P-ISSN: 2709-6254	Journal of Development and Social Sciences	Jul-Sep 2023, Vol.4, No.3
O-ISSN:2709-6262	http://dx.doi.org/10.47205/jdss.2023(4-III)80	[874-887]

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

RESEARCH PAPER

Digital Shadows: The Menace of Cyber Espionage and Pakistan's National Security

[1]Muhammad Shahzad Akram* [2] Rimsha Malik

1. Research officer, Centre for International Strategic Studies (CISS) AJK, Pakistan
2. Associate Research Officer, Centre for International Strategic Studies (CISS) AJK, Pakistan

***Corresponding Author:** Mshahzada22@gmail.com

ABSTRACT

This study aims to comprehensively explore the phenomenon of cyber espionage and its profound impact on Pakistan's national security, shedding light on its implications for international relations, military and nuclear security, economic stability, and critical infrastructure. Cyber espionage, as conducted among nation-states, involves the surreptitious use of computer-based attacks and intelligence-gathering techniques by one country to obtain sensitive information or a competitive advantage over another. This clandestine activity has redefined the nature of modern warfare, necessitating a deeper understanding of its consequences. The research methodology employed is qualitative in nature. The systematic literature review entails a meticulous examination of data sources, encompassing journal articles and various websites. The findings underscore the gravity of cyber espionage as a threat to Pakistan's sovereignty, emphasizing the need for a proactive stance in safeguarding sensitive data and critical infrastructure. This study recommends the development of robust cybersecurity measures, regular security assessments, Implementing an incident response plan, fostering a culture of security, and Working with law enforcement as essential steps to counter the evolving threat landscape posed by cyber espionage.

KEYWORDS Cyber Espionage, Cyber-command, Cyber-deterrence, National Security

Introduction

Cyber espionage, or the use of digital means to gather sensitive information from other countries or organizations, has a relatively short history. However, it has evolved rapidly over the past few decades. The first known instance of cyber espionage occurred in the 1980s when the Soviet Union was known to have used computer viruses to gather information on Western countries. In the following decades, the use of cyber espionage grew as technology advanced and the internet became more widespread.

Cyber threats, cyber warfare, and digital attacks are terms associated with an aura of mysticism and secrecy. The phenomena are a result of the information revolution, which in turn can be experienced as complex, difficult to interpret, and multi-dimensional. Cyber refers to technology, especially computer systems, and networks as well as the internet and virtual reality. It can also refer to the culture and community that surrounds these technologies. It is also a field surrounded by a high level of secrecy since it involves different kinds of illicit influences on information systems (Heickero, 2013). Operating in cyberspace and keeping it secure have become increasingly important in recent years. Our nation's security can be jeopardized by the cyber domain as long as computer networks serve as the cornerstone of our military and economic capabilities (McKenzie, 2017).

The stakes and belligerence of the cyberspace conflict will rise. Around 2.7 billion people, or 40% of the world's population, are connected to the Internet and an estimated 75% of people have access to mobile phones. Our political, economic, and social life are influenced by networks of information and communication (Nocetti, 2016). Although information technology (IT) has contributed to several positive innovations around the globe, it also poses severe security risks to people, nations, and society (*Nadeem et,al,2021*). Cyber espionage is a key component of cyber warfare, which is the use of digital technology to attack and disrupt the information systems of other countries or organizations. It is considered one of the most dangerous forms of cyber-attack as it can lead to long-term damage and can provide an attacker with access to sensitive information that can be used in the future. International law is silent on the issue even though states have acknowledged the existence of espionage and passed domestic legislation to prohibit it. However, States recognize and generally tolerate espionage as a vital element of international affairs (Brown, 2016).

There have been several reports of cyber espionage operations targeting Pakistan in the past. Pakistan has been a target of cyber espionage due to its strategic location, as well as its nuclear weapons program and ongoing conflicts with neighboring countries. In the past, Pakistan has been targeted by various state-sponsored hacking groups, including APT6 (Advanced Persistent Threat 6) from China and the Lazarus Group from North Korea. It is also likely that other countries have also conducted cyber espionage operations against Pakistan, but these have not been publicly disclosed. The UN Conference on Trade and Development's Information Economy Report due to its growing digital economy placed Pakistan ninth in the world (United Nations Conference on Trade and Development, 2021). Cybersecurity professionals predict that by 2025, global cybercrime would cost $10.5 trillion yearly (*Establishing Deterrence in Cyberspace*, 2022). While the internet offers new opportunities to nations around the world, it also presents a wide range of issues in cyberspace.

The banking and energy infrastructures in Pakistan have been the target of some significant cyberattacks. K-Electric, the Federal Board of Revenue, and the National Bank of Pakistan are a few of these. Furthermore, the intercept from 2016 showed that the US National Security Agency (NSA) has consistently targeted Pakistan's senior civilian and security officials for cyberespionage. Moreover, ISPR announced in 2020 that cyberattacks targeting Pakistani military personnel and government officials were carried out by Indian intelligence agencies (*Establishing Deterrence in Cyberspace*, 2022).

Literature Review

Richard A. Clarke and Robert K. Knake argue in their book Fifth Domain that in the cyber domain to create stability you have to dominate the domain. You have to engage with your rival more vigorously to create stability. With the advent of Nuclear weapons, the great powers have gone, and states normally avoid confronting each other. (Mathews, 2019) They try to go for peaceful means. However, with the advent of the cyber domain rivals engage with each other more vigorously than peace-full means. Moreover, the great power war has come back in the cyber domain. If states fail to handle cyber weapons properly it causes conflict that we have been avoiding for decades. (Eugenie, 2015). Moreover, cyber warfare and cyber domain are unique to normal warfare because in cyber those states that cannot defeat you in conventional war pose a significant asymmetrical threat. For example Iran and the US, Iran was to penetrate the US Navy classified documents remain there even after detection.

Daniele Hadi Irandoost in his article Cyber security: A National Security Issue argues that no matter how many precautionary measures the state takes for the prevention of cyber-attack there always remain flaws that give rise to the vulnerabilities that pave the way for the attack. (Irandoost, 2018). An additional salient concern pertains to the susceptibility of states to cyberattacks, which can originate either within or beyond their borders. An illustrative instance of such a threat materialized when a hacker group operating from Lahore compromised the Automated Teller Machines (ATMs) of Habib Bank Limited (HBL), resulting in the illicit withdrawal of a substantial sum of millions of rupees. Furthermore, the issue is compounded by the elusive nature of cyber attackers, who often employ tactics to obfuscate their origins and evade straightforward tracking efforts. Furthermore, the regulatory frameworks governing cyber activities, both on an international and domestic level, are characterized by a state of ongoing development or, in some instances, exhibit inadequate drafting. This deficiency is marked by an inherent lack of comprehension, wherein certain cyber actions fail to be classified as criminal offenses or are inadequately addressed within the existing legal frameworks.

Arquilla, J. & Ronfeldt, D., in their article Cyber War is Coming Comparative Strategy, argues that the advancement of technology, state dependency on the internet, and rapid increase in internet users has made cyber war inevitable.(Arquilla & Ronfeldt, 1993) Whenever it takes place, it brings the whole nation to its knees. Widespread disorder is likely to ensue, akin to scenarios characterized as a "cyber Pearl Harbor" or "Cyber 9/11," (The Russian 'Cyber Pearl Harbor' That Wasn't | Cato Institute, 2020). A pertinent illustration of such a crisis materialized in the form of a recent cyber offensive attributed to China, targeting the power grid infrastructure in the Indian state of Maharashtra. This event precipitated a state of upheaval, encompassing the immobilization of railway services and the disruption of essential sectors, including healthcare, education, and industrial operations, among others, as documented in reports pertaining to the (Kiran Tara, 2021).

Material and Methods

The research methodology employed is qualitative in nature. The systematic literature review entails a meticulous examination of data sources, encompassing journal articles and various websites. These sources are consulted to elucidate the underlying empirical realities and furnish analytical insights. Additionally, the research methodology incorporates the utilization of the Process Tracing method, which places emphasis on the systematic scrutiny of diagnostic evidence. This evidence is subjected to comprehensive analysis in alignment with the research question and hypothesis. This method serves as a crucial tool for qualitative analysis, facilitating the systematic delineation of descriptive inferences derived from extant data. The principal objective herein is to conduct a diagnostic assessment of the evidence available in the literature review or existing dataset.

Cyber Espionage and National Security

Cybersecurity, also known as information technology security, is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from attack, damage, or unauthorized access. It encompasses a wide range of technologies, processes, and practices designed to secure information and information systems from cyber threats such as hacking, malware, and ransomware (*Rimsha, Pakistan Today, 2023*).

The goal of cybersecurity is to ensure the confidentiality, integrity, and availability of information and information systems by preventing unauthorized access, use, disclosure, disruption, modification, or destruction. This requires a multi-layered approach that includes technical measures, such as firewalls, encryption, and intrusion detection systems, as well as non-technical measures, such as employee training, incident response planning, and risk management (Shackelford, 2016).

Cybersecurity is an increasingly important issue as more information that is more sensitive is stored and transmitted electronically, and as the number and sophistication of cyber, threats continue to grow. Organizations of all sizes, from small businesses to large corporations, government agencies, and critical infrastructure providers, must take cybersecurity seriously to protect their assets and maintain the trust of their customers and stakeholders (Onugha, 2018).

Cybersecurity is often considered national security. This is because the reliance on technology and the increasing interconnectedness of systems and networks have created new and more complex security threats that can have far-reaching consequences. Cyberattacks can compromise sensitive information, disrupt critical infrastructure, and harm the economy. In some cases, they can even have a direct impact on national security, such as when classified information is stolen or military systems are disrupted (Johnson, 2021).

As a result, many governments around the world have recognized the importance of cybersecurity and have taken steps to improve their defenses. This has included investing in technical measures, such as firewalls and intrusion detection systems, as well as non-technical measures, such as employee training, incident response planning, and risk management. In addition, many countries have also established cyber security agencies and developed strategies to coordinate their efforts to address the growing threat of cyberattacks. By taking a comprehensive approach to cybersecurity, governments aim to protect their citizens, organizations, and critical infrastructure from the impacts of cyberattacks (Schroeder, 2022).

Cyber espionage is a form of cyberattack that is focused on stealing sensitive information or intellectual property for the benefit of a nation or group. This type of activity is considered a major threat to national security because it can compromise sensitive information, undermine economic competitiveness, and put critical infrastructure at risk. Nation-states and other groups engage in cyber espionage for a variety of reasons, including to gain a strategic advantage in political or economic negotiations, to support military operations, or to gather intelligence on their adversaries. The targets of cyber espionage can include government agencies, corporations, and critical infrastructure providers, among others (de Silva, 2015).

To protect against cyber espionage and other cyber threats, many governments have implemented a variety of technical and non-technical measures, including firewalls, intrusion detection and prevention systems, encryption, and employee training. They also work with the private sector to share threat intelligence and coordinate their efforts to respond to cyberattacks. In addition, many governments have established cyber security agencies and developed strategies to address the growing threat of cyberattacks, including cyber espionage. By working together, governments and the private sector aim to improve their collective cybersecurity posture and mitigate the risks posed by cyber espionage and other cyber threats (Jilani, *The Hill,* 2023.).

Cyber Espionage and Economic Security

Economic espionage refers to the theft of trade secrets or other confidential business information for commercial advantage by a competitor, foreign government, or other organization. This type of espionage is often illegal and can result in significant financial harm to the victim company. Economic espionage can have a significant impact on businesses, governments, and entire economies. It can lead to the loss of proprietary information, loss of competitive advantage, and financial losses for the victim. In some cases, it can even harm national security and undermine the global economy. The power of economic espionage lies in its ability to provide unauthorized access to valuable information and technology, enabling the attacker to gain an unfair advantage over others. This can disrupt fair market competition, harm innovation, and lead to a decrease in trust in the business community.

Economic espionage is a major concern for the United States and has been a target of various countermeasures and legal actions. The US has criminalized economic espionage under the Economic Espionage Act of 1996, which makes it illegal to steal or misappropriate trade secrets for commercial advantage or the benefit of a foreign government. The US has also created agencies such as the Federal Bureau of Investigation (FBI) to investigate and prosecute economic espionage cases. Additionally, the US has implemented various export control measures to prevent the unauthorized transfer of sensitive technology and information to foreign countries. The US also regularly engages in diplomatic efforts with other nations to address economic espionage and to strengthen international cooperation on this issue. Despite these efforts, economic espionage continues to be a significant problem for the US, as foreign governments and companies seek to gain access to valuable US technology and intellectual property.

However, it is more difficult than it seems to remotely collect trade secrets and then use them for your gain by secretly infiltrating a rival's computer networks. This is demonstrated when one attempts to compile a list of the most notable instances of cyber espionage that resulted in considerable economic harm that could be measured; the list is shorter and more contentious than what the media portrays (Rid, 2012). A British case involving a UK-listed company that reportedly lost an £800 million agreement as a result of cyber espionage was made public by MI5's Jonathan Evans in the middle of 2012, albeit the specifics are still unknown (Weissbrodt, 2013). Titan Rain is a more noteworthy illustration. Titan Rain is the US government's codename for a string of attacks that started in 2003 and persisted for years against the government and military computer system. The National Nuclear Security Administration's employees' personal information was taken from more than 1,500 of them, as disclosed publicly by the American Energy Department in June 2006. Although the network of the nuclear security organization was breached in 2004, NNSA didn't become aware of the incident until one year later (Rid,2012). According to the Pentagon's number two, a flash drive with purportedly Russian spyware was installed into a laptop at a base in the Middle East and "placed there by a foreign intelligence agency" (*Rimsha*, 2023).

The term economic intelligence refers to a key idea in the study of economic espionage. The CSIS defines economic intelligence as policy or commercially relevant economic information, which includes technical data, financial, proprietary commercial, and government information, the acquisition of which by foreign interests either could, directly or indirectly, assist the relative productivity or competitive position of the economy of the collecting organization's country. People who engage in economic espionage deliberately seek out this type of data (Lewis, 2011).

The Ministry of Foreign Commerce and Industry in Japan identifies foreign high-tech businesses that are likely to release key innovations soon. The ministry provides vital information to Japanese businesses, encouraging them to acquire overseas enterprises using front companies, false flag operations, or overt methods(Hedieh,2005). More than 1,500-year-old instance of commercial espionage involves the knowledge of silk. A Chinese princess visited foreign countries while wearing a floral cap. She brought the silkworms to an Indian man while concealing them in the flowers. As a result, China's silk-making secret escaped through economic espionage (*Jemahl, Stealing the Secret of Silk, 2021*).

According to the FBI's 2001 Business and people conduct Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 58% of industrial espionage, while just 22% is ascribed to activities supported by foreign governments (Abiodun, 2021).

In the case of Pakistan, the potential for economic espionage from foreign intelligence agencies represents a significant threat to the country's national security; as such, the theft of sensitive information and technology could have a significant impact on the development of key industries such as defense, energy, and telecommunications. It is therefore important for Pakistan to take proactive steps to improve its information security and implement measures to protect sensitive information from theft by foreign intelligence agencies. Additionally, the government must work to improve its domestic intelligence capabilities to detect and prevent economic espionage and collaborate with international partners to counter transnational threats to its national security. Overall, cyber espionage represents a major challenge to national security and requires a comprehensive, coordinated response from governments and the private sector to protect sensitive information and critical infrastructure (*Cyber Espionage A Big Threat*, 2023).

Cyber Espionage and Military Security

Cyber espionage refers to the collection of data through the internet by using illegal means i.e. malicious pieces of code, viruses, and spearfishing. The fundamental objective of cyber espionage is to collect sensitive data and control the opponent's system without their knowledge and consent.

The technological advancement and invention of the internet, the rise of artificial intelligence, and wireless communication pave the new ways of cyber espionage. These were used to collect sensitive data, and have access to your messages, photos, emails, and voice calls. Moreover, they also closely monitored the data traffic of individuals and organizations. The data flow of an organization tells us a lot about its activities for example if an organization like the embassy suddenly increases its flow, it means that something is going on. In contemporary times, cyber espionage remains an important part of cyber warfare and national defense. States continuously monitor opponent systems (Rivera et al., 2022).

With the invention of the internet, cyber espionage has replaced traditional intelligence methods. States are continuously engaging in cyber espionage. According to US declassified files in 2008 sensitive data of the United States government worth $150 billion were stolen. According to a Cyber threat report to the United States Congress in 2008. There are 140 countries involved in cyber espionage against the United States and trying to penetrate United States companies and government agencies (O'Hara, 2010). John Tkarik an expert on counter-cyber espionage stated that the Chinese and Russia were actively involved in cyber espionage against the United States. According to a report by ASIO "Australian National Security Services" and the defense signal directorate China was involved in several cyber espionage against the Australian government (Aquila, 2013.). According to a report by the Wall Street Journal, the United States project named "Joint Strike Fight" has been hacked and the data were stolen. According to a report by German intelligence, the Ministry of Foreign Affairs has been hacked and about 160 GB stolen using malicious software and spearfishing. German magazine "Dev Spiegel" reported that around 60% of cyber-attacks and cyber espionage activities were from China and North Korea on a daily basis (Staff, 2013). According to the United States, ex-defense secretary Robert Gates NIPRNET of the Pentagon has been hacked and un-classified data has been stolen. Moreover, the United States Defense Department and private defense contractors were attacked daily more than three million times (Eugenie, 2015). The United States is also part of the global information grid, which scans more than three million times a day.

The United States was also actively involved in cyber espionage against their enemy and allies. According to the European Union report on US cyber espionage activities "American Signal Intelligence" was involved in global cyber espionage operations and operated under NSA "National Security Agency" has different espionage stations around the world (Poitras et al., 2013). Moreover, this report also argued that European data has been continuously monitored, analyzed, and stored by the NSA. NSA cyber espionage facility at Utah Data Center which becomes functional in 2013 is used to collect, analyzed, and decipher information and global communication network including states and individuals (Staff, 2014). One of the primary examples of CIA involvement in espionage activities was traced back to 1991 when negotiation between the Kingdom of Saudi Arabia airline and a European space company for the purchase of an Airbus. CIA hacked into their system and monitored the data follow including fax, telegraph calls, and emails, and foraged the data and turn the deal into US-based Company Boing Co worth $ 6 billion. In 1996 CIA hacked into Japan's Ministry of Trade and steal information that benefitted the United States companies while negotiating (Ray, 1998).

Another important actor in this espionage great game is Russia. Russian parliament passed a law 40*ffz* in 1991 according to which the Russian intelligence agency KGB was given legal cover to conduct espionage operations including tapping phone calls, and computer systems, monitoring the system, and continue serving internet traffic at domestic and international levels (Reuters, 2022). According to the Russian official and member of the Duma, KGB was given this legal cover to conduct cyber operations in and outside of Russia for safeguarding their nation and interest. Russia uses the SORM-II system for this purpose which refers that all of the data and communication network being monitored and information transferred to a platform known as "Rostelekom", "Elecktrotelekom" will be passed to the Russian intelligence (*This KGB Chief Rang the Alarm About Russia-U.S. Cyberwars. No One Listened.*, 2018). KGB signal intelligence operates all over the world having monitoring stations in Yemen, Socotra, the Gulf of Aden, and the Somalian coast. According to a report by Russian Magazine "Khakar" KGB hires hacker which performs national and international espionage. According to an interview in "Pravda," the head of GRU General Feodor lady gin argued that they had the capacity and capability to hack any computer system in the world *(Gov.UK, UK Exposes Russian Spy Agency behind Cyber Incidents,* 2022). One common example of this is the "Cuckoos eggs".

The third PLA charged Chinese signal intelligence involved in cyber espionage activities, which collect, analyzed, and decipher the information. According to a report Chinese cyber espionage include both friends and foes i.e. Laos, Burma, Thailand, Cuba, and other states of the nearby island. The Chinese Ministry of Information and Technology is responsible for controlling the flow of data and checking on citizens it had web police like the Iran moral police strength of 20,000 personnel. Chinese web police continuously monitor the flow of data, what type of data citizens are consuming, and surveying the internet (Lindsay et al., 2015). The technological advancement and digitization of sensitive data make cyber espionage easy and critical infrastructure vulnerable to attack.

Cyber Espionage and Nuclear Weapon Security.

With the advancement of technology, the cyber-nuclear nexus has also emerged. The Estonian critical infrastructure attack showed the importance of cyber-space for military purposes. The Stuxnet cyber-attack on the Iranian nuclear facility was the first of its nature, which physically destroyed it. The United States and the United Kingdom often involves in offensive cyber-attacks against Iran, Iraq, North Korea, and Pakistan. However. Over the period, cyber has become very important for strategic and military purposes (*This KGB Chief Rang the Alarm About Russia-U.S. Cyberwars. No One Listened.*, 2018).

Computer systems long have been used for early warning detection and missile defense system. In the 1950s United build a number of the computer system used for early warning detection, communication, and processing of information, for example, the US used a semi-automatic ground environment air defense system controlled by the computer (Futter, 2019). Russia also modernizes the command, and control system of its strategic force and digitalizes its ballistic missile system. The rise of artificial intelligence and the use of computers for missile defense systems pave the way for the cyber-nuclear nexus (Futter, 2019). This nexus creates an inherent risk to nuclear weapon security and have serious implication for deterrence. Computer systems or artificial intelligence controlling the nuclear system may malfunction due to programming errors, use of obsolete hardware, design error, or human error even on the most reliable computer system. Nuclear weapons security always remains a security concern for international security while linking it with cyber-space and IT technology creates a new Pandora's-Box and a complex security scenario (Kier et al., 2022).

During the cold war, the United States and Russia often received narrow escapes related to nuclear attacks mostly because of computer system malfunction. According to the declassified document of the United States national security the computer installed to detect early warning systems, often misinterpret the situation, for example, natural phenomena like tornadoes are sometimes considered missiles (Barrett, 2016). However, human error also caused several incidents. During the cold war, the United States and Russia experienced computer-nuclear and missile technology but they often generate false reports, misinterpret the situation, and malfunctioned. According to historians computer systems installed for early warning detection failed on several occasions which led to the state being on the brink of war (Campbell, 1985).

The United States developed electronic warfare capabilities during the cold war and try to conduct an assault on the Russian computer system and Warsaw command and control system. According to the Russian naval war report, Russia had also developed the countermeasure for the US electronic warfare and analyzed its impact on nuclear weapons capabilities. The introduction of advanced automated computer systems further led to creating higher chances of miscalculation and accidental fire (Kier et al., 2022). One such automated system has been introduced by introduced under "Perimeter" which can lunch the rocket and missiles without human intervention. Rapid technological advancement and modernization of nuclear weapons not only increase the state's dependency on the internet and AI but also creates a security threat (Matheson, 2020). With this modernization of defense, Russia and the USA retired the obsolete computer and focused on state-of-the-art technology for their nuclear command and control system (Rivera et al., 2022).

The cyber-nuclear nexus that will be fully controlled by a dead hand (computer code and engineer) will be complex to govern and understand. With the invention of the internet, cyber space has become very important for military purposes. In contemporary times cyber had becomes the hotbed for covert military operations and espionage. Most of the nuclear and non-nuclear weapons states have their cyber force and policy framework (Cimbala, 2016).

According to the Chinese military strategy of 2015 and 2019 white paper cyber space has been given special importance. Controlling cyberspace is vital to preserving international security and the protection of Chinese national interest by developing cyber command, creating awareness among the masses and maintaining a credible minimum cyber deterrence. Focusing more on developing cyber capabilities for defense purposes (Lindsay et al., 2015). The French government passed law No.2018-607 which emphasizes establishing a cyber-command, the strategic importance of cyberspace, and cyber deterrence (Vitel & Bliddal, 2015). The Russian cyber-security doctrine of 2014 focuses on detection, prevention, elimination, and counterattack. Moreover, it also emphasizes cyber-deterrence and its linkages with information security while maintaining cyber police ("Russian Data Localization Laws," 2018). The United Kingdom cyber doctrine "Joint doctrine note 1/18" emphasizes that war is equally applied in cyber as in the operational domain (Onugha, 2018). Moreover, according to Britain's cyber security strategy 2016-2021, cyber deterrence is also possible just like physical and nuclear. Moreover, it focuses on offensive cyber operations and provides expertise to NATO (Onugha, 2018).

The United States had already established cyber command and continuously engage in cyber war, cyber espionage, and information warfare at a larger scale against Russia and China. North Korea had also emerged as a key factor in cyber espionage and cyber-warfare with several cyber-attacks on US and UK networks including hacking of Sony entrainment and malicious software "WannaCry" virus. Indian military doctrine of 2004 sub-section-10 emphasizes the changing warfare. Ex. national security advisor argued that India had already considered cyber-warfare an option for the future. In 2007 joint doctrine of armed forces considered cyber-space as an operational doctrine domain in which future wars will be fought (Gellman & Nakashima, 2013).

Pakistan develop its comprehensive cyber security policy in 2021, which focuses on cyber defense. It also considered cyber-attacks as an act of aggression and threat to the sovereignty and Pakistan will respond according to the nature of the threa. Moreover, Pakistan has securitized the cyber threat and dealt with traditional security concepts.

Cyber espionage had a significant impact on nuclear deterrence. Cyber espionage provides valuable information to potential adversaries about the capabilities and vulnerabilities of a country's nuclear forces. This information can be used to develop strategies for nuclear deterrence or to launch a cyberattack that could undermine a country's nuclear capabilities. The use of cyber espionage can also create mistrust and suspicion between nations, which can undermine the principles of nuclear deterrence. If countries suspect that they are being spied on, they may be more likely to take aggressive actions to protect their interests (Rivera et al., 2022).

Cyber espionage can also create uncertainty about the origins of a cyberattack. If a country cannot determine who is responsible for a cyberattack, it may be difficult to determine an appropriate response. This uncertainty can undermine the effectiveness of nuclear deterrence.

The growing threat of cyber espionage has led many countries to invest heavily in cybersecurity, including the development of offensive and defensive cyber capabilities. This could potentially lead to a new arms race in cyberspace, further complicating efforts to maintain stable nuclear deterrence. Overall, the impact of cyber espionage on the concept of cyber nuclear deterrence is complex and multifaceted (Eugenie, 2015). While cyber espionage can provide valuable information to potential adversaries and create uncertainty about the origins of cyberattacks, it can also create mistrust and suspicion between nations and lead to an arms race in cyberspace. As such, it is important for policymakers to carefully consider the implications of cyber espionage for nuclear deterrence and work to develop strategies for mitigating its impact.

Cyber espionage and its national security implications

Cyber espionage refers to digital surveillance and infiltrating computer systems to steal sensitive information. State and non-state actors such as hackers and cybercriminals do this. Targets include government, military, industry, research institutes, industry, and more. Agent.BTZ is a 2008 computer surveillance program that infiltrated the United States using infected USB devices. Military networks have been expanded to include classified and unclassified equipment.

It allows adversaries to steal confidential security intelligence information. This can compromise job security and put workers at risk. Stealing confidential government communications, policy settings, or communication channels. For example, Operation Shady RAT is a large cyber espionage operation that purportedly targeted more than 70 organizations worldwide, including the United States, as well as government agencies, security professionals, and human rights groups, in 2011.

It can damage international relations. Economic and technological espionage for intellectual property theft can affect economic competition. Monitoring critical infrastructure such as power grids makes them vulnerable to cyberattacks that can self-destruct in conflict. Red October - 2013 marks the beginning of a global cyber espionage operation that has been targeting diplomatic, governmental, and intelligence organizations in Eastern Europe and Central Asia for the past five years

The tracking of personal data and communications by intelligence agencies is considered a violation of citizens’ privacy rights. Massive adversarial cyber espionage campaigns undermine confidence in digital communication tools. Careto/Mask - A sophisticated malware campaign that has been active since 2007, targeting government institutions, embassies, and employees in 31 countries, as disclosed by Kaspersky Lab in 2014.

This can hinder economic growth. Stealing a weapon's technical information allows adversaries to simulate advanced security capabilities. Regin malware - Advanced malware that was used between 2008 and 2011 to target targets such as EU Cryptophone customers and the Belgian telecom business Belgacom before being discovered in 2014.

Reports indicate that countries such as India and the US. Targeting Pakistani military and nuclear sites for cyber espionage. This can compromise sensitive security issues. Economic espionage against Pakistan's burgeoning IT industry could slow growth and competitiveness in key technologies of the 21st century. Visits to critical infrastructure such as dams and power plants make them vulnerable to cyberattacks that can self-destruct in conflict.

Conclusion

In conclusion, the rise of cyber espionage has left an indelible mark on Pakistan's national security landscape. Pakistan, like many others, faces an escalating tide of cyber espionage threats emanating from both state-sponsored entities and non-state actors. These digital assaults have triggered a series of complex and multifaceted consequences, profoundly affecting various facets of Pakistan's security paradigm. Foremost among these repercussions is the profound vulnerability of critical infrastructure, including energy and communication networks. Cyberattacks targeting these essential systems pose an existential threat to Pakistan's economic stability and its ability to function as a sovereign nation-state. The potential for espionage and data theft further compounds these security challenges, placing the nation's military and national security apparatus at risk.

In response to these evolving threats, Pakistan has undertaken commendable measures, establishing dedicated cybersecurity agencies and enhancing infrastructure security. The nation's commitment to fostering indigenous cybersecurity solutions and building a capable cybersecurity workforce reflects its dedication to countering cyber threats effectively. In light of these ongoing challenges, it is imperative for Pakistan to maintain a vigilant stance and continue its investment in cybersecurity capabilities. This proactive approach is essential not only to protect critical infrastructure but also to defend against the ever-evolving landscape of cyber warfare threats. Pakistan's ability to adapt and respond to these challenges will play a pivotal role in ensuring the security and resilience of the nation in an increasingly interconnected and digitally driven world.

Recommendations

Countering cyber espionage can be a complex task, but there are several best practices that organizations can follow to reduce the risk of successful attacks. Here are some strategies that can help:

1. *Implement strong security measures*: States and Organizations should implement strong security measures such as firewalls, intrusion detection and prevention systems, and encryption to protect sensitive data.

2. *Practice good security hygiene*: Employees should be trained on best practices for password management and avoiding phishing attacks. States and organizations should also regularly update software and operating systems to address known vulnerabilities.

3. *Conduct regular security assessments*: Regular security assessments can help organizations and states identify and remediate vulnerabilities before attackers exploit them.

4. *Limit access to sensitive data*: Access to sensitive data should be limited to only those who need it, and privileged accounts should be monitored for unusual activity.

5. *Implement an incident response plan*: States and organizations should have a plan in place for responding to security incidents, including procedures for preserving evidence and reporting to law enforcement.

6. *Foster a culture of security*: States and organizations should foster a culture of security by making security awareness and training a priority, and by regularly communicating the importance of security to employees.

7. *Work with law enforcement*: When incidents do occur, states and organizations should work with law enforcement agencies to identify the attackers and hold them accountable.

By following these best practices, organizations can reduce their risk of being the target of cyber espionage and improve their ability to detect and respond to attacks when they do occur.

Reference

4G is vulnerable to same types of attacks as 3G, researchers say. (2018, July 2). CyberScoop.

admin. (2019, November 6). China-Pakistan Cyber Security Cooperation. *Pakistan Observer.*

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

Aquila, G. (2013). *The Stuxnet Worm The Nexus of Cyber Security and International Policy.*

Ayers, R. (29 March, 2022). *Big Data and AI - A Quick Overview.* In Data Labs.

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

Cyber threat landscape—Establishing a resilient ecosystem. (2021, December 8). *The Nation*.

Calif, Morgen. (13 May 2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*.

Harmen. (2015, March 12). How the CIA can get from spy to cyberspy*, Wilson Center*.

Heickero, R. (2013*). The Dark Sides of the Internet: On Cyber Threats and Information Warfare.* Peter Lang.

Hachigian, N. (2001). *China's cyber-strategy.* Foreign Affairs

Haque, Rehman. (28 July 2015). Hacking Team hacked: The Pakistan connection, and India's expansion plan. *The Dawn*

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.*

King, Griffith, Mileweski. (9 June, 2021). *Cyber Espionage: National Security in the Digital Age,* Wilson Center

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.

Lonsdale, D. J. (2016). *Britain's Emerging Cyber-Strategy. The RUSI Journal,* 161(4), 52–62.

Malik, R. (2023, April 30). Cyber Espionage A Big Threat. *Pakistan Today.*

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*

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

McKenzie, T. M. (2017). *Is cyber deterrence possible?* Alabama: Air University Press, Air Force Research Institute.

Maann, E. (2021, Sep 27). Scientists create their own GPS by spying on internet satellites | Science*, AAAS.*

Nocetti, J. (2016). The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age. By Adam Segal: Internet wars: the struggle for power in the 21st century. By Fergus Hanson, *International Affairs, 92*(5), 1263–1266,

Neil, P. (2022, Feb 28). How China built a one-of-a-kind cyber-espionage behemoth to last. *MIT Technology Review.*

News Agencies. (2010, Dec 4). India and Pakistan in cyber war | Science and Technology News*, Al Jazeera*

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*

Rajasekar,V, Dhanaraj, R. (2022). *Cyber Security Strategy—An overview,* ScienceDirect Topics.

Rawat, R., Mahor, V., Chirgaiya, S., & Garg, B. (2021). *Artificial cyber espionage based protection of technological enabled automated cities infrastructure by dark web cyber offender.* 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). *Governing 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.

Rid, T. (2012*). Cyber war will not take place. Journal of strategic studies, 35*(1), 5-32.

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

Segal, A. (2017). Chinese cyber diplomacy in a new era of uncertainty. Hoover Institution, *Aegis Paper Series*, 1703, 1–23.

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.*

Shoebridge, M. (2018). *Chinese cyber espionage and the national security risks Huawei poses to 5G networks.* Macdonald-Laurier Institute for Public Policy.

Staff, S. (2013, February 25*). Digital Spying Burdens German Relations with Beijing.* Der Spiegel.

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), 15–20.

Times, G. (2022). *Exclusive: How CIA uses cyber weapon 'Beehive' to monitor, attack global key targets - Global Times*

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 defence: An overview. Information & Security*, 32(1), 1.

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

Yang, J. (27 Feb, 2023). *The Government cannot be win at Cyber Warfare without Private Sector. The Hill.*