decided by the king, queen, or pope. In 1648 with the signing of the treaty and the creation of the nation-state not only did the concept of security change but it also changes the principle governing the state's affairs from universal principle to peace, prosperity, and stability. [8] In contemporary times the international system is more secure and more stable than Westphalia and pre-Westphalia because of its hierarchal structure and the presence of a powerful hegemon. National security is a recently emerging phenomenon after World War II however traces of this concept were found in the historical work of Madison and then in Walter Lippmann's famous work "US foreign policy" which was originally published in 1948.[9] The word national security found its place in the dictionary of strategic studies after World War II.[10] In contemporary times national security is associated with the protection of a state's sovereignty. Dr. Vojin Dimitrijevic an expert

[4] "4G Is Vulnerable to Same Types of Attacks as 3G, Researchers Say," *CyberScoop* (blog), July 2, 2018, https://cyberscoop.com/4g-vulnerable-types-attacks-3g-researchers-say/.

[5] Arnold Wolfers, "'National Security' as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 4 (1952): 481–502, https://doi.org/10.2307/2145138.

[6] "Cyber Security: Where Does Pakistan Stand?," accessed January 26, 2023, https://think-asia.org/handle/11540/9714.

[7] "What Is National Security?," The Heritage Foundation, accessed November 11, 2021, https://www.heritage.org/military-strength-essays/2015-essays/what-national-security.

[8] "Nation-States and Sovereignty | Boundless World History," accessed December 25, 2021, https://courses.lumenlearning.com/boundless-worldhistory/chapter/nation-states-and-sovereignty/.

[9] "National Defense," Congressman Madison Cawthorn, January 3, 2021, http://cawthorn.house.gov/issues/national-defense.

[10] Wolfers, "'National Security' as an Ambiguous Symbol."

on international law gave the following key elements of national security. [11]

- Ensuring the survival of a state (as a political community) and the nation as a population.
- Ensuring the territorial and geographical survival and protection
- Independence state with international recognition
- People living in that state should have a good quality of life
- Subordination of national interest in national security

Mario Nobilo an expert on international relations defines national security as "the highly complex link between social, political, economic, legal, societal, military, ideological and as well as other internal and external factors through which state protect its sovereignty, ensure the survival of masses, political an independent entity and having stable economic and social development". [12] Amin Hewedy a diplomat and international expert defines national security as "A state capacity to ensure its survival while keeping in view national and internal changes/development". [13]

In contemporary times, cyber security is also very important because most theorists considered cyber security as national security because of technological development. Cyber is considered the backbone of the state, its critical infrastructure, and private business is dependent on the cyber domain. Therefore, while keeping all of these in mind we can refer to that national security refers to the protection and defense of a state's territorial, geographical, air, space, water, and cyber also.

Cyber Security as National Security

With the rise of cyberspace, the internet and states' rapid dependency on cyber for smooth and efficient working created serious security issues for states. In modern times cyber threats from the internet are a major source of state concern regarding national security. The traditional concepts of national security were no more applicable in the cyber domain mainly because of cyber uniqueness. Traditionally armed attacks from opponents were considered a major source of threat to the state's national security. [14] However, this concept remains a sense of insecurity until the rise of non-state actors in early 2000 when non-actors including freedom fighters (those who were fighting against the oppression like in Indian-held Kashmir, Israel occupied Palestine) were designated as a terrorist and threats to the national and global security. Traditionally armed attack either from another state or non-state actors was considered a major threat to state national security. These traditional concepts were challenged by the rising cyber because cyber threats are not physical but virtual and the actors involve in cyber are also unidentifiable.[15] So in the 21st century, we have witnessed a shift in security studies from traditional security threats to non-traditional security threats. While keeping in view the nature of the threat from the internet Richard Clarke an ex-United States official and advisor

[11] Anton Grizold, "THE CONCEPT OF NATIONAL SECURITY IN THE CONTEMPORARY WORLD," *International Journal on World Peace* 11, no. 3 (1994): 37–53.

[12] Grizold.

[13] Khalil Shikaki, "Amin Hewedy, Militarization and Security in the Middle East: Its Impact on Development and Democracy (London: Pinter Publishers, 1989). Pp. 144.," *International Journal of Middle East Studies* 24, no. 1 (February 1992): 141–43, https://doi.org/10.1017/S0020743800001525.

[14] "Rise of Non-State Actors in Cyberwarfare - Oxford Scholarship," accessed December 26, 2021, https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780198717492.001.0001/acprof-9780198717492-chapter-7.

[15] "Richard Clarke on U.S. Cyberdefenses: 'We're Paying Lip Service,'" accessed December 26, 2021, https://www.fastcompany.com/90378700/richard-clarke-is-sounding-the-alarm-about-another-kind-of-9-11.

to President Bush gave the concept of "Cyber Pearl Harbor".[16] While Berry Buzan gave the concept of securitization in securitization Buzan argues that an issue is undertaken as an existential threat to such a level that it needs quick measures.[17] In cyberspace, the possible threat agents can be anyone from an individual hacker, group of hackers, professional cyber-criminal, terrorists, and nation-states while the same implies on receiving ends that victims can also be diverse.[18] Buzan further argues that threats to national security are diverse like military, political, and even social, economic, and even ecological. This is where cyber threats are referred to as national security threats. According to Buzan in contemporary times cyber security threats are considered a potential major security threat to the national security of the state. Moreover, the developed nation has already started the securitization of cyber threats through writing, policy drafting, and even through their speeches for example, the Federal Agency FBI (Federal Bauru of Investigation) historically whose main objective was to deter any kind of terrorist attack and counterintelligence has seen a change in their policy of national security as they added cyber threat as a national security threat. In contemporary times most of the conflicts have a cyber-dimension from India and Pakistan to the United States of America and China they are continuously engaging in the cyber domain to prove their technological superiority. Contemporary security expert of security expert believes that in today's time; most of the conflict can be fought and won from the comfort of the bedroom.

Dimension of Cyber Warfare and Pakistan National Security

Today world population stands at about 7.7 billion out of which 4.66 billion use the internet which is about 59.5% of the population and about 92.6% population[19] access the internet via mobile phone. [20] Out of the total 7.7 billion population of the world, [21] about 226 million live in Pakistan from which 61.34 million people have internet access.[22] However, with technological advancement telecommunication has revolutionized the world but still; cyberspace is considered a haven for criminal activities.

With globalization, the world has been turned into a global village and most of the activities were performed virtually through cyber using the internet but during the early 90s internet has been turned into a new mode of fighting the war and performing illegal activities as most of the cyberspace is lawless, there is no central authority. In contemporary times cyberspace is used by different states, multi-national organizations and non-state actors, terrorists, and individual criminals and hackers to perform illegal activities and cyber war. Strategically in the Pakistani context, we have categorized cyberspace into four "C" **Cyber-Crime, Cyber-Terrorism, Cyber-Economy, and**

[16] "What Is Cyber Pearl Harbor? - Definition from Techopedia," accessed December 26, 2021, https://www.techopedia.com/definition/29052/cyber-pearl-harbor.

[17] "Securitisation Theory: An Introduction," accessed December 26, 2021, https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/.

[18] "National Security | Journal of American History | Oxford Academic," accessed December 26, 2021, https://academic.oup.com/jah/article-abstract/77/1/143/756627?redirectedFrom=PDF.

[19] "Individuals Using the Internet (% of Population) | Data," accessed October 25, 2021, https://data.worldbank.org/indicator/IT.NET.USER.ZS.

[20] "• Internet Users in the World 2021 | Statista," accessed October 25, 2021, https://www.statista.com/statistics/617136/digital-population-worldwide/.

[21] "Broadband Users in Pakistan Shoot up to 100 Million: PTA," accessed October 25, 2021, https://www.thenews.com.pk/latest/814261-broadband-users-in-pakistan-shoot-up-to-100-million-pta.

[22] "Media Center | PTA," accessed October 25, 2021, https://www.pta.gov.pk/en/media-center/single-media/ptas-response-to-hootsuites-digital-2019-pakistan-report-210619.

Cyber-Warfare. These are four of the "C" of cyber warfare and they have the potential to retard the medium.

Cyber Terrorism

According to a UNSC counter-terrorism committee Executive Director, Terrorists, and terrorist groups exploit the Internet and social media not only to commit terrorist acts, but also to facilitate a wide range of terrorist activities, including incitement, radicalization, recruitment, training, planning, collection of information, communications, preparation, and financing.[23] In the modern era, as the need for information technology is augmenting at a fast pace, so are the threats emanating from it. The main tools utilized in cyberterrorism are computers and the internet.

Propaganda

In the 1980s, terrorists produced films, and videotapes, and printed high-quality magazines for propaganda and radicalization.[24] These were not circulated through the internet, but rather through mail or were handed out to people manually at particular spots. However, as media technology went through a paradigm shift, so did the terrorists. During the days, when terrorist organizations would manually disseminate their content for propaganda, its reach was limited. Not only that it carried more risk but it also cost more comparatively doing the same through the newly emerged cyber world. For instance, radical jihadists in the United States transferred their magazine Al-Hussam (the Sword) to email in digital form from paper. It used to cost around $1000 to publish the magazine on paper, however, its cost reduced to zero when done through email.[25] Moreover, it could easily be sent to a wider audience, even across borders effortlessly. Similarly, radical recruiters to influence people from a distance used platforms like Yahoo and AOL.

As time progressed, the world witnessed the advent of enhanced social media outlets, which revolutionized communication, such as Twitter, Facebook, and YouTube. The internationally infamous terrorist organizations, for instance, Al Qaida and ISIS utilized these to the maximum to propagate their viewpoints to increase their support base, and relevance and to ensure their existence. Nonetheless, both used cyber resources differently. Al Qaeda mainly used cyber-resources to propagate its ideologies, which was 31. 8% of its total content, on the other hand, ISIS used it as an instrument to spread fear and threat, which constituted 37.9% of its content.[26]

In Pakistan, the outlawed Tehreek-e-Taliban Pakistan (TTP), a notorious militant group that for years has been spearheading a deadly terror wave resulting in the killings of thousands of Pakistanis, also jumped the bandwagon. After witnessing the popularity of the cyber world and social media, TTP launched 'Umar Media', the official media platform of terror organizations, in 2012. The terror group has since been using Umar Media as well as other mediums of social media to spread its propaganda actively. In this regard, TTP has

[23]"Ctc_cted_factsheet_ct_in_cyberspace_oct_2021.Pdf," accessed February 15, 2023, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf.

[24] "(PDF) A Guileful Ruse: ISIS, Media, and Tactics of Appropriation | Piotr Szpunar - Academia.Edu," accessed February 15, 2023, https://www.academia.edu/37523301/A_guileful_ruse_ISIS_media_and_tactics_of_appropriation.

[25] Stern Jessica, J. M Berger, "ISIS: The State of Terror: Stern, Jessica, Berger, J. M.: 9780062395559: Amazon.Com: Books," accessed February 15, 2023, https://www.amazon.com/ISIS-State-Terror-Jessica-Stern/dp/0062395556.

[26] Kyung-shick Choi, Claire Seungeun Lee, and Robert Cadigan, "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS," *The International Journal of Cybersecurity Intelligence and Cybercrime* 1, no. 1 (August 15, 2018): 21–39, https://doi.org/10.52306/01010418ZDCD5438.

pursued a thematic approach to inject empathy into its targeted audience. Which is then used to increase support for the group, and to lure fighters and donors. Such popular themes include depicting the Pakistan state as a paid US mercenary, hailing itself as the real patron of Islam, the harbinger of peace and liberators.[27]

Cyber Terror Financing

Terrorist organizations require significant funding, which not only is needed for carrying out terrorist acts but also to maintain the functioning of the organization, to provide for its necessary technical requirements, and match up costs related to spreading ideologies. Traditionally, terrorist organizations have resorted to high-dollar data breaches, cash couriers, and formal and informal transfer systems for funding. Similarly, criminal sources, such as drug trafficking, fraud, smuggling of weapons and other goods, kidnapping, extortion, and charities have proven to be even important sources of funding for terrorist activities.

However, the cyber-space has also brought about a transformation in this aspect. Not only that terror financing through cyber-space become complex to tackle but the advent of cryptocurrency has further exacerbated the issue. According to Financial Action Task Force (FATF), the anonymity associated with cyber transactions attracts terrorists who utilize such a medium to carry out money laundering, by engaging in the drugs trade, illegal arms smuggling, fraud, tax evasion, cyber-attacks, sanctions evasion, child exploitation, and human trafficking.[28] While cryptocurrency is further enlarging such leverage by increasing the level of anonymity. As Al Qaida and its affiliated groups ran a Bitcoin money laundering network utilizing various forms of social media to enable cryptocurrency donations to advance their terrorist goals.[29]

As for Tehreek-e-Taliban Pakistan (TTP); so far, it has been resorting to traditional methods for fundraising.[30] However, such a possibility cannot be ruled out that TTP would turn to online funding in the future. The way TTP has shifted its propaganda to cyber-space, amply foreshadows that it would also attempt to raise funds on the very platform.

Cyber Terror Recruitment, Training, and Planning

Just like terror organizations use cyber-space to induce their ideology to radicalize the masses and raise funds for the functioning of their organizations. They also bring the very platform to recruit like-minded individuals.[31] Cyber Space also offers a variegated mechanism in the form of visual videos as well as information that acts as training programs for potential terrorists.[32] Similarly, many criminal justice practitioners have signified that almost certainly every persecuted case of terrorism involves the use of cyber, especially when planning an act of terrorism. [33]

A significant portion of Cyber-space comprises youth, who remain vulnerable to the bait of terrorist organizations. Terrorist groups employ

[27] Tahir, Saif ur Rehman, "A Study of Tehreek-e-Taliban Pakistan (TTP) Social Media Communication: Major Trends, Key Themes and Propaganda Appeals" [PAKISTAN JOURNAL OF TERRORISM RESEARCH, VOL II, ISSUE I (n.d.).

[28] "12 Month Review of Revised FATF Standards - Virtual Assets and VASPs," accessed February 15, 2023, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html.

[29] "Global Disruption of 3 Terror Finance Cyber-Enabled Campaigns | ICE," accessed February 15, 2023, https://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns.

[30] "Pakistan Taliban Racketeering Hits Borderlands," accessed February 15, 2023, https://www.france24.com/en/live-news/20221125-pakistan-taliban-racketeering-hits-borderlands.

[31] Saqib Khan and Khalid Manzoor Butt, "Cyber Technology, Radicalization and Terrorism in Pakistan," *Journal of Indian Studies*, n.d.

[32] Ibid.

[33] "The Use of the Internet for Terrorist Purposes," n.d.

young recruits in almost every capacity: in support roles, as recruiters, as propagandists, and as fighters. Individuals' specific roles are often determined by their age and gender.[34] In this way, Cyber-space remains to be an effective medium through which terrorist organizations recruit jobless youth and minors. It is a cheap podium for terrorist organizations to get connected with limitless organizations. When it comes to Pakistan, the country's economy remains in dire straits. Where the inclination of a proportion of the population remains perched on a dangerous juncture that could be enticed by terrorist organizations, such as TTP.

Cyber Crime

Crime always remains part of society. However in the 21st century with the rise of technology, the nature of crime has transformed which makes it more difficult for law enforcement agencies to detect and prevent them. In the contemporary digitalized world crime has become one of the main threats to personal as well as national security. Electronic devices like computer systems, laptops, and mobile phones are mostly used for various types of cybercrimes. Cybercrime is mostly related to the activities of individual hackers or groups which carried out attacks on government and private intuitions as well as financial sectors for personal financial gains. Cyber-criminal can be local, regional o international but their utmost objective is financial gain. There are different means of attacking which mostly hackers used common one is the use of malicious code, Trojan Horse (Trojan Horse is the most effective one as it not only destroys the software but also transfers sensitive data back to the hacker through a botnet).[35]

DDoS is another attack that was for a specific system for a specific time common examples are the Sindh high court website and the Russian attack on Georgia. So if we look at the history of the nature of cyber-crime in Pakistan we came to know that two types of cyber-crime took place in Pakistani cyberspace over the period one is the low-level cyber-attack from Indian individual hackers and the second from

[34] Jessica Trisko Darden, "Tackling Terrorists' Exploitation of Youth," n.d.

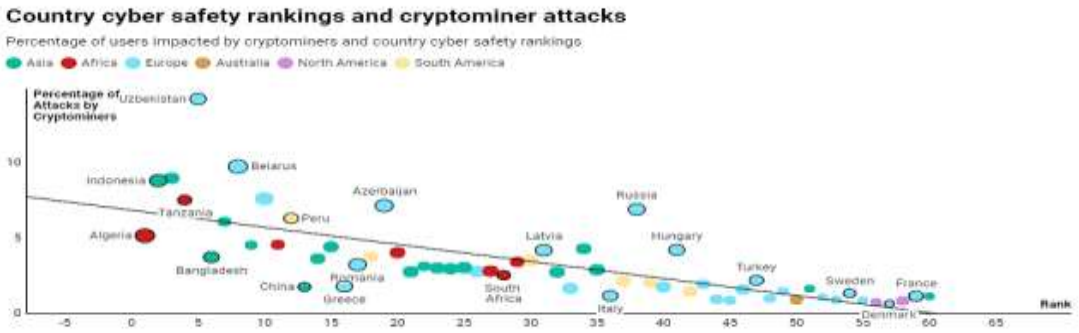
[35] Khawar Ghumman, "Cyber Attacks against Govt Expose Fatal Cracks in Pakistan's Digital Fence," DAWN.COM, May 19, 2015, http://www.dawn.com/news/1182856.

the local and international hackers for financial gains.[36]

Rank	Country	Score	Percentage of Mobiles Infected with Malware	Financial Malware Attacks (% of Users)	Percentage of Computers Infected with Malware	Percentage of Telnet Attacks by Originating Country (IoT)	Percentage of Attacks by Cryptominers	Best Prepared for Cyberattacks
1	Algeria	55.75	22.88	0.9	32.41	0.01	5.14	0.432
2	Indonesia	54.89	25.02	1.8	24.7	1.51	8.8	0.424
3	Vietnam	52.44	9.62	1.2	21.5	1.73	8.96	0.245
4	Tanzania	51.00	28.03	0.7	14.7	0.04	7.51	0.317
5	Uzbekistan	50.50	10.35	0.5	21.3	0.01	14.23	0.277
6	Bangladesh	47.21	35.91	1.3	19.7	0.38	3.71	0.524
7	Pakistan	47.10	25.08	1.4	14.8	0.4	6.07	0.447

Source: Pakistan Ranked 7th Worst in Cyber-Security: Report," accessed December 26, 2021, https://propakistani.pk/2019/02/14/pakistan-ranked-7th-worst-in-cyber-security-report/.

Hacker hacked the Meezan bank and 69,189 card details were put online for sale. Moreover, this security breach caused the bank about $3.5 million in data loss.[37] Moreover, the hacker also hacked the K-electric and threatened to pay the ransom of about $3.5 million. The ransom becomes doubled after a week of $7 million but K-electric still didn't pay much attention and all of the stolen information has been leaked online for sale.[38] K-electric has millions of users and has customer-sensitive data i.e. customer name, address, CNIC, and bank account details. Moreover K Electric didn't pay any ransom to the hacker nor do they try to improve their cyber security and the hacker leaked 8.5 GB of data.[39]



Source: Pakistan Ranked 7th Worst in Cyber-Security: Report.

Cyber Economy/Digital Economy

With the advancement of technology, the nature of crime has changed. Pakistan has observed a spike in cybercrime in the last two decades. Pakistan despite having a nuclear country still lack the capability of digital forensics, cyber expert, and proper technical equipment.[40]

[36] "Pakistan Ranked 7th Worst in Cyber-Security: Report," accessed December 26, 2021, https://propakistani.pk/2019/02/14/pakistan-ranked-7th-worst-in-cyber-security-report/.
[37] "Pakistani Banks Hit by Biggest Cyber Attack in Country's History - SAMAA," accessed October 28, 2021, https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history/.
[38] Ibid.
[39] "Hackers Leak Files Stolen in Pakistan's K-Electric Ransomware Attack," accessed October 28, 2021, https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/.
[40] "Pakistan Ranked 7th Worst in Cyber-Security: Report."

According to an UN-CTAD United Nations CAD report on the digital economy, in 1992 the digital flow of data was about 100 GB per day, in 2017 about 45000 GB while in 2022 it is about 150,700 GB per day.[41] This enormous growth of data flow led to an increase in the digital economy which is about $7 trillion. Cybercrime remains the main threat to the digital economy. According to the Forbes Magazine report on cybercrime global economy lost about $ 5.2 trillion. According to a report in Cyber Security magazine global economy lose about $ 6 trillion in 2021 and this will further increase up to $ 10.5 trillion in 2025.[42] Global cybercrime increases by about 15% each year. Pakistan is a developing country with a low-ranking global digital economy of 56/60.[43] According to a report by the Ministry of Planning and Development Pakistan's economy is estimated at $3.5 billion.[44] With the rapid advancement of technology and digitization of the economy, identity theft remains one concern. Recently because of privacy issues Google and Facebook had to pay $ 13 million and % 35 billion. During the last decades, Pakistan has witnessed about an 83% rise in cybercrime.[45] FIA in 2020-21 blocked about 30 malicious gateways involved in different crimes. The accounts were involved in financial crime, creating fake profiles, hacking, stealing, fake information, and propaganda. The most common tools used for cyber-crime are Facebook, WhatsApp, Instagram, Line, and Telegram given below detail.

Cyber Warfare.

Cyber warfare refers to the launch of a cyber-attack to such a level that caused massive disruption of the state institutions and seriously impacted critical infrastructure. Such full-scale cyber warfare was launched by Russia in Georgia and Crimea. However, while keeping in mind Pakistan's security concern through the strategic lens, we have divided the current cyber warfare into two sub-topics which lie under the domain of cyber warfare and pose a security threat to the national security of Pakistan. These two are propaganda warfare and cyber espionage.[46]

Propaganda warfare

Propaganda and fake information were always remaining an important part of warfare from ancient times to current modern warfare. Historically the concept of propaganda warfare dated back to the time of ancient Chinese general Sun Tzu time when he talked about the best win being when you won without fighting and indirect attack also.[47] In contemporary times the use of information to spread propaganda as a tool of warfare is becoming common and important. This propaganda has been used by foreign intelligence, and governments against their opponent to defame, and discredit them. Propaganda and information are cheap, easy to use, and easy to

[41] "ECommerce Week 2022: Data and Digitalization for Development | UNCTAD," accessed January 25, 2023, https://unctad.org/eweek2022.
[42] cybercrimemag, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine* (blog), February 21, 2018, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
[43] "PB-Cyber-Crime-in-Pakistan.Pdf," accessed January 26, 2023, https://cgr.com.pk/wp-content/uploads/2020/08/PB-Cyber-Crime-in-Pakistan.pdf.
[44] Ibid.
[45] "PB-Cyber-Crime-in-Pakistan.Pdf," accessed January 26, 2023, https://cgr.com.pk/wp-content/uploads/2020/08/PB-Cyber-Crime-in-Pakistan.pdf.
[46] "The Cyber Dimension of the 2008 Russia-Georgia War," accessed August 18, 2021, https://www.gfsis.org/blog/view/970.
[47] "Sun Tzu's 'The Art of War' Is Still Relevant - The Hindu," accessed December 26, 2021, https://www.thehindu.com/books/how-to-win-without-fighting/article25797014.ece?__cf_chl_captcha_tk__=w5_bDVtXtuuM7lZb1ezZOHPt.iYenZJvM7G.lG4x0Aw-1640531076-0-gaNycGzNCKU.

manipulate opponents. Disrupt. Russian and American experts even equate information warfare with weapons of mass destruction. This means that propaganda warfare is as lethal as a weapon of mass destruction. Information warfare is the first time used by Russia against Crimea and Georgia.[48] However, Pakistan like the rest of the world is also facing the threat of propaganda warfare. Mostly Pakistan becomes a victim of propaganda spread by India, Israel, and European media. They try to discredit Pakistan for its anti-terrorism success and portray a very pessimistic view of Pakistan. This foreign-sponsored propaganda actively targeted the Pakistani army, intelligence, and China Pakistan joint initiative CPEC.[49] In the 21st century with the rise of technology availability of large information, easy access to the information, and uses of information to spread propaganda against Pakistan and defame its image at global levels. There are possibilities that in the future states won't fight conventional war instead they go for propaganda war as it is much cheaper, easy to fight, and much more powerful and effective than traditional conventional war.[50] With the rise of technology in the 21st century, it has become more complex and provides an easy way for non-state actors to exploit societal cleavages. In the future war, cyber-warfare will act as a force multiplier.[51] The traditional concept of power especially the power dynamic between the attacker and attacked one was also redefined. It is one of the most powerful tools that can achieve the desired objective signal handily and it also impacts the cultural, political, economic, and societal dynamic of a state.[52]

Pakistan has also become a victim of this propaganda war. Most of this propaganda was directed against Pakistan by India with the help of Israeli and Western media. The targeted range from sovereignty to the common societal cleavage. During the anti-terrorist operation in Baluchistan and FATA in 2008 and 2009, a properly well-planned propaganda campaign was launched against the Pakistani military.[53] This anti-military campaign overshadowed the Pakistan anti-terrorism success over the minor terrorist attack. However, this campaign was remaining quite successful as it develops a very strong anti-military narrative among the people. In the same case over the decades, Baluchistan also has been a victim of this propaganda war as it is one of the minerals enrich provinces, and the billion-dollar CPEC is also located there. CPEC is targeted by Western media and propaganda cells they call it “CPEC a modern East India company”.[54] Moreover, when it comes to Indian-directed propaganda against Pakistan it is not only limited to fake information, and fake news through social media or other news agencies but Bollywood also plays a very active role in defaming Pakistan and the Muslim ancient ruler. Moreover, India through its Bollywood movies portrays a pessimistic image of Pakistan and Muslims as well.[55] In several movies, they

[48] “The Cyber Dimension of the 2008 Russia-Georgia War.”
[49] “India and America Collude to Disrupt the China-Pakistan Economic Corridor,” openDemocracy, accessed January 26, 2023, https://www.opendemocracy.net/en/india-and-america-colludes-disrupt-china-pakistan-economic-corridor/.
[50] “India and America Collude to Disrupt the China-Pakistan Economic Corridor | OpenDemocracy,” accessed December 26, 2021, https://www.opendemocracy.net/en/india-and-america-colludes-disrupt-china-pakistan-economic-corridor/.
[51] Ibid.
[52] Ibid.
[53] “Hybrid Warfare Threats for Pakistan: Security Dynamics and the Way Forward - Centre for Strategic and Contemporary Research,” accessed December 26, 2021, https://cscr.pk/explore/themes/defense-security/hybrid-warfare-threats-for-pakistan-security-dynamics-and-the-way-forward/.
[54] “India and America Collude to Disrupt the China-Pakistan Economic Corridor.”
[55] “Islamophobia In Bollywood Movies | Youth Ki Awaaz,” accessed December 26, 2021, https://www.youthkiawaaz.com/2021/09/do-we-recognize-bollywoods-affair-with-islamophobia-in-indian-cinema/.

portray Muslims as barbaric, homosexual, uncivilized, and non-human and Pakistan as unsafe, terrorist safe heavens, global security risk, etc. After the separation of Bengal in 1971 Indian academics, writers, media, and Bollywood attacked the two-nation theory and try to tell the Muslims of the subcontinent that there isn't any theory like the two nations and portray it as an absurd idea.[56] Not only has this but Bollywood and Indian media over the period also played a very crucial role in creating hate and negativity between Pakistan and Afghanistan.

Recently EU dis-info lab also debunked a massive propaganda campaign against Pakistan which was named "Indian Chronicles". The report reveals that the Indian-sponsored propaganda war against Pakistan was continuously defaming and portrayed a negative image of Pakistan since 2005.[57] Propaganda is not only limited to Pakistan but China was also targeted. Srivastava group was the main brain along with Indian news agencies and RAW (Research and Analysis Wing). The main objective of this propaganda warfare is to help India to preserve its power at the global level and in global institutions e.g.[58] EU, UN, IMF, World Bank, and other tech giants. The Srivastava group has created a fake profile of EU officials, UN officials, and other high-profile officials of European states, think tanks, and NGOs.[59] They have also created fake news channels, newspapers, journals, etc.

Cyber Espionage

Cyber espionage or cyber spying refers to an act of spying through cyber or using cyber technology. It refers to a method through which attackers can steal confidential information, and keep spying like in the case of the Pegasus virus without even knowledge and consent. In contemporary time technological advances and the protection of personal data has become a very growing concern. Mostly personal data security breaches are either in the form of third-party access to personal/confidential data which include, access to private emails, social media accounts, GPS tracking, data mining, or using a malicious piece of code that may explode the device for example (Stuxnet a malicious software designed to derail Iranian nuclear program). In cyber-espionage main concern was either to steal confidential or remain in the opponent's system as long as possible and keep spying. The protection of personal information is very difficult as cyber espionage is not only limited to states but professional cyber-criminals, and notorious and rogue organizations are also involved in this act of data mining and cyber spying.[60] Singh and Bang argue that neither law nor law-enforcement agencies work the same as they work in physical crime. In most cybercrime attacks attacker is unknown. So, the attacked one must contact the concerned law-enforcement agencies and fully try to cooperate with them and a collective effort is needed for a joint response.[61] However, while looking at the sensitivity of the issue EU and the US passed several laws to tackle privacy and espionage issues in the early '90s and '80s. In

[56] Muhammad Ashraf Khan, Syeda Zuria Bokhari, and M Phil, "Portrayal of Muslims in Indian Cinema: A Content Analysis of Movies during (2002-8)" 8 (2011).

[57] "Indian Chronicles: Deep Dive into a 15-Year Operation Targeting the EU and UN to Serve Indian Interests - EU DisinfoLab," accessed December 26, 2021, https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/.

[58] "Research and Analysis Wing," in *Wikipedia*, December 24, 2021, https://en.wikipedia.org/w/index.php?title=Research_and_Analysis_Wing&oldid=1061877366.

[59] Ibid

[60] "Indian Cyber-Espionage Activity Rising amid Growing Rivalry with China, Pakistan," The Daily Swig | Cybersecurity news and views, February 25, 2021, https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan.

[61] Ibid.

contemporary times with the technological advancement of the world, the availability of a wide range of information that is easy to access almost made privacy fades away. One of the important examples of privacy was the United States vs. Antonio Jones when police use a GPS tracking device to track a criminal.[62] Pakistan is also facing severe privacy and espionage issues from local cyber-criminals and foreign-sponsored hackers.[63] According to the 2015, Snowden leak United States security agency NSA (National security agency) spied on Pakistan using different malicious software like "SECOND DATE" and breaches the security system of the Pakistan National Telecommunication Corporation known as NTC and its VIP Division.[64] This communication network is considered the backbone of the Pakistan communication network which is mostly used by civilians as well as military top brass to share confidential information. Pakistan is not only facing espionage threats from the West but also its regional rival India. India through its cyber power tries to manipulate Pakistan's cyber cleavages. India uses two malicious software "Horn Bill" and "Sun Bird" to target Pakistani officials.[65] They mostly targeted Pakistani intelligence officials, military officials, civilian officials who are heading strategically important institutions, and officials of Pakistan's nuclear authority. This software was used for espionage purposes where they fetched important information like text messages, emails, gallery, and GPS to track their location.[66] Moreover, Pegasus is notorious malicious software developed by Israeli and used by the Indian government against Pakistan and China for espionage purposes all of these details are revealed by a US-based company report.[67]

Counter Measures

Cyber warfare poses a significant threat to the security of Pakistan and countering it requires a multifaceted approach. Some of the ways in which states can counter cyber warfare are:

Develop a robust cybersecurity strategy: States need to develop a comprehensive cybersecurity strategy that outlines the policies, procedures, and mechanisms for protecting their critical infrastructure and data. The strategy should include a risk assessment, threat intelligence, incident response plans, and continuous monitoring.

Strengthen the legal framework: States need to strengthen their legal framework to criminalize cyber-attacks and provide law enforcement agencies with the necessary legal authority to investigate and prosecute cyber-crimes.

Develop a strong cybersecurity workforce: States need to invest in developing a strong cybersecurity workforce, including training cybersecurity professionals and recruiting experts from academia, industry, and government.

Enhance international cooperation: Cyber threats are often transnational, and states need

[62] "United States v. Jones," Oyez, accessed December 26, 2021, https://www.oyez.org/cases/2011/10-1259.
[63] Ibid.
[64] "UK Hacked Routers to Monitor Pakistan Communications Data: Snowden," accessed December 26, 2021, https://tribune.com.pk/story/968194/uk-hacked-routers-to-monitor-pakistan-communications-data-snowden.
[65] "US: Pro-India Malware Spying on Pakistan Military," accessed December 26, 2021, https://www.aa.com.tr/en/americas/us-pro-india-malware-spying-on-pakistan-military/2145536.
[66] "Scientists Create Their Own GPS by Spying on Internet Satellites | Science | AAAS," accessed January 26, 2023, https://www.science.org/content/article/scientists-create-their-own-gps-spying-internet-satellites.
[67] "US Company Believes India Used Its Software to Spy on Pakistan and China," accessed December 26, 2021, https://www.geo.tv/latest/371204-us-company-believes-india-used-its-software-to-spy-on-pakistan-and-china.

to enhance international cooperation to share threat intelligence, collaborate on cyber investigations, and work towards developing international norms and rules for cyberspace.

Improve the security of critical infrastructure: States need to improve the security of their critical infrastructure, such as energy, communication, and transportation networks, by implementing security measures such as access control, encryption, and intrusion detection and prevention systems.

Conduct regular cybersecurity assessments and audits: States should conduct regular cybersecurity assessments and audits to identify vulnerabilities and weaknesses in their systems and take appropriate measures to address them.

Encourage public-private partnerships: States should encourage public-private partnerships to promote information sharing, collaboration, and the development of cybersecurity solutions.

In conclusion, countering cyber warfare requires a concerted effort from states and a multifaceted approach that includes developing a robust cybersecurity strategy, strengthening the legal framework, developing a strong cybersecurity workforce, enhancing international cooperation, improving critical infrastructure security, conducting regular cybersecurity assessments and audits, and encouraging public-private partnerships.

Conclusion

Cyber warfare has had a significant impact on the national security of Pakistan in recent years. Pakistan, like many other countries, has increasingly become a target of cyber-attacks, both from state and non-state actors. These attacks have had various impacts on the country's national security. One of the most significant impacts of cyber warfare on Pakistan's national security has been the threat to its critical infrastructure, such as its energy and communication networks. Cyber-attacks on these networks could have a debilitating effect on the country's economy and its ability to function as a nation-state.

Another impact of cyber warfare on Pakistan's national security is the potential for espionage and data theft. Pakistan has a large military establishment, and its defense-related data and intelligence are highly sensitive. Cyber-attacks targeting these systems can lead to the loss of critical military and national security information, putting the country at risk. Cyber warfare has also been used as a tool to spread disinformation and propaganda, which can create social unrest and destabilize the country. In recent years, there have been instances of fake news and propaganda campaigns spreading through social media, which have created confusion and mistrust among the public.

To counter the impact of cyber warfare on its national security, Pakistan has taken several measures, including setting up cybersecurity agencies and improving its infrastructure security. Pakistan has also increased its focus on developing indigenous cybersecurity solutions and building the capacity of its cybersecurity workforce. In conclusion, cyber warfare has had a significant impact on the national security of Pakistan, and the country continues to face various cyber threats. Pakistan needs to remain vigilant and continue to invest in its cybersecurity capabilities to protect its critical infrastructure and defend against cyber-attacks.