Pakistan Languages and Humanities Review
www.plhr.org.pk

RESEARCH PAPER

Cyber Warfare between Pakistan and India: Implications for the Region

[1]Dr. Ghulam Mustafa* [2]Zainab Murtaza [3]Khadija Murtaza

1. Assistant Professor, Department of Political Science & International Relations, Government College University Faisalabad, Punjab, Pakistan
2. Ph. D Scholar, Department of Political Science & International Relations, Government College University Faisalabad, Punjab, Pakistan
3. Ph. D Scholar, Department of Political Science & International Relations, Government College University Faisalabad, Punjab, Pakistan

DOI http://doi.org/10.47205/plhr.2020(4-I)2.5

PAPER INFO

Received:
January 14, 2020
Accepted:
June 15, 2020
Online:
June 30, 2020

Keywords:
Cyber security, Cyber warfare, Indian Advanced Persistent Threats, Pakistani Advanced Persistent Threats

Corresponding Author*

ghulammustafa@gcuf.edu.pk

ABSTRACT

In 21stcentury, Cyber security threats are one of the principle national securities and each country faces financial difficulties. The internet is a characterizing highlight of current life. People and networks overall interface, mingle and arrange themselves in and through the internet. The presence of various Cyber security issues on different circles of life normally increment political enthusiasm for settling them. When the Cold War ended, professionals started to argue that the main subject of global security must be change to reflect the changing nature of conflict. The main aim of this paper is investigating cyber warfare between Pakistan and India. The relations of Pakistan and India are mostly contradictory because both sides are always trying to gain their strategic goals first by nuclear program then by cyber warfare. New technologies are immediately coordinated into standard military and diplomatic doctrine. Both states utilize the internet as cyberspace to hassle or deter the opponent with little danger of retribution and counter. The race of cyber technology as cyber weapon is creating threat to regional security.

Introduction

Cyber security has become a national significance of state due to cyber warfare in cyber space. The study of this new age of national cyber security techniques uncovers a key development in policy making of government; however, cyber security is raised among priorities of government. According to these strategies general assessment of government is that the network and Information and Communication Technologies (ICTs) are basic for monetary and social development. In a general setting of monetary downturn, the open Internet and ICTs are another tool of development and a driver for advancement, social prosperity and individual articulation. As the Internet economy develops, including governments, the entire economy and society become progressively dependent on this computerized framework to play out their fundamental functions. Both states India and Pakistan are nuclear powers, moreover, both have traditional military tactics as well as both have involved in virtual war of words and trying to damage each other by hacks the secure and secret information from 1990s (Fazzini, 2019).

The global dynamics are weakening due to high mobilization. Now the society understands by a study of message and communication facilities (Alker, 2011).Both states are competently using cyber warfare capabilities to pursue the regional objectives in South Asian, especially to maintain hegemony and increase influence in the south Asia. India always violates the Line of Control, however, it is against the international law and during the peacetime it is not acceptable to target the civilians or moving near the border according to international law. On the other side, India always attempts to defame the Pakistan's image by misguiding and manipulating global media. A RAW sponsored group caught in Karachi University by the end of March 2020, fuelling terrorist and propagation activities against Pakistan (Khan, 2020). These types of activities are increasing warfare threats which pose serious security concerns for Pakistan. Cyber warfare use different skills and techniques. Now a day, Cyber warfare is major threat in South Asian region which used to influence the adversary. There are new technologies quickly introducing and incorporating into the strategies of both states, Pakistan and India. The aim of study to check the impact of cyber war of Pakistan and India on region. Cyberspace a useful tool has develop a space where nationalistic and devoted hackers their patriotic feelings and denigrate the adversary from both sides can express. Cyberspace is also working as Advanced Persistent Threats (APTs), however, these patriotic and activist groups have highly grip and links to the institutions of state, they are working to spy and steal information to achieve the strategic goals. APTs use different techniques like spear phishing for getting contact and control to the network of adversary, after that infect them with different viruses like malware of spying (Khalil, 2020). The paper examines cyber warfare among Pakistan and India.

Literature Review

The book name Cyber security Policies and Strategies for Cyber warfare Prevention Cyber security has written by Richet, Jean-Loupin 2015, according to writer due to cyber warfare, cyber security has become a subject of worry over the previous decade as private industry, organization and business have increased a more noteworthy online nearness. In book, author describes a vital production on the most recent legitimate and cautious measures being actualized to ensure people from cyber warfare. Inspecting on the web criminal systems and dangers in both general society and private circles, this book is a vital expansion to the reference assortments of IT pros and executives keen on revealing better approaches to obstruct digital penetrates and ensure delicate computerized data.

The book name Cyber Warfare Its Implications on National Security written by Sanjeev Reli in 2016. According to writer, every time carries with it new systems and techniques for pursuing a war. This book is an endeavor to comprehend different subtleties of cyber warfare and how it influences national security. In view of the cyber threat condition, the books suggests a system of cyber precept and cyber procedures just as hierarchical structure of different associations which a country needs to put resources in this policy.

In both book writers did not explore the implications and threats against Cyber security. They did not explain the cyber warfare risk and threat to region or world in detail.

Material and Methods

The cyber space has begun to grow in terms of information with the passage of time and also in the population of users.The study is primarily analyzing the changing trends and patterns of Pakistani and Indian Cyberspace policies and strategies which adopted by both states in diverse times of history. So, the study is based on analytical and descriptive design of research. The requisite data for article is collected from secondary sources like books, newspapers, documents, journals and previous research works. The nature of data collected for this study is qualitative.

Historical Background

In this global world, the security covers variety of organized issues that influence endurance. It ranges from the traditional military force methods, financial quality, the causes and results of conflict in the middle of different states, to religious, ideological and ethnic conflicts, financial and cost-effective clashes, vitality provisions, science and technology, further, risks to security of human and the state's stability from natural debasement, eco-friendly change, seductive disease, and the exercises of non-state actors.

World War II saw the presentation of atomic weapons, cruise and ballistic missiles, which activated and different major changes in the warfare scenario. During the Cold War, the attention of international security studied was normally on superpower strife and nuclear war in light of the fact that customary ideas of security concentrated on the utilization of power between incredible forces. When Cold War ended, professionals started working and arguing that the main subject of global security must be change to reflect the changing nature of conflict. As the Internet encountered its fast extension during the 1990s, programmers started participating in cyber tricks called as pranks while low-level crooks started investigating the potential for cybercrime. When it was indicated that wrongdoing pays in the cyber space, the crime started muscling its direction onto the scene, at times clearly with the help of the governments on whose region they were working.

Cyber security has become a national significance of state. The study of this new age of national cyber security techniques uncovers a key development in policy making of government; however, cyber security is raised among priorities of government. According to these strategies general assessment of government is that the Internet and ICTs are basic for monetary and social development.

The South Asian states India and Pakistan since their birth in 1947 have fought three major conventional wars ever, in 1947-48, 1965 and 1971, and a slighter battle in 1999 (Relations, 2020). The tension between the two nations increased at the end of the 20th century to its highest level when both states got the status of nuclear weapon states. The relationship among both states Pakistan and India is mostly stressful and the both states are trying to get strategic gain from the beginning to present. Different innovations, for instance, are instantaneously coordinated into ordinary military and diplomatic doctrine. Hence, both states saw the chance to utilize the internet as cyberspace to hassle or deter the opponent with little danger of retribution and counter. In 1998, the hackers of Pakistan effectively infiltrated the Atomic Research Center of India (Down.com, 2011). Throughout the late 1990s to today, Pakistani patriotic groups have introduced in history many successful campaigns related to hacktivism. Cyber provocation comprises for the most part of website damages and this ordinarily happens on Independence Days and remembrance. Pakistan despite everything remains behind in this domain and don't have exactly any solid arrangement and policy to avoid risk.

Cyber space is a lot riskier than other customary threat. In Pakistan the department of technology is not getting serious attention, on the other side, India is fixed huge budge for hi-tech technology field to exceed expectations in the cyber space to overcome different competitors in the region. The technological collaboration of India and Israel in the cyberspace has profited the previous. In 2013, India tried to maintain dominance in technology field by way of their National Cyber Security Policy was established. India for recent years designates an attractive measure of budget in cyber space for research work. Relevantly, According to Indian Business Standard in 2017, 2017-18 financial limit, India allocated 8% budge for improvement in cyberspace along with 2,58,589 crores of defense budget. Then again Pakistan has not gained a lot of ground in Cyber space specifically and technology advancement generally. According to World Intellectual Property Organization (WIPO), Global Innovation Index that gives detail about measurements of developments of 127 states around the global world. This study includes 81 pointers to investigate summon, training or education, world of politics, framework and business complexity. Cyber attacks are normally low force, unsophisticated which cause little harm (Rizwan Naseer, 2018). (Relations, 2020)

An entertainer can't be recognized as the culprit of a cyber attack with supreme sureness. Culprits can impersonate or emulate the apparatuses, procedures and conduct of different on-screen characters to befuddle the examiners. On-screen characters associated with the both states Pakistani and Indian condition of tit for-tat in the cyber space is various. According to Hotspot Analysis, the both states have been quarantined in 2 gatherings: first is the patriotic hackers and programmers, and second is the Advanced Persistent Threats (APTs). Most entertainers are hackers or devoted programmers, who regularly take part in site mutilations. The programmers or activists frequently freely guarantee the disfigurement tasks, yet this is hard toward discern whether they help out comparable gatherings or whether they appreciate state support. Here one important thing is about hackers and devoted programmers in Pakistan and India have neutralized the states by mutilating their own administration's sites towards decry defilement or forces fierceness. Cyber Security companies have likewise watched then distinguished APT gatherings which originating from Pakistan and India that directs more complex cyber attacks instead of site disfigurement.

Pakistan

Pakistan approved the Electronic Crime Ordinance in 2007 to give strict principles over the utilization of network (Usman, 2019). The National Response Center for Cybercrimes of Federal Investigation Agency of Pakistan tries to improve the ability of administration to avert and explore Cyber Crime, resources of secure material and give suitable information to offices and basic management related to cyber threats and restoration methods. The Center is the point for global joint effort which created in 2003 and assembles intelligence of cyber security. It seeks mainly the virus attacks, fraud of credit card cases and economic criminalities. In Pakistan, there is active hacker groups validated attentiveness in cyber skills.

India

In 1990s, the armed force of India moved strategy to join cyber warfare and activities of information in its policy. The policy encouraged the modernization of four military components development of electronic warfare, information technology, basic structure of security and armed force flexibility. Senior Indian Army officials emphasized the requirement in December 2009 for India to build up the capacity to counter threat and explicitly cyber threats (James A. Lewis, 2011). Inside the Ministry of Defense India includes different units to improve its cyber security. The Defense Information Warfare Agency of India organizes retorts of information warfare. The National Technical Intelligence Communication Center of India and the Defense Intelligence Agency have attempting toward make a collective cyber squad that can hack lawfully make the government aware of potential cyber vulnerabilities. The Development Organization and Defense Research made two zones for testing systems of electronic warfare. The Indian Army made the Cyber Security Establishment in 2005 to make sure about systems at the dissection level and audits of direct security. Additionally, the military settled Indian Cyber Security Laboratory in April 2010 at the Indian Military College of Telecommunications Engineering. Basis of cyber intelligence is primarily based by the Research and Analysis Wing of the office of Prime Minister. However, National Security Advisory Board of India suggested the formation of focal cyber security order which modeled on the Cyber Command of United States. More recently, the National Technical Research Organization, alongside the Defense Intelligence Agency, are answerable for creating hostile cyberspace capacities. India and United States also signed memorandum of understanding (MOU) that empowers operational and technical collaboration to stop the cyber threats. The small grid of India has made traditional grid operations to be more reliant on IT infrastructure to monitor the system then control and compute the requirements. Cyber security service level agreements can help to reduce the risk of attack (Reji Pillai, 2017).

Pakistani Hacker Groups

In start, Pakistani patriotic programmers and hackers appear to utilize the internet to focus on the enemies especially in the competition with India. Pakistani hacker generally focused on Indian government websites utilizing mutilation strategies just like Indian hacktivists. Especially, Pakistani hackers were energetic to counter Indian hacking after the events or explicit physical actions in Indian occupied Kashmir. Likewise with Indian hackers, it stays hazy that Pakistani hackers were working in groups or individually for themselves and for the reason. In November 2008, Pakistan Cyber Army (PCA) worked first time in the mutilation of the Indian Oil and Natural Gas Company (Team, 2014). However, the PCA apparently worked in counter for the previous mutilation of the websites of Pakistani after Mumbai attacks (Research, 2019). The PCA utilized basic techniques to ruin websites of India. In 2013, a cyber-security firm, Threat Connect, identified at least three individuals from the PCA. In any case, it stays not clear that the gathering consumes connections to the government of Pakistan or they acted just as individual.

Pakistani Advanced Persistent Threats (APTs)

The Pakistani Advanced Persistent Threats (APTs)(Former, 2019)uncovered by Cyber security firm Proof point in report on Operation named Operation Transparent Tribe, which included a lance phishing effort in February 2016 against Indian embassies in Kazakhstan and Saudi Arabia. In March 2016, Trend Micro uncovered the story that similar hacking team of Pakistan was behind Operation called C-Major. Since at least 2012, Pakistani APT has been active. The APT made fake news websites and sent the connection by using email to download tainted records. The Pakistani APT utilized command and control along with Pakistani Internet Protocol (IP) addresses. However according Trend Micro, the APT utilized known susceptibilities to convey virus malware and its command and control structure that was easy to plot. While, it also shows generally naive cyber attack capacities. Despite the fact that the objectives of Pakistani APT are additionally suspiciously in accordance to the interests of the government of Pakistan, further Trend Micro had not the proof point and option to interface their relationship.

Indian Hacker Groups

Indian hackers and patriotic programmers are to a great extent identified in cyberspace working with defense to Indian national interests. Indian hacktivists and energetic programmers mostly executed website destruction on government sites of Pakistan. These programmers also proclaimed secret attacks on Pakistani governmental websites and air terminals. These culprits were generally active on commemoration of the Mumbai psychological militant attacks and Pakistan Independence Day. It stays uncertain if the hacktivists and enthusiastic programmers were individual or groups. However, they worked in a joint effort along with different hacker and patriotic programmers. Some of them took part in one destruction battle afterward vanished from the scene. This type of behavior recommends that these hacktivists are in all possibility content kiddies. In that capacity, they may took interest in these campaign for the adventure or to check their knowledge. There are famous hacker group named Mallu Cyber Soldiers (MCS) (Salik, 2019) that also working with government because of the severe attacks it has executed. This was established in October 2014 as Indian cyber security specialists group whose goal is to secure and reestablish the Indian sites from cyber attacks of Pakistan.

Indian Advanced Persistent Threats (APTs)

In 2013, the Indian APT Norwegian broadcast communications firm found an Indian APT that focused with stick phishing emails. Shadow server Foundation and the Norman Shark, two cyber security organizations that examined the Indian APT. They explored the groups which had been active since 2010. Different cyber security specialists have expressed that the Indian APT groups are not made out of profoundly advanced hackers, as the APT ordinarily utilized malware accessible for free. Specialists also observed that the Indian APT once in a while reused its infrastructure of C&C and bait records in spear phishing emails (Baezner, 2019). According to various specialists this particular APT is working for India for the most part focused on Pakistani associations. The main objectives of this firm is to work for military and political interests of India. Notwithstanding keeping an eye on Pakistan, since 2013 or 2014, the APT's exercises have pulled together China. In any case, this firm has also targeted firms in Europe such as Telenor company in Norway, however such type of activities may be increasingly likened to financial spying. The Indian APT re-appropriate a portion of its work to external contractors. In light of different cyber security provides the details regarding Indian APT, it has support from the Indian specialists.

Targets by Both States against each other

According to Myrium Dunn the American scholar, the process of securitization has inevitably meant a move towards the more extreme end of cyber-threat spectrum and increasing talk of cyber warfare, as most important element of cyber-threat. Cyber actors from India and Pakistan focused on generally equal objects and targets. However, hackers of India and Pakistan inclined to target each other's governmental and different websites of media. When hackers attacked government sites reflects that they are doing for the political goals which indicated that they needed their activities to be taken note. In 2010 December, thirty-six websites of government were hacked by Indian group of Indian Cyber Army. Later, they claimed that Pakistan Navy, foreign affairs, education, National Accountability

Bureau, finance, NADRA were among of hacked websites. These websites were hosted no same server that's why they hacked easily. The Indian hackers then sent massage to all websites that they hacked websites in retaliation to the Mumbai attacks 26/11. Pakistan removes this message from websites. However since 2001, these type of cyber attacks have been seen from both sides (Haque, 2010).

Just after two days, Pakistani hackers took revenge and the group named Predators PK hacked more than 200 Indian websites. They did similar to Indian cyber attackers and inserted pages on Indian servers and sites. The Predators PK group mainly focused on Central Bureau of Investigation, college websites, NGOs, religious sites and Indian companies. They damaged most of Indian websites. The Predators PK messaged to Indian hackers as Warning to all cursive tots to stop hacking websites of Pakistani, they further said your security of websites was good but we like breaking it(Haque, Cyber war escalates: Pakistani hackers 'take revenge', 2010).

Pakistani APT focused on principally Indian military and strategic staff for the motivations behind national security secret activities, yet additionally focused on other political and military substances in South Asia. The equivalent was watched for the Indian APT. India's APT directed for the most part cyber espionage against Pakistani private firms and government organizations, yet in addition against global ventures. Universal attacks were likely endeavors to increase monetary data. The report of Norman Shark and Shadow server Foundation uncovered that the Indian APT's tasks didn't generally line up with the interests of the state. It is conceivable that there were a progression of ineffectively planned littler tasks inside the Indian government that undermined the APT's adequacy. Additionally, a few tasks could have been redistributed to a contractual worker that reuses a similar foundation for numerous customers. As far as following attacks on cyber security, whole employments of mutual foundation could show up as though they were executed by APT of India.

In 2014, according British news agency Pakistani hackers name Team Madleets attacked on 2118 websites of India including Central Bank of India and web page of Indian actress Poonam Pandey, the team Madleets wrote Pakistan Zindabad on its main page and also set Nation Anthem as background music. British agency said that Indian cyber security official claimed that Indian hackers attacked on nearly hundred Pakistani sites in retaliation. But there is no verification of India about hacking Pakistani Websites (Desk, 2014).

In 2018, Pakistani hackers attacked mass cyber-attack on Indian websites. Border conflicts between Pakistan and India also have great effect on Cyber world. However, Pakistani programmers and hackers attacked and defaced a large number of websites of India including top hosting companies, Government of Gujarat website official website of the Kerala Government. The Pakistani Hackers display massage on home page that Security is only an illusion and Pakistan Zindabad. Pakistani Hackers used Indian Servers to phishing attempts on US based banks. However after these cyber-attack, Indian government authorities did not issue any statement. While the Indian prime Minister is investing huge amount on the Digital India to strong the department of Indian Cyber Security. On the other side India has also facing huge unavailability of Cyber Security Professionals as gradually India is rushing to make a mark on the front (Rahul, 2016).

In 2017, on the day of Independence of Pakistan sseveral Pakistani Ministries websites hacked by Indian Hackers in retaliation to Pakistan hackers defaced over 7000 Indian websites. However there has been continuing battle between the hackers of both states. Both states hackers often times leave a mark with their virtual hacking tags and circulate patriotic material on these websites (techjuice, 2017).

Tools and techniques Used by APTs

India and Pakistan in cyber warfare used different tools and techniques to achieve their aims against opponent. APTs use spear phishing to trace the network of their victim and then make them infected with virus of spying malware. Pakistani and Indian hackers use malicious Android applications in their operations. These type of malicious applications can steal messages, emails, call logs, addresses, photos, contacts, SD card data and record voice calls. In February 2016, a chat application popular in Indian Army forces named SmeshApp, at that time the Indian Army warned about threat regarding this application (Cimpanu, 2016). They also accused ISI Pakistani agency for developing the application to acquire access smartphones of military forces.

Regional Implications

There is no system in the cyberspace which cannot be hacked. In cyber warfare, any patriotic hacker of any state can break any kind of lock and the same can hack websites. In dealing with the hacking problem, states never establishes seriousness, which poses a threat to all state of the region even world. While in both countries aggression is the only tactic followed by the hacker groups, on the contrary, the security providers for the cyber space have always been deficient in care to provide security to cyber networks of their country.

Threat to National Security

According to Executive Director of the Bangalore-based Centre for Internet and Society name Sunil Abraham, the Indian government has a very low level of awareness about cyber space and cyber security. India is not taking serious cyber security as the rest of the world. The cyber programmers who carry out hacking and website defacing jobs may also get involved in cyber espionage and data stealing against their enemy states. These people can be serve for the terrorist organisations just for money, in result the situation will be alarming.

According to a cyber security professional working with one of intelligence agencies of India. There are some new malwares Stuxnet, Flame, Duqu etc. and many more are in the process of developing. If these are not protected properly, these can be operate as cyber weapons incredibly and unbearable by the hacker groups, then the situation would become more dangerous for the security of region. Because it is equivalent important to terrorists for getting access to nuclear weapons for power. Though Pakistan does not have perfect national cyber security strategy and it is also on alert. But Pakistan is doing serious effort to develop a framework that will protect Pakistan network and critical institutions from cyber attacks. The Edward Snowden leaks motivated and appreciated these efforts. However Pakistan needs to address the gaps in their information security.

Race of Cyber Weapons

Each state has their own cyber espionage dissection, which taps critical information from national security of other states and intelligence organizations. India launched Operation named Hangover Operation to target Pakistan. Later, in response, Pakistan also organized Operation Arachnophobia, the aim of this operation to obtain intelligence from Indian officials. However these operations are famous and well-known, but there is still a lack of awareness on how much each country spends on cyber technologies to get information and which types of technologies they are employing to gain its interest (Baig, 2019). The whole economies of some states have been paralysed due to race of cyberspace and states have to make their selves more resilient. Due to the cyber warfare, the areas of telecom, defence and power are on top of our agenda. In result, Pakistan and Indian hacker groups hacking and defacing websites and stealing information to take personal revenge, economic influence, to get technical supremacy and to do anti-national propaganda. The hacker groups are working on making more malwares and applications to effect and influence other state which is increasing the race of cyber weapons for national interest. It can be dangerous for region because other states get motivation from India and Pakistan.

Geopolitical threat in the Region

According to Indian specialists, India faces many cyber attacks which can be attributed back to China, such as highlighted in a recent report by a department in the Ministry of Electronics and Information Technology to the National Security Council Secretariat. The Pulwama attack (BBC, 2019) and the escalating tensions between Pakistan and India, China has wanted to ensure a war does not break out. If a war started, China would be more inclined to offer support to Pakistan because of China's close relationship with Pakistan. As China is far more advanced in this arena, this support could include cyber capabilities and actions. In this way Pakistan can maintain influence on India.

Conclusion and Recommendations

Cyber space is a lot riskier than other customary threat. Cyber warfare has excavated its roots in South Asian region especially in Pakistan. However, War cannot be fascinating but Cyber warfare use different type of tools in conflicts. Mostly these conflicts consist of cyber threats sideways social dissolution, economic and political subversion. Pakistan should take quick and tough measures to identify the real people behind hacking and cyber. Pakistan should more research to understand the cyber capabilities of each country.

As most of the hackers are teenagers, Pakistan should recruit more patriotic programmers in its cyber security infrastructures. In this way Pakistan will not only give a future to these youngsters but will also create a strong cyber security culture in the country. Pakistan has very talented people in the private IT sector which can be beneficial for development in cyberspace. Furthermore, the experts of cyber security in the private sector can also be invited to train the professionals of governmental cyber security of the country. Then extremely reliable government cyber security civilian professionals can also be used to train the defense cyber security personnel for national interest. In this way Pakistan will prepare for any kind of cyber espionage and cyber attack, and will able to protect its civilian and military infrastructure more effectively. However Pakistan should work hard for in the field of cyber space and develop large industry of cyber security for defense of Pakistani technology and websites. Pakistan should develop different policies regarding cyber warfare to secure cyber technology of Pakistan and control the Indian cyber threats. So, Pakistan can maintain balance of power in Cyberspace area. Different organizations at national level and at the degree of military should be raised which can secure state's benefits and are additionally equipped for undertaking hostile cyber tasks. However, the importance of cyber politics is increasing nowadays, so, in cyberspace Pakistan needs more political expertise and policymakers to resolve cyber issue.

References

Alker, H. R. (2011). The powers and pathologies of networks: Insights from the political cybernetics of Karl W. Deutsch. *European Journal of international relations, 17*(2), 354-378.

Baezner, :. M. (2019). Hotspot Analysis: Ir*anian cyber-activities in the context of regional rivalries and international tensions.* Center for Strategic Studies.

Baig, R. (2019, March 26). *Could Offensive Cyber Capabilities Tip India and Pakistan to War? The Diplomat*

BBC. (2019, may 1). Kashmir attack: Tracing the path that led to Pulwama. *BBC News*:

Cimpanu, C. (2016, March 19). *smeshapp removed from playstore because Pakistan used it to spy Indian army. softpedia*

Desk, N. (2014, January 30). *Pakistani hackers attacked 2,118 Indian websites. Pakistan Todays*

Down.com. (2011, July 28). The futility of Indo-Pak cyber wars. *Dawn:*

Fazzini, K. (2019, February 27). In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides. *CNBC*

Former, B. (2019, November 27). *India and Pakistan waging a cyberwar over Kashmir intelligence.*

Haque, J. (2010, December 4). *Cyber war escalates: Pakistani hackers 'take revenge'. The Express Tribun*

Haque, J. (2010, December 1). *Cyber warfare: Indian hackers take down 36 govt websites. The Express Tribuen*

James A. Lewis, K. T. (2011). *Cyber security and Cyber warfare*. Center for Strategic and International Studies.

Khalil, B. (2020, April 8). *India's Hybrid / Cyber threats and its regional implications. moderndiplomacy*

Khan, F. (2020, April 2). JIT on local RAW network finds weapons in Karachi University raid. *The News*

Rahul. (2016, February 9). *Mass Cyber Attack 2016 : Pakistani Hackers deface Indian Websites*. VieEns: https://viaens.com/blog/mass-cyber-attack-2016-pakistani-hackers-deface-indian-websites/

Reji Pillai, R. S. (2017). Indian manual for cyber security in power systems. *IET journals The Institution of Engineering and technology*.

Relations, C. o. (2020, April 22). *Global Conflict Tracker*. Retrieved from Council on Foreign Relations: https://www.cfr.org/interactive/global-conflict-tracker/conflict/conflict-between-india-and-pakistan

Research, C. E. (2019, November 11). *Mumbai Terror Attacks Fast Facts*. *cnn*:

Rizwan Naseer, M. A. (2018). Cyber-Threats to Strategic Networks: Challenges for Pakistan Security. *A Research Journal of South Asian Studies, 33*, 35-48.

Salik, Z. I. (2019, september 9). *Pakistan-India Cyberspace Shenanigans*. T*he day spring*

Team, T. R. (2014, June 10). *Debugging the Pakistan Cyber Army: From Pakbugs to Bitterbugs*.

techjuice. (2017, August 14). Pakistani Ministries websites hacked by Indian Hackers. *techjuice*

Usman, M. (2019). Cyber Crime: Pakistani Perspective. *Internationational Islamic University Journal*. https://www.iiu.edu.pk/wp-content/uploads/downloads/journals/ilr/volume1/num-3/Article-2-Vol-1-No-3-140119.pdf