Original Article (JSPGA) Publishing Date: 30th December 2020

Journal of Strategic Policy and Global Affairs

Vol: 01, Issue: 01(2020) DOI:https://doi.org/10.58669/jspga.v01.i01.03

State-Level Response and Cyber Security: A Comparative Study of Pakistan and India

Dr. Sadia Fayaz

Assistant Professor, Department of political science, Shaheed Benazir Bhutto University.

Email: dr.sadiafayaz@sbbwu.edu.pk

Abstract: Pakistan and India's ties have yet to be amicable since their inception. Many long-standing, unsolved disputes, including those over Kashmir, Siachen, the border, Sir Creeks, and many more, are to blame for the harsh bilateral ties. Following Pakistan and India's overt nuclear development, the risk concept has now been complicated to include both lethal and non-lethal threats. A new sort of threat has emerged as a result of increased interconnectivity and urbanization. In addition to more conventional methods, data and the internet are now powerful impact features. Nevertheless, until recently, Pakistan's and India's national security decision-makers focused on kinetic risks. Still, non-kinetic difficulties are now starting to make an impact that is gradually coming to light. The main focus of this paper is the State-Level Response and Cyber Security by analysis of India and Pakistan. The first section will briefly describe the perspective of cyber security. In the next section, the paper will explore the historical background of cyber security events in India and Pakistan. The third section will highlight the comparative analysis of the cyber security of Pakistan and India. Recommendations will be given at the end of the paper.

Keywords: Kashmir, Bilateral Ties, Nuclear Development, Urbanization, Cyber Security, State-Level Response

Introduction

As the 21st century progressed, the cyber era established strong foundations in society and invaded peoples' everyday routines to the point where the web acts as an essential component of daily life, elevating its users to the level of "online users." Additionally, innovation in cyberspace has become more dynamic, growing the number of surfers. This was achieved in the cyber world not because all people were tech-savvy but partly because this equipment was made more approachable. However, because there were so few limitations and regulatory challenges imposed by the authority of the nations in the cyber realm, the full extent of the "free to speech" was easily accessible there. With age, the quantity of data in cyberspace and the volume of traffic started to increase. Teenagers searching for data for academic tasks to business owners eager for profits were only a few of the people who accessed the internet. Terrorists and non-state entities used it for hidden discussions and e-governance activities for the general people. This ungoverned cyber area eventually developed into a billion-dollar data mining company, creating a conflict where users could gather this massive knowledge and damage it to help them achieve their goals (Dilaprij, 2013). The crucial aspect of this conflict was that it did not need a military to win. Anyone who could write just a few lines of programming and had a basic understanding of cyber warfare could launch an attack against a nation. According to the offenders' motivations and the outcomes, this type of conflict between internet users in cyberspace is alluded to by several names, including cybercrime, cyberattacks, and cyber warfare. Because of its low tier of limitations and regulatory hurdles, confidentiality, lack of fatalities, and perhaps most notably, its employability of limited support and requirement for insubstantial numbers of unskilled individuals, this also happened to come to be the primary way of the citizenry's resistance against their political adversaries, which could range from an entity to authorities.

Historical Background

Cybercrime Events - India and Pakistan

Date	Incidents
1947	India and Pakistan emerged as sovereign nations, but the northern border regions of Kashmir and Jammu remain unclear.
1947	The Pakistani authorities back a Muslim protest in Kashmir. The 1947-1948 conflict begins. (Baezner, 2018)

1949	India and Pakistan signed an agreement to end the 1947-1948 battle and reach an agreement on establishing a Line of Control
1965	Conflicts among border police on the Line of Control kicked off the 1965 war, which lasted until January 1966.
1971	During the Indo-Pakistani conflict of 1971, East Pakistan declared independence and renamed Bangladesh.
1972	Pakistan commences its nuclear program.
1988	India's first nuclear equipment is launched.
1989	India and Pakistan agreed not to target their nuclear plants.
1996	Pakistan successfully launched a rocket.
1998	India and Pakistan are constantly pursuing a political way to normalize regional complications.
1999	India conducted a nuclear test in the western state of Rajasthan, while Pakistan replied by conducting the first-ever nuclear bomb testing in Baluchistan in Pakistan's southwest.
1999	Pakistani hackers compromised the website of India's Bhabha Atomic Research Center.
1999	Pakistani President Nawaz Sharif was deposed by a military led by General Musharraf.
2001	An military invasion of Kashmiri kills 38 people.
2001	Two Indian news sites are defaced by nationalistic Pakistani hackers.
2001	14 people are killed in a military invasion of the Indian Parliament.
2002	Pakistani President Musharraf vowed that his country would combat terrorism on its soil, but Kashmir is Pakistan's.
2004	The Composite Discussion Method, also known as the process of direct talks, begins between Indian and Pakistani officials.
2008	Indian authorities allege Pakistani Inter-Services Intelligence (ISI) of terrorism the Indian ambassador in Kabul
2008	Lashkar-e-Taiba7, a Pakistani militant organization, bombed many Mumbai targets, including the Taj Mahal Hotel.
2008	Indian cybercriminals deface several Pakistani sites in retribution for the terrorist attacks in Mumbai (Baezner, 2018).
2008	Pakistani cyber criminals deface Indian networks in reprisal for the attacks (RFSID, 2016; Ribeiro, 2008).
2009	The Pakistani government acknowledges that Pakistan played a role in the Mumbai terrorist attacks but denies ISI participation.
2010	Pakistani and Indian soldiers open fire throughout the Line of Control in Kashmir (Hashim, 2014).
2010	On the occasion of the Mumbai terrorist incident, Indian cybercriminals besmirch 35 Pakistani networks.
2010	In retribution for the November 2010 hackings, Pakistani cyberattacks stole and deleted data from the Indian Central Bureau of Investigation website (Leyden, 2010).
2011	Dozens of Pakistani webpages have been defaced by Indian hacker attacks (Kumar,

	2011a).
2011	Till February 2012, Indian and Pakistani cyber criminals participated in many tit-for-tat cyber acts (Joshi, 2012).
2012	In addition to the hacks mentioned earlier, Pakistani cyber criminals ripped down more than 400 Indian domains on Indian Republic Day (Mid Day, 2012).
2012	On Pakistan Republic Day, Indian hackers vandalize Pakistani networks (Garsein, 2012).
2013	A Norwegian telecoms company has revealed that it has been the subject of a hacktivist effort, presumably from India.
2013	On the centenary of the Mumbai invasion, Indian cyberattacks besmirch various Pakistani web pages. Pakistan Digital Army, a nationalistic group of hackers in Pakistan, responds by trashing the Indian Central Bank's website.
2014	On Indian Independence Day, Pakistani terrorists damage hundreds of Indian networks (Khan, 2014).
2014	On the one-year commemoration of the Mumbai terrorist attacks, Indian cybercriminals tear down many Pakistani government databases (Web Desk, 2014a).
2015	On the occasion of the Mumbai terrorist attacks, Indian cybercriminals hit over 200 Pakistani domains. Pakistani cyberattacks respond by hacking into the Indian Central Bank's website.
2016	Terrorists assaulted an Indian Air Force facility in the northern Indian city of Pathankot.
2016	Indian hackers desecrate Pakistani webpages in retaliation for the terrorist incident in Pathankot (RFSID, 2016).
2016	Pakistani officials apprehended an Indian citizen accused of spying.
2016	On Pakistan Independence Day, Indian hackers try to destroy over 50 Pakistani web pages.
2016	In an operation in Uri, Jammu, a Pakistani terrorist organization kills 19 people.
2016	India responded to the Uri tragedy with targeted strikes.
2016	Pakistani hackers have defaced hundreds of Indian internet sites in retaliation for the missile attacks, and Indian cyberattacks allege connection to critical Pakistani infrastructure networks.
2017	In Pakistan, the Indian detained in 2016 was sentenced to death.
2017	In Pakistan, the Indian detained in 2016 was sentenced to death.

Analogy and Analysis

Hacker Groups

India

In cyberspace, nationalistic Indian coders and hackers are primarily recognized as defending the Indian country's interests. Indian hacker groups and enthusiastic developers carried out the majority of site devastation on official Pakistani websites. These hackers also announced covert cyber attacks on Pakistani airports and internet sites. These criminals typically engaged in criminal activity on Pakistan Liberation Day and the anniversary of the horrific terrorist invasions in Mumbai. It's still unclear whether the hacktivists and passionate developers were people or organizations. Yet, they collaborated with other hackers and nationalist coders in this project. A few of these actively participated in a single fight of devastation before leaving the area. Such actions suggest that these hacker groups might just be satisfied kids, which is entirely possible. In that role, individuals might have become interested in these campaigns because of a desire for action or to test their expertise. Due to the

devastating invasions it has carried out, a well-known hacker organization by the designation of Mallu Cyber Arm collaborates with the state. It was founded in October 2014 by a team of Indian cyber security specialists to protect and reestablish Indian websites from cyber assaults by Pakistan (Mustafa, 2020).

Pakistan

In the beginning, Pakistani nationalist developers and hackers seem to use the web to target adversaries, particularly in the battle with India. Pakistani hackers frequently targeted Indian legislative databases using similar mutilated techniques to Indian hacker groups. Particularly after the incidents or overt, direct acts in Indian-occupied Kashmiri, Pakistani attackers made a concerted effort to combat Indian cyberattacks. Similar to Indian hackers, it is unclear if Pakistani hackers were working together or alone for personal gain and for this cause. Pakistan Cyber Army (PCA) first participated in the assault on the Indian Oil and Natural Gas Company in November 2008. Yet, it appears that the PCA sought to combat the earlier destruction of Pakistani sites following the Mumbai killings (Research, 2019). The PCA used simple methods to deface Indian sites. Risk Link, a cyber-security company, detected at least three PCA members in 2013. However, whether the group had ties to the Pakistani legislative entities or operated independently is still being determined (Mustafa, 2020).

Cyber Legislation

India

The Information Technology Act was originally proposed in the nation in 2000, and both cyber rules and the law were included when the Indian Legislature's House approved it. This law's main objective was to provide a legislative structure for e-commerce in the nation that would prevent cyberattacks and safeguard both buyers and sellers from them. Although this Act attempted to update antiquated legislation and provided a comprehensive framework for combating human cyber fraud, it always leaves out important aspects of the violence, such as confidentiality and information theft. In the Act of 2008, the change occurred in these regions. The law that governs criminality in India is the Information Technology (Amendment) Ordinance 2008. The goal of this law is to advance the e-commerce and IT sectors as well as to lessen cybercriminals. Moreover, it is stated that the ownership of the unique IP address will be made liable for any exploitation carried out through it (Tufail, 2018).

With time, that law has undergone numerous adjustments. The big shifts were that this Act made financial fraud, copyright offenses, cyber warfare, and deceiving crimes criminal. A maximum of three years in prison and criminal penalties are possible consequences. It demonstrates that other laws address cybercrime in addition to the IT Act. In the future, cyberattacks may be prosecuted under the India Penal Code (IPC). For illustration, the use of S.66 r/w S.43 IT Act to punish crimes like cracking, data theft, malware assaults, denial of services, illegal modification with code snippets, and cybercrime. IPC laws may punish incidents of faking a credit card or even copying a mobile SIM to cause loss, damage, or unjust profit. This Law was condemned as lacking sufficient protections to preserve people's civil rights and reduced a few of the cyber attack's punishments.The ability to detect, censor, and conduct spying on internet traffic has reportedly been granted by this Act, based on various publications.

In this manner, there are insufficient balances and controls to prohibit the abuse of knowledge. To combat acts of corruption and limit the spread of sexual information, the Indian Home Ministry announced in 2018 that they intend to establish the "Indian Cyber Crime Coordination Center" (I4C). This unit will collaborate with the authorities and keep an eye on online communities and other areas of cybercrime. Its major objective is to prohibit all sites that circulate ethically inappropriate material against the legislation. It will keep track of offenders, compile all the evidence discovered during the inquiry, and then give them to the criminal justice Agencies. Additionally, India has created a CERT, known as CERT-FIN, specifically for the financial industry. This CERT reviews cyber issues in commercial banks and notifies its national CERT of any cybercrime occurrence.

Pakistan

The Pakistani legislative authority passed the Electronic Transactions Ordinance 2002 (ETO) in 2002, which served as the country's initial constitutional system to fight cyberattacks. This ordinance's main goal was to make data, papers, interactions, online payments, and records easier to locate and recognize. This regulation offers security from any unauthorized use of digital transfers, such as bank withdrawals and web goods purchases. However, it only offers a few facts on how an unauthorized use scenario might be discovered.

Recognizing the legitimacy of these internet banking was helpful. Pakistan has officially joined the list of nations with constitutional recourse for any digital information thanks to this specific ETO 2002 regulation. The adoption of this regulation marks the beginning of the e-commerce sector and a crucial step in the nation's information technology growth. Several things could have been improved in the ordinance, such as the fact that it should have penalized the majority of the offenses relative to other commonwealth nations, even if it did establish some fines for several cybersecurity threats.

There was a requirement for a brief revision because of this. The Electronic Crime Act 2004 was developed in 2004 by the Ministry of Information Technology. It is centered on the ETO 2002 but has been improved. The concepts "cyber warfare," "illegal intrusion," "online theft," and "data or computer harm" were all contained in this statute. However, these criteria were included in this Legislation, they were pretty specific, and there was no discussion of creating a force to combat cybercriminals. This Law's primary goal was to give constitutional immunity to other anti-cybercrime initiatives. The administration modified the Electronic Crimes Ordinance in 2007. The law addressed the supervision of the digital economy. Still, the significant improvements were that it specified the sanctions for 17 different forms of cybercrimes, with sentences ranging from six months to execution. It also added a brand-new category called "Cyber Trolling," defined as illegal behavior intending to coerce, intimidate, or harass a target via a pc, core router, a website, system website, email, or another related method of interaction.

Stacking and cyber warfare were other sorts of crimes that have changed. The ISP had to keep traffic data for a minimum of 90 days under this regulation. The Federal Parliament approved the most recent cybersecurity legislation in Pakistan in 2016. The bill is known as the Prevention of Electronic Crimes Act (PECB). This measure has elements that enable monitoring, censure, and the immediate punishment of internet conduct. It did include some protections for the government and law enforcement organizational factors cyber malware inquiries. To address all pc-based crimes and receive data for these instances, Pakistan formed the National Response Centre for Cyber Crimes (NR3C) in 2007. With the help of this institute, the government has access to incredible tech skills in Testing Processes, Vulnerability Scanners, and Computer Security Assessments. The appropriate concerns of cybercrime occurrences are immediately received by it, and it also supports the other government-based authorities in their instances (Tufail, 2018).

Strategy For Cyber Security

India

Since 1998, Indian intelligence agents have focused on a cyber security plan, taking different actions and holding numerous discussions with security and IT specialists. In August 2010, the Indian government established a cyber plane in their military bases. It intended to shield any virtual threats from anywhere globally and protect valuable frameworks from federal and non-governmental performers inside and outside the regions. This hacker army can be utilized to eavesdrop on the aligned data of making threats to regions - Pakistan and China - by getting hacked into their system of computers. Since India is moving towards an online framework, it is crucial to have a facility that can be used in the event of a negative occurrence. In this regard, technological and security specialists are collaborating to develop a plan of action to deal with this danger. On July 29, 2010, a draft of a protocol was created.

According to the plan developed at the conference, India would hire IT specialists and coders who will be assigned to be in full assault mode or to launch preventative operations by tearing the safety barriers of the enemy's network system. On July 2, 2013, India unveiled its national cyber defense program, culminating four years of effort. The program statement clearly shows how important IT is to India. The program is built on a variety of components. Additionally, it focused on IT security and the issue with IT in Indian economic activity. Additionally, it provided instructions on safeguarding the infrastructure and improving India's image on the web. The security of the core network and addressing challenges, including support, are the main focuses of this program. It offers the fundamental guidelines to develop capacities for avoiding and responding to online threats.

It also contributes to reducing the impact of cyber threats through a mixture of political institutions, people, processes, tech, and collaboration. Developing a framework for gathering intelligence data about concerns to the foundation of technological tools (ICT) is suggested as the third step. This system is employed to take

preventative, remedial, and reactive actions. Fourth, various public and commercial organizations will hire five lac computer tech specialists throughout the upcoming period. Solid relationships and collaboration among public and private enterprises are required to combat cybercrime. Sixth, the Indian Army will develop a cyber control unit and strengthen the cyber security defense.

Pakistan

Edward Snowden, a contractor for the CIA, revealed how the United States uses it to watch various nations. As per sources, Pakistan is the second-largest priority of the United States. Edward Snowden alleged that the US national security agency (NSA) was snooping on Pakistan through the internet and other cellular technologies, intercepting 13.5 billion emails, phone calls, and faxes. In this respect, Senator Mushahid Hussain Syed, the head of the Senate Standing Committee on Defence, called a crucial meeting where a representative from the Pakistan Information Security Association (PISa), headed by Ammar Jaffri, managed to meet with Senator Syed at National assembly House to talk about cyber security policy (Malik, 2020).

The following was on the event's initiative: First, it was decided to work together for the nation's military, commerce, and cyber security of its people. Second, it was chosen to file a Personal Bill in the Senate and the National Assembly on August 14, 2013. Thirdly, the proposed bill will be developed after comprehensive discussion with the Pakistan Information Security Association and the national response of the computer crimes center. Fourth, a proposal of the cyber security reform agenda will be prepared by PISa. Fifth, the Senator advocated for the hiring of professionals with the necessary skills and knowledge, competence, and experience levels in multiple security organizations. Finally, in order to defend the cyber world in accordance with global norms, the Government must step forth and assume its proper role in accomplishing international best practices.

Additionally, In 2007, Pakistan established an updated cybercrime bureau named National Response for Computer Crime Center. It was the result of various things that happened in past decades. Such as, it's because more private and government entities are using the internet. Following that, the terrorists now communicate via the Web. India is also creating sophisticated cyber warfare. Furthermore, it also aids in obtaining information on IT security problems and monitoring general security matters. Lastly, handle and look into cybercrime to enforce current rules to combat computer-related offenses and protect buyers and Internet users (Malik, 2020).

Conclusion

No doubt that Information technology has come to be viewed by administrations as an arena for geopolitical warfare and a key ally for global defense (Parmar, 2018) thus, it is necessary to review state security, enhance offensive capabilities, and adjust to different patterns and cyberattacks previously unanticipated. A closer examination of terrorist attacks like the situation presents a unique dimension to terrorism and, thus, more conventional interstate confrontations, where cyber warfare can fuel or even start an armed confrontation. While there haven't been any significant, widespread cyber crimes involving India and Pakistan, the often-overlooked cyber components of combat could significantly alter how the two nations fight. Entities with minimal defense capabilities, such as terrorist organizations, can inflict significant harm owing to the relatively low prices of cyber impact activities. This is especially true if vital infrastructure and state technology are not adequately safeguarded and are the target of an enemy state. Because of the threat that cybersecurity issues represent, they still need to be clarified. Nevertheless, given that assaults frequently aim at crucial institutions and pose the threat of becoming quite palpable for people, safety advancements call for a greater emphasis on cyber advancements. An increased focus on responsibility allocation and fostering a deeper involvement with cybersecurity by governments and the sector must accompany the study. Since information technology has become a driving force in development, Cybersecurity must be a key component of digitization to protect people's rights, confidence, and security in India and Pakistan.

References

Baezner, M. (2018). *Hotspot Analysis: Regional rivalry between India- Pakistan: tit-for-tat in cyberspace*. *CSS CYBER DEFENSE PROJECT*. CSS/ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-

interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf

Dilaprij, E. (2013). 173 AIR POWER Journal Vol. 8 No. 3, MONSOON 2013 (July-September)CYBER WARFARE AND NATIONAL SECURITY. *Air Power*. https://www.researchgate.net/publication/333651250_Cyber_Warfare_and_National_Security_An_Analysis_of_Incidents_Between_India_and_Pakistan

Garsein, A. (2012). Pakistan vs India: Who's the better hacker?]. Express Trib.

Blogs.

Hashim, A. (2014). Timeline: India-Pakistan relations. Al Jazeera. URL

Joshi, S. (2012). 112 government websites hacked in the last 3 months]. The

Hindu. URL Kumar Jha, A., 2014. Indo-Pak Conflict rises up, Hackers on the way for a Cyber war!!!

Khan, L.A. (2014). Hitting back, Indian hackers deface Pakistani websites .

The Hindu.

Kumar, M. (2012). 30 Pakistan government Sites goes down . Hacker News.

How to Citation: Fayaz, S. (2022). State-Level Response and Cyber Security: A Comparative Study of Pakistan and India. *Journal of Strategic Policy and Global Affairs*, *01*(01), 11–17.

Leyden, J. (2010). Indian feds' site besmirched in tit-fortat Pak hack attack.

Mid Day. (2012). Indo-Pak cyber war on Jan 26. Day.

Malik, M. B. (2020). *Pakistan & India Cyber Security Strategy | Muhammad Baqir Malik*. Academia.edu. https://www.academia.edu/7935735/Pakistan_and_India_Cyber_Security_Strategy

Mustafa, G. (2020). Cyber Warfare Between Pakistan and India: Implications for the Region. https://www.researchgate.net/publication/347409992_Cyber_Warfare_Between_Pakistan_and_India_Implications_for_the_Region

RFSID. (2016). Hacktivism: India vs. Pakistan

Ribeiro, J. (2008). Feuding India, Pakistani hackers deface web sites Networkworld.

Tufail, T. (2018). COMPARING THE NATIONAL CYBER SECURITY FRAMEWORK OF PAKISTAN WITH INDIA AND UNITED KINGDOM. *TALLINN UNIVERSITY OF TECHNOLOGY*. file:///C:/Users/khan/Downloads/56aa279d3c194610b25da33defc6d149.pdf

Web Desk. (2014a). Suspected Indian hackers deface Pakistan's MET website. Express Tribe.