ISSN Online: 3006-4708
ISSN Print: 3006-4694

SOCIAL SCIENCE REVIEW ARCHIVES

https://policyjournalofms.com

India-Pakistan in Cyberspace: Pakistan's Path to Cyber Resilience

Muhammad Shahzad Akram

Muhammad Shahzad Akram is a research officer at CISS-AJK. He holds and M.Phil. degree in IR from Quaid e Azam University Islamabad and also NESA Alumni

Abstract

The cyber conflicts between India and Pakistan, stemming from their longstanding geopolitical rivalry, have materialized in significant events such as the OGDCL virus attack and the Bhabha Atomic Research Centre hacking. These incidents exemplify the deliberate utilization of cyber methods for espionage, disruption, and propaganda, highlighting the intricate dynamics between governmental and non-governmental entities in the realm of cyber warfare. The attacks emphasize the susceptibility of essential infrastructure and the possibility of substantial economic and security consequences. This potential for significant repercussions should raise concern and awareness. In order to address these increasing threats, Pakistan must allocate resources towards developing strong cybersecurity systems, encourage collaboration between public and private sectors for sharing information on threats, participate in cyber diplomacy to establish global standards and cooperative mechanisms, improve the technical expertise of cybersecurity professionals through training programs, and update legal frameworks to combat cyber crimes and ensure responsibility effectively.

Key Words: Cyber Warfare, India-Pakistan Relations, Cyber Skirmishes, State-Sponsored Cyber Attacks, Cybersecurity, Cyber Espionage, Critical Infrastructure Protection Cyber Propaganda

Introduction

Warfare strategies encompass multiple dimensions and are characterized by advanced weapons and technology utilization. Non-lethal techniques are employed to carry out undercover operations against the enemy, particularly when the adversary possesses unconventional weaponry. Grey zone methods encompass a range of terms, including asymmetrical, unconventional, non-linear, non-kinetic, and sub-conventional, which describe these types of warfare tactics. Cyber warfare is a contemporary style of warfare. ICT has become a crucial and highly precarious security concern in the modern world *(Saud & Kazim, 2022).*

The academic community has shown significant interest in the cyber warfare between Russia and Western countries in recent years. A wide range of research work has been produced and available on the issue. These studies primarily focus on the purported online propaganda by Russia during the Ukrainian conflict *(Hoskins & Shchelin, 2018)* and the dissemination of false information campaigns online during elections in the United States and other European countries *(Hoskins & O'Loughlin, 2015; Lucas & Nimmo, 2015; Ramsay & Robertshaw, 2018)*. While concrete data about the direct impact of these digital campaigns on public opinion is lacking, experts believe that the extensive volume of content on social media platforms led to confusion and chaos among the general population *(Woolley & Howard, 2018).* Some argue that the achievements of pro-Trump and pro-Brexit campaigns prove that social media has been capable of influencing public opinion to a certain degree *(Bastos & Mercea, 2017; Freelon & Wells, 2020; Howard et al., 2016).*

In this study, we examine the digital conflict between India and Pakistan, two nuclear

archrivals, while shifting the focus away from Russia's information war against the West and its neighboring countries. Both countries have been actively involved in information warfare for decades *(Seth, 2016).* However, until now, scholarly research in this area has focused on traditional media *(Iqbal & Hussain, 2018; Seth, 2016),* and the dynamic realm of cyber warfare has yet to be investigated.

A groundbreaking study examined India's computerized dissemination of propaganda during conflicts with Pakistan *(Neyazi, 2019)*. However, currently, no similar study focuses on the Pakistani context. A systematic and objective study would be beneficial in examining the scope and orientation of digital information warfare in the Indian subcontinent.

It is essential to analyze this because the two countries, with a total population of 1.5 billion, have experienced significant adoption of social media during the last twenty years. Over 600 million individuals in India have internet connectivity. Similarly, in Pakistan, over 76 million individuals have internet connections, making it the 10th highest population of internet users globally *(Pakistan Telecommunication Authority, 2019)*. Indian Prime Minister Narendra Modi has around 60 million Twitter followers, but his Pakistani rival Imran Khan has more than 10 million Twitter followers. Based on the analysis conducted by Twitter audit (www.twitteraudit.com), it has been determined that 18% of Narendra Modi's followers are classified as false. In contrast, Shehbaz Sharif has 14% of his followers categorized as fraudulent. Similarly, the Pakistani military spokesperson has 3.9 million followers, out of which 15% are determined to be false followers. In comparison, the Indian counterpart has a more significant following of 6.6 million but with a higher percentage of fraudulent followers, amounting to 28%. While it is, debatable whether these individuals have intentionally generated phony followers or if the bots are following them due to their popularity, these accounts' sheer scale and extent are remarkable *(Neyazi, 2019)*.

Because of the low labor cost in the area, governments and militaries have employed large numbers of staff to spread propaganda on social media platforms. These staff members are paid for their work *(Cheema, 2020; Jorgic & Pal, 2019).* Several analysts and critics have highlighted the nationalistic and aggressive role played by these internet provocateurs in recent disputes *(Biswas, 2019; Chawla, 2020; Sriram, 2019).* In this study, we examine the digital information warfare that took place between India and Pakistan following the Pulwama attack on February 14, 2019, in the Indian-administered Kashmir. We also analyze the surgical strikes carried out by Indian forces in Pakistani territory on February 26, 2019, during which an Indian pilot was captured. Our analysis is based on relevant scholarly sources. Before delving into these events, a concise overview of the turbulent 73-year history of Indo-Pak ties is provided to offer a more comprehensive understanding of this subject.

India-Pakistan Relations

Both India and Pakistan achieved independence from the British Empire in 1947. However, shortly after gaining independence, the two nations conflicted, incorporating the princely state of Jammu and Kashmir *(Qadir, 2002).* Pakistan alluded to the independence agreement in which all Muslim states were to join Pakistan and Hindu states were to join India. Due to its predominantly Muslim population, Kashmir needed to be included in Pakistan. The Indian administration, however, asserted that the Hindu king of Kashmir had formally joined India, and hence, a vote was unnecessary. As a result, the initial Indo-Pak war erupted in 1948, resulting in the division of Kashmir into two regions: Pakistani-administered Kashmir and Indian-administered Kashmir.

Nevertheless, this partition failed to appease both governments, and in 1965, a significant conflict broke out between the two nations. The battle concluded following a peace truce, during which they both agreed to address their bilateral concerns *(Oh et al., 2011)*. In 1971, a third conflict arose between the two parties, resulting in the fragmentation of Pakistan. Bangladesh formed as an independent nation, previously a part of Pakistan *(Iqbal & Hussain, 2018)*.

In the 1970s, competition for military superiority began between the two nations, with significant missile and nuclear technology investments. In the latter half of the 1990s, they successfully exploded atomic bombs, so achieving the status of being nuclear-capable nations. However, it was not entirely practical despite the use of nuclear deterrence. As a result, in 1999, the two nations found themselves involved in the fourth conflict, generally referred to as the Kargil War. Nevertheless, this conflict was confined to the Kashmir region and did not escalate to other areas due to international pressure *(Rabasa et al., 2009).*

In addition to these four significant wars, several critical escalations have occurred in the preceding two decades. The Indian parliament attack in 2001, the Mumbai attack in 2008, and the Uri incident in 2016 are significant acts of violence for which India has accused Pakistan of colluding with militants *(Mathur, 2017).* Pakistan has made allegations against India, claiming that India has provided support and encouragement to the Pakistani Taliban, who are responsible for numerous lethal attacks *(Hussain, 2020; Hussain et al., 2021).* In addition, Pakistan alleges that India is assisting the insurgency in the resource-abundant province of Balochistan *(Hussain & Lynch, 2019; Hussain, 2015).*

Over the last two decades, Pakistan has seen exploitation of its cyberspace in the form of religious extremism, provocative and hate speech, anti-state propaganda, etc. However, over time, we have seen that social media has been used as a platform for most social, political, and religious movements. Furthermore, the government of Pakistan has neglected Pakistan's cyberspace as it lacks the will and capacity to draft/formulate an effective cyber policy. As we know, cyberspace is an anarchic and unregulated domain. It is abused by cyber-criminals and is considered a haven for terrorist organizations. Most non-state actor, especially terrorist organizations, uses cyberspace for recruitment, financial assistance (for example, an Uzbek terrorist who fought in Afghanistan, Iraq, and Syria used YouTube and other websites for fundraising), and communication purposes (*Foreign Policy*, 2022). Pakistan's dependency on the IT and telecom sector has rapidly increased, expanding Pakistan's cyberspace. Most of the cyberspace in Pakistan is unprotected and unsecured, which can be easily exploited.

India and Pakistan, Asian archrival, both fought four wars: 1948, 1965, 1971, and 1999. Both achieved nuclear weapon states at the beginning of the 21st century *(Lancelot, 2019).* However, after achieving atomic weapons, both states did not go for any full-scale conventional war. Moreover, hate against each other has been exaggerated, and this hate started deepening when India began to support anti-Pakistan elements in Baluchistan, FATA, and Afghanistan. This anger and frustration were outbursts through cyberspace as there is no authority to keep check and balance. Cyberspace is anarchic. There is no central authority because of its unruly nature and no checks and balances. It is used to abuse and humiliate emotionally and psychologically all over the world. In the cyber world, when a specific entity or group attacks another particular group, entity, or organization, which disrupts or destroys the system, it is known as a cyber-attack; these attacks came to Pakistan in the late 90s. In 1998, when the Indian Atomic Research Center was hacked, they accused Pakistan of this. Later, the investigation revealed that it was not from Pakistan but that a group of hackers from Europe and Russia were involved (*Madras Courier*, 2016). However, the blame game further provoked anger and hate against each other, which resulted in a series of low-level cyber-attacks between Pakistan and India. In 1999, four cyber-attacks were carried out from Pakistan. In 2000, the number increased to 72, and from the Indian side, 18 attacks were launched against Pakistan *(Shad, 2019).* However, this saga of virtual anger, hate, and aggression from the Indian side did not stop there. It started increasing with the emergence of private individual hacking groups like "Hindustan Hacker Organization" and "Team Nuts." They were involved in several cyber crimes against Pakistan *(Rehman, 2015).* It is believed that they hacked about 57 crucial websites of Pakistan state and private intuitions in a single day.

India Pakistan Cyber Skirmishes

Indian Cyber Army launched a cyber-attack on Pakistan on the anniversary of the 26/11 Mumbai attack. They hacked about 870 crucial websites, including about 34 essential

government institutions, including the Navy, the official websites of Chief Minister Sindh, the Foreign Ministry of Pakistan, etc. *(Tribune, 2022).* According to the ICA "Indian Cyber Army," the purpose of these attacks was to pay tribute to the martyred of 26/11. The Pakistani authority investigated the hacking of 870 websites, and the report reveals that the Technical Intelligence Agency of India, a parent organization of the National Technical and Research Organization, launched the attack. Moreover, the investigation also reveals that NTRO, "A National Technical and Research Organization," hired private hackers to launch a massive number of cyber-attacks on Pakistan state and private institutions (*Hacker,* 2022).

On the anniversary of the 1971 war, PCA, the "Pakistan Cyber Army," responded by launching a cyber-attack on Indian websites *(Dilipraj, 2013).* They hacked about 270 significant Indian websites, which include the official website of CBI, "Central Bauru of Intelligence." The CBI website was one of the worst affected websites. It remained unavailable for the user for about a month. They have to change all the websites' software to make it available to the user. The preliminary investigation of this cyber-attack reveals that those attackers were from Pakistan and based in Peshawar. The cyber security of the Indian Air Force system was compromised and provided back-door access to the CBI system.

In response to a cyber-attack from PCA "Pakistan Cyber Army" on Indian websites on the anniversary of 197, ICA Indian Cyber Army launched a Cyber-attack on the OGRA "Oil and Gas Regulatory Authority" *(Tribune, 2010).* A hacking group, "Jaguar Hacker," launched a cyber-attack on Pakistan on Jan/26/2012. In this attack, they posted a message saying there was nothing to worry about; it was our Republic Day. Just the index page was renamed (*India Time,* 2021).

Most of these hackers are private Individual hackers or group hackers. They attacked without the state's consensus. With the increase in attacks in cyberspace, state-owned and private institutions, as well as the governments of both states, stepped in. As the government stepped in, most of these hackers started fading away. However, according to ICA, the "Indian Cyber Army" and PCA, the "Pakistan Cyber Army," both have access to each other's systems; if any of them launched an attack, they are fully capable of responding.

Federal Bureau of Revenue (FBR)

Recently, one of the biggest cyber-attacks was carried out on FBR. This attack has raised serious questions about institutions' cyber security capabilities, compromising the security of millions of users' personal and sensitive information (*FBR,* 2020). As per the investigation, the real reason for the security breaches of FBR is obsolete hardware and pirated software. The Federal Board of Revenue uses the pirated version of Microsoft Hyper V software. The initial investigation reveals that pirated software is the main reason behind the cyber-attack. Moreover, Alice Walls, a United States diplomat and expert on South Asian affairs on his last visit, also accused the FBR of using pirated software, which the FBR denied in an official statement (*FBR,* 2020). The hacker not only hacked the official FBR websites but also compromised the security of its subdomain. A large amount of stolen data was put on sale at a Russian cyber forum for $30,000. The principal security engineer of Ebryx, while explaining the method of attack, argues that the attacker attached the malicious software code in an email, which is spoofed as an official email from the ministry. (Report, 2021) When FBR officials open that email, the virus is installed automatically and spread all over the network, and within no, the system is hacked. Moreover, over a week, about 1500+ FBR computer systems with confidential and sensitive information were stolen and sold online *(Kamran, 2021).*

Sindh High Court

Sindh High Court's official website has been hacked by an Indian hacker named "Indian Cyber Troops" (*Sindh High Court*, 2020). It is not the first time an Indian hacker has hacked any government institution's website. Historically, some cyber-attacks have been carried out from India to Pakistan. Most recently carried out cyber-attacks on Pakistani institutions were Swabi University, Sindh Finance Department's official website, and K Electric *(Ikram, 2020).*

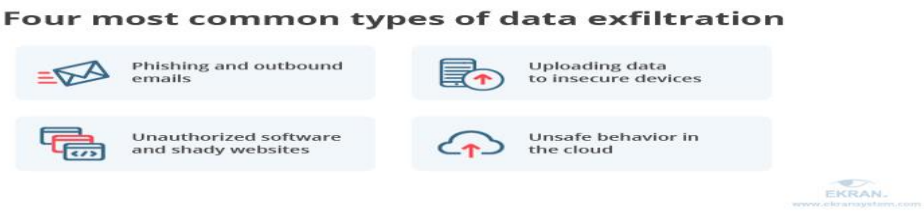
Patari
PATARI is a renowned Pakistani online music-streaming website similar to SoundCloud and Spotify. Recently, it was hacked, resulting in the loss of sensitive personal data of more than 250,000 users (Patari, 2020). The hacked data was leaked on Russian and English forums and is available for sale.

K Electric
K Electric is a Karachi-based electric company mainly responsible for supplying electricity to the Karachi metropolitan area. Last year, K Electric's security was compromised, and sensitive data was stolen from its database *(Hashim, 2020)*. Moreover, the hacker also threatened the K Electric administration to pay the ransom of about $3.5 million, which, if not paid, will be doubled within a week. The ransom doubled after a week of $7 million, but K Electric still did not pay much attention, and all the stolen information was leaked online for sale *(Hashim, 2020)*. K Electric has millions of users and customer-sensitive data, i.e., customer name, address, CNIC, and bank account details. Moreover, K Electric did not pay any ransom to the hacker, nor did they try to improve their cyber security, and the hacker leaked 8.5 GB of data.

Meezan Bank
In contemporary times, the banking sector is more vulnerable to cyber-attacks than other sectors, mainly because of financial interests and its poor cyber security system. Meezan Bank is also one of those banks with inadequate cyber security arrangements. This poor cyber security arrangement compromised the bank's security. The bank was hacked, and about 69,189 details were sold online (*Economist, 2022*). Moreover, this security breach caused the bank about $3.5 million in data loss *(Zaidi, 2022).*

Bank Islami
In contemporary times, the banking sector is more vulnerable to cyber-attacks than other sectors. Because of the financial interest and poor cyber security system, Bank Islami is also one of those banks. In 2018, a massive cyber-attack against Pakistan's economic sectors, mainly the banking sector, was the key target. This attack affected Pakistan's banking sector and breached the cyber security of almost all banks, and about 20,000 users' data were stolen. The bank Islami lost about $6 million along with the suspension of some services (*Pakistan Today*, 2020). The hacker mainly targeted debit card users and stole millions of dollars. Moreover, many user-sensitive data has been dumped on the dark web. It also stated that about 11000 debit card details from 22 banks were included in that data *(Pakistan Today, 2020).*

Types of Cyber Attack
Information exfiltration
These types of cyber-attacks are longer lasting. A full-scale attack may take from one minute to years. They mainly aim to steal sensitive information about state intuition, e.g., armed forces, defense, national security, and critical infrastructure. The opponent can use such sensitive information as a tool to manipulate.



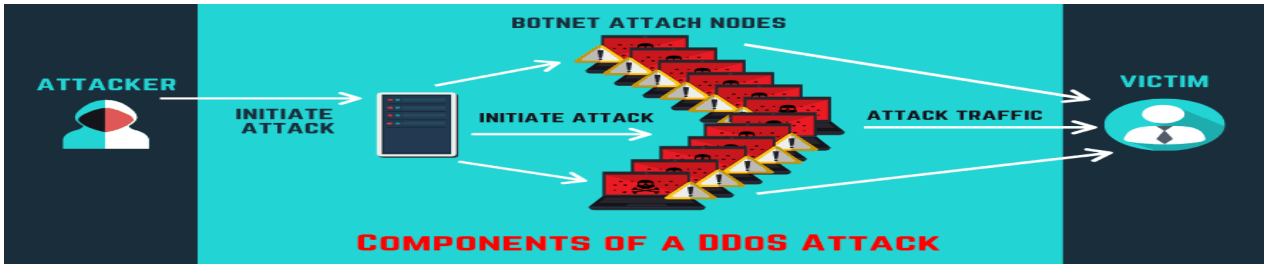
Source https://www.ekransystem.com/en/blog/prevent-data-exfiltration

Direct Disruption

Direct disruption, also known as de traditional destruction, is another method of cyber-attack. Attackers usually use virtual methods to stop any physical program or operation in this attack—for example, the Stuxnet attack on Iran's nuclear facility. A malign, vicious code disrupts the opponent's system in these cyber-attacks *(Tunggal, 2022)*. The primary objective is to make any security unit of the opponent state dysfunctional. In these types of cyber-attacks, different methods were used to achieve the purpose; for example, deletion of sensitive information and stolen important information also cause physical damage like they did in Iran, but the chances of physical damage are rare.

Cyber Blockade

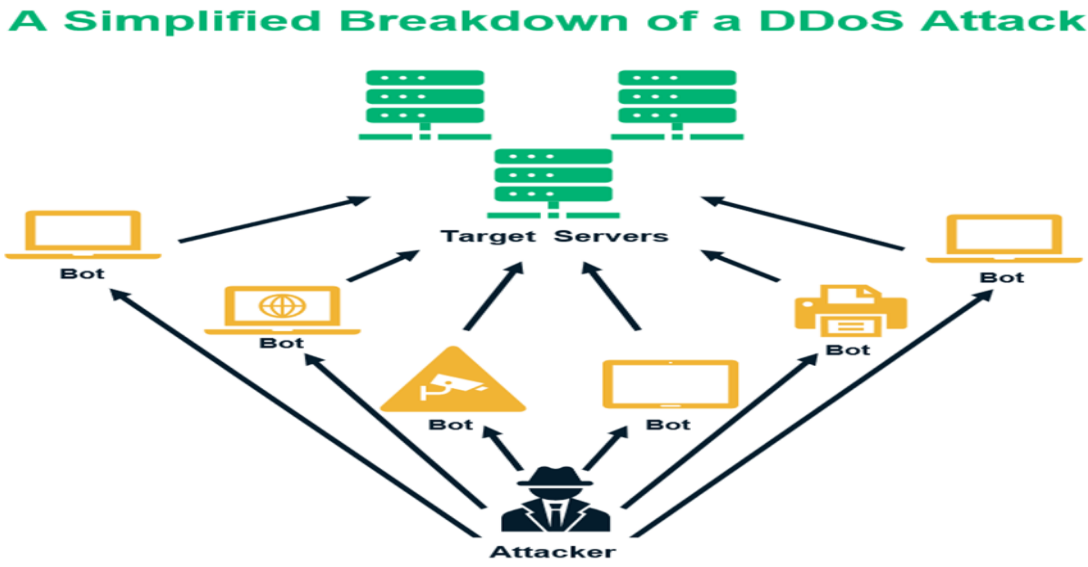
In this cyber-attack, attackers usually target a specific entity, like an organization or an institution. When different computer systems are under attack, they are disconnected from the Internet due to heavy traffic. Many DDoS attacks were carried out to block traffic or overload the server. These attacks were not long-lasting *(The DOD, 2019)*. They can be overcome within an hour.



Source *https://phoenixnap.com/blog/cyber-security-attack-types*

Enabling Attackers

In enabling cyber-attacks, attacks were carried out against the military deployment, strategically important bases, their communication system, air defense system, and missiles to help the military in their conventional warfare as Russia did to Georgia during the Georgian attack. Most of these attacks were DDoS, a Cyber blockade type *(Kumar & Carley, 2016).*



Source of the Picture "A simplified breakdown of DDoS attack

Information Manipulation

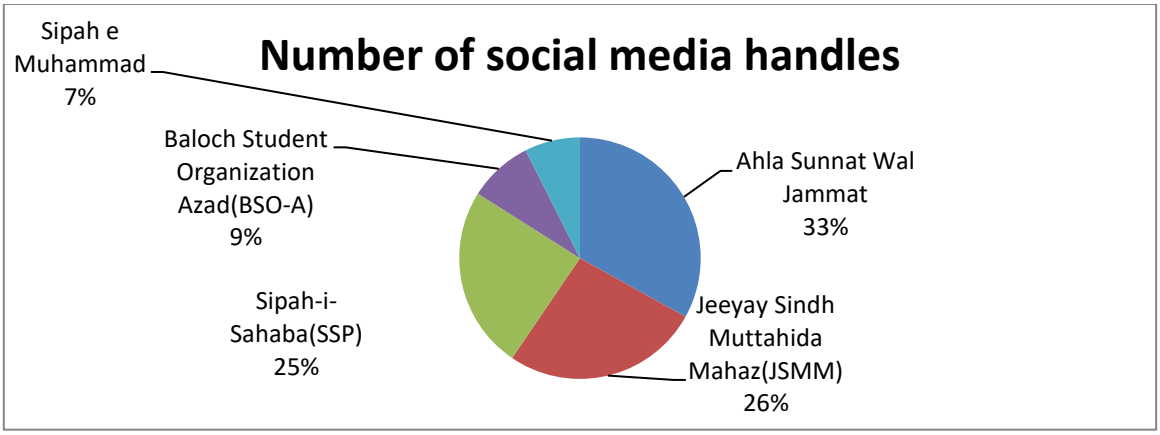
In contemporary times, information manipulation is another type of cyber-attack. It is also known as information warfare. In this attack, information used in strategic planning, policy-making, and other activities was manipulated, fake information was exchanged with original fake news, and false information was circulated for propaganda *(RAND, 1996).* Information

manipulation is done on a specific objective to achieve an important goal. For example, during the TLP protests and clashes with police's different hashtags, the #Civil war in Pakistan was floating all over the internet. Moreover, misinformation has also spread against CPEC, labeling it a modern-time East India Company *(Pak, Observer, 2023).*

Cyber Warfare and Pakistan

Today, the world population is about 7.7 billion, of which 4.66 billion use the internet. That is about 59.5% of the population, and about 92.6% of the population access the internet via mobile phone (*Statista*, 2021). Out of the total 7.7 billion people in the world, about 226 million live in Pakistan, of which 61.34 million have internet access. (*PTA*, 2019). With technological advancement, telecommunication has revolutionized the world, but cyberspace is still considered a haven for criminal activities. (*PTA*, 2019.). During the early 90s, the internet became a new mode of fighting the hub of illegal activities as most of cyberspace is lawless, and there is no central authority *(PTA, 2019*).

Cyber is a recently emerged phenomenon because most states and individuals lack a basic understanding of it, and no such prominent law has been passed for its proper regulation. Therefore, the anarchy in cyber bonus for non-state actors, terrorist organizations, individual hackers, and cyber-criminals as the world transformed from physical means to cyber also transformed the warfighting strategy from conventional to cyber/virtual terrorism. (*Critical Infrastructure*, 2018.) Cyber-attacks on any state's critical infrastructure are one of the biggest threats to national security, and cyber-warfare is much more destructive than conventional. However, warfare mode has changed, but the objective remains the same as during conventional: psychological, political, religious, ideological, and economic. The rise of cyber provides an upper hand to the offensive attacker, who can easily exploit the opponent's system weakness and even global enterprises. For example, Sony's entrainment could not save itself from cyber hacking, and the security of the United States Office of Personal Management was compromised (*CFR*, 2015.) The security loopholes in cyber security provide an excellent opportunity for the non-state actor to attack, hack, and steal sensitive data if not detected, then cyber espionage, even crippling and sabotaging the entire system. Terrorist organizations like ISIS, ISIL, AL Qaeda, and Hijab-ut-Tahurr use the cyber as a medium to incorporate their radical agenda. They use social media by writing blogs for recruitment and creating familiarity with its ideology. According to PTA (Pakistan Telecommunication Authority), recent statistics show that today's 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% of the population access the internet via mobile phone (*Statista*, 2023). Out of the total 7.7 billion people in the world, about 226 million live in Pakistan, of which 61.34 million have internet access (*Pakistan Has More than 181 Million Mobile Subscribers: PTA*, n.d.) Pakistan's internet users have increased rapidly. Social media users increased by almost five times in 2015, primarily young people between 15 and 25. The anarchic cyberspace is a haven for terrorists and extremists. They can easily exploit the young people through their nefarious agenda using religion. Most terrorist, extremist, and radical organization have their social media handles on Facebook, YouTube, and Twitter (*US Designates Hizbul Mujahideen as a Foreign Terrorist Group – The Diplomat*, n.d.). Hizbul Islam and RSS (Rashtriya et al.) use social media platforms to upload their daily training session, and they launched a militant cartoon series for children to create familiarity with their ideology. Moreover, "Alqal" is the official website of a banned outfit in Pakistan. It works to promote its ideology (*Shandler, 2021*). The globally renowned terrorist organization Al Qaeda has Facebook pages with more than 250 million members, and they have a contributor forum with almost 50,000 to 100,000 active contributors and supporters named "Al Falaja."



Source: Made by Researcher

According to the Brooking investigation, Twitter has banned about 500,000 Twitter handles belonging to ISIS and other terrorist organizations. According to the Dawn leaks, the Pakistani government has banned 64 outfits involved in terrorist and extremist activities, and 41 of them are still active on social media (*DAWN, 2018*).

Moreover, India is also exploiting cyberspace to provoke religious sentiments in Pakistan and promote terrorist activities; for example, the Pakistani authority investigated the hacking of 870 websites in 2010, revealing that the attack was launched by a Technical intelligence agency of India, a parent organization of National Technical and research organization carried out a high-level investigation *(Gul, 2024)*. Moreover, the investigation also reveals that NTRO, "A National Technical and Research Organization," hires private hackers to launch massive cyber-attacks on Pakistan state and private institutions *(Khalid, 2023).*

Source: Twitter

As far as Pakistani cyber security is concerned, the government lacks the will and interest to develop a proper policy for cyberspace and regulation, and individuals lack understanding and awareness of it. According to unofficial resources, the government of Pakistan is spending less than 1% on cyber security, which is much less than our neighbors India and Iran (*Pakistan Today*, 2023).

The cyber-attack is unlike a conventional attack, as it has a much more severe impact on the adversary's critical infrastructure. In contemporary times, low-level cyber-attacks (these millions in number per day) are considered part of low-level cyber conflict. Cyber espionage is digitally spying on adverse and passing the sensitive data back to the host *(Daily, 2023).* Pegasus is a malicious code that can infiltrate your device without your consent and permission, like a missed call, a text message, or a WhatsApp message. According to the WhatsApp report,

this virus has compromised about 1400 phones' security and is increasing *(WhatsApp, 2018).* Once your phone is hacked, the hacker can read your text messages, WhatsApp messages, and emails, view your calendar and browser history, and track your location. Moreover, it can also record your calls, open your phone camera, record your video, and turn your phone into a surveillance device.

The Intercept reported that during these operations, the NSA also hacked the security of the National Telecommunication Corporation to spy on Pakistan's civil and military leadership *(Intercept, 2019)*. The NSA also uses the "Second Data" tool to hack the Pakistani NTC. Moreover, India uses malicious software named "Hornbill" and Sun Bird" to spy on Pakistan's military and civilian officials. Horn Bill and Sun Bird fetched sensitive information, such as text messages, location, emails, photos, and other data on the phone. This stolen information was later used against the adversary. The fear is that using cyberspace as a full-scale battleground against each other in a race of domination and power superiority will lead to World War III.

Counter Measures for Pakistan

Implementing prevention methods is crucial for protecting organizations and individuals from cyber dangers. These proactive methods and practices aim to reduce vulnerabilities and lessen the danger of cyberattacks. Here, we present a concise summary of essential preventative tactics:

Software Update Management: Patch management regularly applies updates and patches to software, operating systems, and applications. These updates frequently include crucial security patches that target identified vulnerabilities. Efficient patch management minimizes vulnerabilities that cybercriminals can exploit, decreasing the likelihood of successful assaults (*Akram et al., R. (2023*).

Training on Security Awareness: Human mistakes significantly contribute to cybersecurity vulnerabilities. Security awareness training is designed to instruct staff and users on potential dangers and how to identify and react to them. It enables individuals to be more alert, particularly when it comes to typical methods of assault such as phishing and social engineering.

Intrusion Detection and Prevention Systems (IDPS) are crucial tools for monitoring and protecting against real-time security breaches. The analysts examine network traffic and system activity, identifying and flagging or obstructing suspicious behavior. These solutions aid organizations in promptly identifying and addressing possible security events, thereby preventing or reducing harm.

The zero-trust security model disrupts the conventional concept of trust in network systems. It functions based on the philosophy of "never rely, always confirm." This strategy necessitates ongoing authentication of the identity and reliability of devices and users, irrespective of their position within or outside the network.

Access control refers to managing permissions for accessing specified resources or locations inside a network. The notion of least privilege is crucial in this context, as it guarantees that users are granted only the essential degree of access required to carry out their activities. This reduces the scope of potential attacks and restricts the potential harm that can be caused.

This method involves segregating essential resources from the more extensive network, making it more difficult for attackers to navigate horizontally within the network in the event of breaching one section.

Threat intelligence offers organizations up-to-date information regarding developing risks and vulnerabilities. This data enables organizations to preemptively modify their security procedures and defenses to successfully handle evolving cyber threats.

Regular security audits and testing, including vulnerability assessments, penetration testing, and security audits, are crucial for discovering flaws in an organization's defense systems. These evaluations aid in determining the order of importance for mitigation endeavors and guarantee the continued efficacy of security measures. Multi-factor authentication (MFA) is a

security measure that requires users to submit various kinds of verification to gain access. Including this extra level of security dramatically diminishes the likelihood of unauthorized entry, even if credentials are compromised. Continuous monitoring is essential for rapidly recognizing and responding to network and system activity irregularities. Organizations can use it to detect and address security risks as they occur promptly.

User and Entity Behavior Analytics (UEBA) refers to using advanced technology to examine and analyze the behavior of users and entities to detect and identify any unusual patterns or deviations from the expected norm. These observations can assist organizations in identifying security breaches or internal dangers.

Regular backup and recovery processes are essential for safeguarding valuable data. Backups expedite prompt restoration in the event of data loss caused by cyberattacks or other catastrophes.

Bibliography

Researchers say 4G is vulnerable to the same attacks as 3G. (2018, July 2). Cyber Scoop. https://cyberscoop.com/4g-vulnerable-types-attacks-3g-researchers-say/

12-Month Review of Revised FATF Standards—Virtual Assets and VASPs. (n.d.). Retrieved February 15, 2023, from https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html

admin. (2019, November 6). China-Pakistan Cyber Security Cooperation. Pakistan Observer. https://pakobserver.net/china-pakistan-cyber-security-cooperation/

Ahmad, S. (2022). CYBER SECURITY THREAT AND PAKISTAN'S PREPAREDNESS: AN ANALYSIS OF NATIONAL CYBER SECURITY POLICY 2021. Volume No. 05(Issue No. 01 (June, 2022)), 16. https://doi.org/10.37605/pjhssr.v5i1.381

Akram, M. S., Mir, M. J., & Rehman, A. (2023). Dimension Of Cyber-Warfare In Pakistan's Context. Journal of Positive School Psychology, 7(6), Article 6.

Aquila, G. (n.d.). The Stuxnet Worm The Nexus of Cyber Security and International Policy.

Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? (n.d.). New America. Retrieved February 10, 2023, from http://newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Comparative Strategy, 12(2), 141–165.

Digital Shadows: The Menace of Cyber Espionage and Pakistan's National Security | Journal of Development and Social Sciences. (n.d.). Retrieved August 2, 2024, from https://www.ojs.jdss.org.pk/journal/article/view/743

Banks, W. C. (2016). Cyber espionage and electronic surveillance: Beyond the media coverage. Emory LJ, pp. 66, 513.

Barrett, A. M. (2016). False alarms, actual dangers. RAND Corporation Document PE-191-TSF, DOI, 10.

Big Data and AI - A Quick Overview. (n.d.). Retrieved February 21, 2023, from https://indatalabs.com/blog/big-data-tech-and-ai

Campbell, D. (1985). Nuclear War and Computer-Generated Nuclear Alerts. Brigham Young University Studies, pp. 77–90.

Chinese cyber attack: Why Maharashtra should worry. (n.d.). India Today. Retrieved September 20, 2023, from https://www.indiatoday.in/india-today-

insight/story/chinese-cyber-attack-why-maharashtra-should-worry-1774905-2021-03-02

Cimbala, S. J. (2016). Nuclear Deterrence in Cyber-ia: Challenges and Controversies. Penn State Brandywine Media United States.

Cyber Espionage A Big Threat. (2023, April 30). https://www.pakistantoday.com.pk/2023/04/30/cyber-espionage-a-big-threat/

Cyber Espionage: National Security in the Digital Age | Wilson Center. (n.d.). Retrieved August 17, 2023, from https://www.wilsoncenter.org/video/cyber-espionage-national-security-digital-age

Cyber Power – Tier Three. (n.d.). Retrieved July 4, 2023, from https://www.iiss.org/en/research-paper/2021/06/cyber-power---tier-three/

Cyber Security Strategy—An overview | ScienceDirect Topics. (n.d.). Retrieved July 4, 2023, from https://www.sciencedirect.com/topics/computer-science/cyber-security-strategy

Cyber Security: Where Does Pakistan Stand? (n.d.). Retrieved January 26, 2023, from https://think-asia.org/handle/11540/9714

Cyber threat landscape—Establishing a resilient ecosystem. (2021, December 8). The Nation. https://nation.com.pk/08-Dec-2021/cyber-threat-landscape-establishing-a-resilient-ecosystem

Cybercrime A New Frontier of Organized Crime. (n.d.).

Cybercrime may. (2018, February 21). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

De Silva, E. (2015). National security and counterintelligence in the era of cyber espionage. IGI Global.

"Dodgy bank, poppy cultivation": New book tells how Pakistan raised money for nuclear weapons. (n.d.). Retrieved August 12, 2023, from https://theprint.in/softcover/dodgy-bank-poppy-cultivation-new-book-tells-how-pakistan-raised-money-for-nuclear-weapons/1686657/

Eugenie, de S. (2015). National Security and Counterintelligence in the Era of Cyber Espionage. IGI Global.

Firdous, M. A. (2018). Formulation of Pakistan's cyber security policy. CISS Insight Journal, 6(1), 70–94.

Global disruption of 3 terror finance cyber-enabled campaigns | ICE. (n.d.). Retrieved February 15, 2023, from https://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns

Internet users in the world 2021 | Statista. (n.d.). Retrieved October 25, 2021, from https://www.statista.com/statistics/617136/digital-population-worldwide/

Banking card data worth $3.5 million was stolen for online sale. (n.d.). Retrieved October 25, 2021, from https://www.thenews.com.pk/print/435450-banking-cards-data-worth-3-5mln-stolen-for-online-sale

BankIslami lost $6m within 23 minutes in cyber attack | Pakistan Today. (n.d.). Retrieved October 25, 2021, from https://archive.pakistantoday.com.pk/2018/12/21/bankislami-lost-6m-within-23-minutes-in-cyber-attack/

Broadband users in Pakistan shoot up to 100 million: PTA. (n.d.). Retrieved October 25, 2021, from https://www.thenews.com.pk/latest/814261-broadband-users-in-pakistan-shoot-up-to-100-million-pta

Chief of WhatsApp, which sued NSO over alleged hacking of its product, disputes the firm's denials on the scope of involvement in spyware operations. (n.d.). *Washington Post*. Retrieved August 14, 2021, from https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/

Connect the Dots on State-Sponsored Cyber Incidents—Compromise at the Office of Personnel Management. (n.d.). Council on Foreign Relations. Retrieved July 31, 2024, from https://www.cfr.org/cyber-operations/compromise-office-personnel-management

Critical Infrastructure: Control Systems and the Terrorist Threat. (n.d.). Retrieved October 28, 2021, from https://www.everycrsreport.com/reports/RL31534.html

Digital Shadows: The Menace of Cyber Espionage and Pakistan's National Security | Journal of Development and Social Sciences. (n.d.). Retrieved August 2, 2024, from https://www.ojs.jdss.org.pk/journal/article/view/743

Dilipraj, E. (2013). *Cyber Warfare and National Security: An Analysis of Incidents Between India and Pakistan*. *8*, 173–187.

FBR is Investigating The Hacker Behind Recent Cyber Attack. (n.d.). Retrieved October 25, 2021, from https://propakistani.pk/2021/09/05/fbr-is-investigating-the-hacker-behind-recent-cyber-attack/

Hashim, A. (2020, September 14). *Pakistan's Power Utility K-Electric Suffered Ransomware Attack*. Latest Hacking News. https://latesthackingnews.com/2020/09/14/pakistans-power-utility-k-electric-suffered-ransomware-attack/

Indian cyber-espionage activity is rising amid growing rivalry with China and Pakistan. (2021, February 25). The Daily Swig | Cybersecurity News and Views. https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan

Individuals using the Internet (% of the population) | Data. (n.d.). Retrieved October 25, 2021, from https://data.worldbank.org/indicator/IT.NET.USER.ZS

Kumar, S., & Carley, K. M. (2016). Understanding DDoS cyber-attacks using social media analytics. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, pp. 231–236.

Mapping Global Cyberterror Networks: An Empirical Study of Al-Qaeda and ISIS Cyberterrorism Events—Claire Seungeun Lee, Kyung-Shick Choi, Ryan Shandler, Chris Kayser, 2021. (n.d.). Retrieved October 28, 2021, from https://journals.sagepub.com/doi/abs/10.1177/10439862211001606

Media Center | PTA. (n.d.). Retrieved October 25, 2021, from https://www.pta.gov.pk/en/media-center/single-media/ptas-response-to-hootsuites-digital-2019-pakistan-report-210619

Neglect caused the FBR cyber-attack. (n.d.). Retrieved October 25, 2021, from https://tribune.com.pk/story/2316604/neglect-caused-fbr-cyber-attack

Pakistan has more than 181 million mobile subscribers: PTA. (n.d.). Retrieved October 28, 2021, from https://www.geo.tv/latest/350516-pakistan-has-more-than-181-million-mobile-subscribers-pta

Pk: Sindh High Court Website Hacked By Indian Hackers. (n.d.). Retrieved October 25, 2021, from https://www.databreaches.net/pk-sindh-high-court-website-hacked-by-indian-hackers/

Rehman, J. H. | A. (2015, July 28). *Hacking Team hacked: The Pakistan connection and India's expansion plan*. DAWN.COM. http://www.dawn.com/news/1196767

Report, R. (2021, September 13). *FTO orders probe into FBR cyber attack issue*. Brecorder. https://www.brecorder.com/news/40119824

Rs2bn was released to upgrade the cybersecurity apparatus: Minister—Pakistan Today. (n.d.). Retrieved October 28, 2021, from https://www.pakistantoday.com.pk/2021/09/27/rs2bn-released-to-upgrade-cyber-security-apparatus-minister/

Saud, A., & Kazim, N. (2022). Disinformation and Propaganda Tactics: Impacts of Indian Information Warfare on Pakistan. *Journal of Indian Studies*, *8*(02), 335–354.

Shad, M. R. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan. *Strategic Studies*, *39*(1), 1–19.

The Blackwater of Jihad – Foreign Policy. (n.d.). Retrieved October 25, 2021, from https://foreignpolicy.com/2017/02/10/the-world-first-jihadi-private-military-contractor-syria-russia-malhama-tactical/

The Cyber Threat Facing Pakistan. (n.d.). Retrieved August 10, 2021, from https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/

The Need for Détente: Cyberwarfare in India/Pakistan Conflict | Small Wars Journal. (n.d.). Retrieved October 25, 2021, from https://smallwarsjournal.com/jrnl/art/need-detente-cyberwarfare-indiapakistan-conflict

US Designates Hizbul Mujahideen as a Foreign Terrorist Group – The Diplomat. (n.d.). Retrieved October 28, 2021, from https://thediplomat.com/2017/08/us-designates-hizbul-mujahideen-as-a-foreign-terrorist-group/

US NSA spying on Pakistan's mobile networks: WikiLeaks | Business Standard News. (n.d.). Retrieved October 25, 2021, from https://www.business-standard.com/article/international/us-nsa-spying-on-pakistan-s-mobile-networks-wikileaks-117041100888_1.html

When India's Nuclear Secrets Were Hacked | Madras Courier. (n.d.). Retrieved October 25, 2021, from https://madrascourier.com/opinion/when-indias-nuclear-secrets-were-hacked/

Hachigian, N. (2001). China's cyber-strategy. Foreign Affairs, 118–133.

Hacking Team hacked: The Pakistan connection, and India's expansion plan—Pakistan—DAWN.COM. (n.d.). Retrieved January 25, 2023, from https://www.dawn.com/news/1196767

How China built a one-of-a-kind cyber-espionage behemoth to last. (n.d.). MIT Technology Review. Retrieved February 10, 2023, from https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/

How Realistic Are China's Plans to Expand CPEC to Afghanistan? – The Diplomat. (n.d.). Retrieved January 29, 2023, from https://thediplomat.com/2022/12/how-realistic-are-chinas-plans-to-expand-cpec-to-afghanistan/

How the CIA can get from spy to cyberspy | Wilson Center. (n.d.). Retrieved February 10, 2023, from https://www.wilsoncenter.org/article/how-the-cia-can-get-spy-to-cyberspy

Irandoost, D. H. (2018, May 3). Cybersecurity: A National Security Issue? E-International Relations. https://www.e-ir.info/2018/05/03/cybersecurity-a-national-security-issue/

Johnson, J. (2019). The AI-cyber nexus: Implications for military escalation, deterrence, and strategic stability. Journal of Cyber Policy, 4(3), 442–460.

Johnson, J. (2021). The AI-cyber security nexus. In Artificial intelligence and the future of warfare (pp. 150–167). Manchester University Press.

Khan, S., & Butt, K. M. (n.d.). Cyber Technology, Radicalization and Terrorism in Pakistan. Journal of Indian Studies.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (2015). China and Cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford University Press, USA.

Malik, Z. U. A., Xing, H. M., Malik, S., Shahzad, T., Zheng, M., & Fatima, H. (2022). Cyber security situation in Pakistan: A critical analysis. PalArch's Journal of Archaeology of Egypt/Egyptology, 19(1), 23–32.

Matheson, W. (2020). The Cyber-Nuclear Nexus in East Asia: Cyberwarfare's Escalatory Potential in the US-China Relationship. Intersect: The Stanford Journal of Science, Technology, and Society, 14(1).

Maxwell, P. (2020, April 20). Artificial Intelligence is the Future of Warfare (Just Not in the Way You Think). Modern War Institute. https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. Daedalus, 140(4), 70–92.

Nanda, P. (2023, May 25). Cyber Army! US Mulls Creating A New Military Unit That Can "Track & Whack" Chinese, Russian Aggression. Latest Asian, Middle-East, EurAsian, Indian News. https://www.eurasiantimes.com/cyber-military-us-mulls-creating-a-new-army-unit-that-can-counter/

Nandrajog, E. (n.d.). Hindutva and Anti-Muslim Communal Violence in India Under the Bharatiya Janata Party (1990-2010).

NTSB report on cyber security—Google Search. (n.d.). Retrieved July 4, 2023, from https://www.google.com/search?q=ntisb+report+on+cyber+security&bih=714&biw=1536&hl=en&sxsrf=AB5stBj9u_rXhbFXYivM9djZrBXS2_wUyA%3A1688452744326&ei=iL6jZOrLE9a7kdUPwJWp2Ag&oq=ntisb+report+on+cyber&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQAxgBMgcIIRCgARAKMgcIIRCgARAKOgoIABBHENYEELADOgQIIxAnOgcIIxCKBRAnOgUIABCABDoECAAQHjoGCAAQBRAeOgUIIRCgAToHCAAQDRCABDoGCAAQHhANOggIABAIEB4QDToICAAQigUQhgNKBAhBGABQ5wNY9yxg9ThoAXABeACAAcEDiAHzQpIBCDItMy4xMi45mAEAoAEBwAEByAEF&sclient=gws-wiz-serp#ip=1

O'Hara, G. (2010). Cyber-Espionage: A growing threat to the American economy. CommLaw Conspectus, pp. 19, 241.

Onugha, C. V. (2018). Partners in national cyber security strategy? An analysis of the cyber security strategies of the Ministry of Defence and police in the UK [PhD Thesis]. London Metropolitan University.

Pakistan's Cybersecurity Policy in 2021: A Review. (n.d.). ISACA. Retrieved July 4, 2023, from https://www.isaca.org/resources/news-and-trends/industry-news/2021/pakistans-cybersecurity-policy-in-2021-a-review

(PDF) A guileful ruse: ISIS, media, and tactics of appropriation | Piotr Szpunar—Academia.edu. (n.d.). Retrieved February 15, 2023, from https://www.academia.edu/37523301/A_guileful_ruse_ISIS_media_and_tactics_of_appropriation

Raud, M. (2015). China and cyber: attitudes, strategies, and organization. Cyber Research Workshop 2015, p. 12.

Rawat, R., Mahor, V., Chirgaiya, S., & Garg, B. (2021). Artificial cyber espionage-based protection of technologically enabled automated cities infrastructure by dark web cyber offenders. Intelligence of Things: AI-IoT Based Critical-Applications and Innovations, 167–188.

Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). An Analysis of Cyber Espionage Process. Developments and Advances in Defense and Security: Proceedings of MICRADS 2021, 3–14.

Rosli, W. R. W., Kamaruddin, S., Mohamad, A. M., Saufi, N. N. M., & Hamin, Z. (2021). They govern cyber espionage threats via the integration of the risk society-cyber securitisation theory. 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), 1–7.

Saud, A., & Kazim, N. (2022). Disinformation and Propaganda Tactics: Impacts of Indian Information Warfare on Pakistan. Journal of Indian Studies, 8(02), 335–354.

Schneider, J. (2020). A strategic cyber no-first-use policy? Addressing the US Cyber strategy problem. The Washington Quarterly, 43(2), 159–175.

Shin, S. H. (2022). The Cyber-Nuclear Nexus and its Impact on the Stability of the International Security Order. Journal of Peace and Unification, 12(4), 79–110.

Shoaib, M. (n.d.). The Cyber-Nuclear Nexus and Threats to Strategic Stability.

Staff, S. (2013, February 25). Digital Spying Burdens German Relations with Beijing. Der Spiegel. https://www.spiegel.de/international/world/digital-spying-burdens-german-relations-with-beijing-a-885444.html

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

United Nations Conference on Trade and Development. (2021). Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow. United Nations. https://doi.org/10.18356/9789210058254

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). Cyber strategy: The evolving character of power and coercion. Oxford University Press.

Vitel, P., & Bliddal, H. (2015). French cyber security and defense: An overview. Information & Security, 32(1), 1.

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. Minn. J. Int'l L., 22, 347.

What is Cyber Espionage | VMware Glossary. (n.d.). VMware. Retrieved February 10, 2023, from https://www.vmware.com/topics/glossary/content/cyber-espionage.html

Why U.S.-China AI Competition Matters from Essay: Reframing the U.S.-China AI "Arms Race": Why This Framing is Not Only Wrong But Dangerous for American Policymaking on JSTOR. (n.d.). Retrieved February 21, 2023, from https://www.jstor.org/stable/resrep19970.6

Wolfers, A. (1952). "National Security" as an Ambiguous Symbol. Political Science Quarterly, 67(4), 481–502. https://doi.org/10.2307/2145138

Wuermeling, U. (1989). New dimensions of computer crime—Hacking for the KGB — A report. Computer Law & Security Review, 5(4), 20–21. https://doi.org/10.1016/0267-3649(89)90055-1