INDIA'S CYBER WARFARE CAPABILITIES: REPERCUSSIONS FOR PAKISTAN'S NATIONAL SECURITY

Ms. Nageen Ashraf and Dr. Saima Ashraf Kayani[*]

Abstract

Cyber warfare refers to a state's ability to penetrate another state's digital systems to cause disruption. Cyber warfare has emerged as the fifth operational warfighting domain. India has been strengthening its cyber warfare capabilities for a long time, which can seriously affect Pakistan. Considering the theoretical constructs of Barry Buzan and Ole Waever regarding the broader concept of security, this paper aims to highlight the possible threats and security challenges that India's cyberspace can pose to Pakistan's national security. The paper argues that India has acquired a robust cyberspace that can potentially cause financial damage, political instability, societal unrest, and radicalisation in Pakistan's society. Furthermore, strong cyberspace can also challenge nuclear deterrence between the two neighbours, thus threatening military security. The paper concludes with recommendations regarding what Pakistan can do to mitigate this growing cyber threat.

Keywords: Cyber Warfare, Cyber Security, Social Instability, Political Interference, Cyber-Nuclear Threat.

Introduction

Pakistan's expenditure on its defence makes a good deal of sense considering the regional dynamics. Since its independence, Pakistan has been struggling with its physical security due to multiple threats, especially from its neighbourhood. Therefore, Pakistan's focus on securing its borders does not come as a surprise. However, Pakistan must work on traditional and non-traditional security challenges to counter all possible future threats without compromising border security. For Pakistan, it is essential to have a system robust enough to retaliate against a cyber-attack if not prevented. The gradual change and escalation in India's nuclear stratagem after the Mumbai attacks depict that India has become aggressive with

[*]Ms. Nageen Ashraf is currently an MPhil scholar at the School of Politics and International Relations (SPIR), Quaid-i-Azam University, Islamabad. Dr. Saima Ashraf Kayani is a Chairperson Department of International Relations, Fatima Jinnah Women University (FJWU), Rawalpindi. The authors' email address is nageenashraf13@gmail.com.

time. Since geopolitical tensions regarding the nation's cyber security considerations cannot be disregarded,[1] it is pertinent for Pakistan to be prepared for cyber warfare. The question is, in what ways can India threaten Pakistan's national security using cyberspace as an instrument? This paper aims to answer this question using primary data (official government documents, policies, and interviews) and secondary data.

Theoretical Framework

The term 'security' has broadened with time, especially after the landmark contributions of Barry Buzan and Ole Waever. Buzan and Waever presented the broader concept of security. They argued that security was not just limited to the security of borders but also other domains, including economic, political, environmental, and societal security.[2] Some scholars have also looked at cyberspace and its emergence as a grave threat to national security from the realist point of view. Anthony Craig, Brandon Valeriano and multiple scholars have argued that cyberspace, its anomalies, instability and challenges to deterrence can be aptly understood using the realist school of thought. In addition, realism also helps to explain existing anarchy and security dilemmas in the realm of cyberspace.[3] In contrast to cyber realism, this paper aims at theorising cyberspace from Copenhagen's school of thought.

Even though Buzan failed to identify cyber security threats, cyberspace is a domain that can, to some extent, affect all other national security domains. Buzan argued that cybersecurity did not need to be theorised as a separate security sector.[4] However, with time, multiple changes in the security dynamics demanded cyber security be granted the same level of attention as other domains.[5] Rachel E. Yould asserted, "[Information Technology] IT may be the common underlying factor upon which all security sectors are destined to converge."[6] Considering the broadened concept of security, this paper argues that cyber security can have severe implications for military security, economic security, political security, and societal society. The paper identifies various scenarios in which India's robust cyberspace can cause instability in Pakistan and, thus, is a serious national security concern.

Cyber Warfare

With time, the dynamics of warfare have also changed. The changing dynamics are attributed to cyberspace, Artificial Intelligence, and other factors. Wars, now, can be carried out without inflicting any kinetic attack on the adversary. The battlefields have shifted from physical battlegrounds to virtual and physical armies to cyber armies. States use the internet, social media and cyberspace to run propaganda, information, or cyber warfare against an adversary. In all such types of

warfare, the primary aim of the attacker state is to acquire essential (and sometimes classified) information or cause disruption to jeopardise the targeted state's national security. Due to these reasons, cyber security has become an integral part of the national security framework, and South Asia is not an exception to this cyber security dilemma.

Cyber warfare is a contested concept. There are multiple definitions of cyber warfare. According to the most accepted report given by Clarke and Knake, cyber warfare can be defined as "actions by a nation-state to penetrate another nation's computers or networks to cause damage or disruption."[7] Some sources also include information gathering and cyber-attacks in cyber warfare. On the other hand, some refuse to consider them a part of cyber warfare.[8] Due to the ambiguity and contestation that exists on an international level, states have tried to define cyber warfare in their terms, further exacerbating the cyber security dilemma.

India's Robust Cyberspace

India has been working towards strengthening its cyberspace for a long time. Some of the significant efforts by India towards digitisation and self-dependency include the development of the National Informatics Centre in 1976, the New Electronics Policy (NEP) in 1984, the establishment of the National Task Force on IT and Software Development in 1998, the Information Technology Act in 2000, a comprehensive National Cyber Security Policy in 2013, and Modi's efforts towards Digital India in 2015.[9] All of these efforts indicate India's ambitions to become one of the leading IT industries in the world.

Considering the definition of cyber warfare by Clarke and Knake mentioned earlier, India's efforts towards digitisation have enabled it to develop cyberspace capabilities strong enough to penetrate Pakistan's computers and network systems. It is indicative of the fact that India possesses cyber warfare capabilities. On the other hand, various factors did not enable Pakistan to grow in its cyberspace capabilities. These factors include lack of awareness, slow digitisation, reliance on traditional methods, meagre investment and subsidies in Research and Development (R&D) and IT, and reluctance to develop a comprehensive national cyber security framework/policy. This gap has profound implications for the national security of Pakistan.

Repercussions for Pakistan

Baker defines cyber warfare as comprising "threats against national sovereignty."[10] Considering the growing cyberspace capabilities of India, the chances of a cyber war between Pakistan and India are plausible. Undoubtedly, India's

pursuit of cyber power affects Pakistan in many ways. For decades, both states have been fighting each other over Kashmir. Contemplating modern warfare, it is easier for India to launch a cyber-attack against Pakistan than a physical attack. A minor cyber incident can have a domino effect and start a chain of cyber-attacks having consequences like economic losses, security threats, radicalisation, political instability, crippling of critical infrastructure and propagation of anti-national propaganda, etc.[11]

a) **Economic Implications**

Launching a cyber-attack would be advantageous for India not only because it will be cheaper than a physical attack but also because cyber-attacks can deteriorate the domestic security of an opponent, which can cause severe economic consequences.[12] Growing cyber criminals are a direct economic as well as national security threat to the states all around the world.[13] As per the Data Breach Investigation Report (DBIR) of 2020, out of all the cyber-attacks carried out, almost 91% of the attacks had financial and economic motives.[14] Usually, the stolen data is of no use to cyber criminals. They only steal data (of governmental departments or officials) under different contracts with business owners and companies to benefit from this identity theft.[15] In such a scenario, states can often hire the nationals of their adversary and pay them large amounts in return for their identity theft and data leakage. For instance, after the cooperation on cyber security began in the early 2000s, there was an incident where India found out that some of the nationals were serving US intelligence. After the incident, cyber cooperation saw a setback because of a lack of trust between Delhi and Washington.[16]

During Covid-19, Pakistan had been at a greater risk of cyber-attacks targeting the banking and e-commerce sector. In 2020, K-electric was affected by a cyber-attack where hackers threatened to expose the data of all K-electric customers if the management failed to pay $3.8 million in Bitcoin, threatening to double the mentioned amount if the command fails to comply with the said demand.[17] In 2021, Pakistan's FBR system was breached, and the hackers threatened to sell the data of FBR for US $30,000 on the Russian forums.[18] The economic loss can also be in a way that Pakistan spends millions of dollars on a project or a technology and India can steal it without direct military confrontation. So, all the money goes down the drain when the adversary obtains such information without spending a penny.

b) **Security Implications**

One of the biggest problems with tackling cyber security is that whenever a threat is recognised, and action is taken to securitise the threat, new forms of threats can emerge in response to security measures taken to tackle previous threats, thus making security measures obsolete.[19] In 2021, Pakistan went through 'Pegasus' cyber-attacks in which the cell phones of government officials were hacked. Such attacks have profound security implications and are used for surveillance. The attacker can also monitor the victim's movement and collect data through their microphones about essential discussions. It undermines the democratic system of the state as well by listening to the meetings and text messages.[20] Moreover, cyberspace poses multiple security threats in various forms, like nuclear threats,[21] cyber blockades,[22] radicalisation of population,[23] and its contribution to domestic instability.[24]

- **Nuclear Threat**. South Asia is considered a nuclear flash point, where an escalation of events can lead to a nuclear war between adversaries. The situation between both states has exacerbated after the Pulwama attack (2019) and India's abrogation of Article 370 in IIOJK. Terrible security implications of a cyber-attack cannot be disregarded because cyber security is essential to nuclear security. With time, cyberspace has become more integrated into nuclear systems.[25] For this reason, cyberspace has emerged as a serious threat to nuclear infrastructure in South Asia. There have been various incidents where cyber threats exposed the vulnerabilities of nuclear systems. A notable example is that of Stuxnet, one of the most sophisticated cyber weapons ever created, which is regarded as a game changer in cyber security.[26] Even though Stuxnet is mainly associated with Iran, it is an eye-opener for all the states possessing nuclear weapons.

Another example is Operation Orchard, initiated by Israel to destroy the Syrian nuclear reactor. The operation made use of cyber-attacks and kinetic attacks to achieve success.[27] As a result, the process successfully destroyed the Syrian nuclear reactor and halted Syria's acquisition of atomic weapons. Considering these examples and that conventional means could also be used alongside cyberspace, Pakistan faces a cyber-nuclear threat from India. Furthermore, insurgent groups are present on both sides, along with other non-state actors that can exploit cyberspace. In that case, if hacker groups access such cyber weapons, both states' national security would be at stake because it would be the same as terrorists getting access to nuclear

weapons.[28] Despite several crises, India and Pakistan did not declare a nuclear war against each other. The Kargil conflict was a small-scale conflict which could have escalated to a nuclear war, but fortunately, it did not. That is because even though India holds an offensive defence posture that asks for the first strike in case of a nuclear war, Pakistan's nuclear deterrence and second-strike capability refrained India from launching the first strike. However, things are changing now as India ambitiously moves towards developing hypersonic missiles.[29] Hypersonic missiles deprive the states of a second-strike capability and challenge nuclear deterrence because of their ability to remain undetectable by the opponent.[30] In such a dynamic scenario, cyber-attacks on the nuclear command and control systems can provoke states to launch a nuclear attack. This change has challenged the nuclear deterrence between India and Pakistan.

- **Cyber Blockade**. Analogous to the blockade of Cuba by the US in the 1960s, cyber-attacks can also serve as a blockade that isolates a state. During WW-I, the British separated Germany by disrupting its communication with other states.[31] Likewise, suppose India tries to carry a potential cyber-attack on Pakistan, having multiple political and economic objectives. In that case, it can also cripple the state's network system and can completely isolate it. Moreover, India could use modern cyber warfare techniques like launching Denial of Service attacks.[32] In such a scenario, Pakistan would barely have the potential to retaliate and ask for help from other states.

- **Domestic Instability**. Cyber-attacks can become a reason for communal division in a state. Vulnerable cyberspace can allow other state or non-state actors to influence the population and affect internal stability. In August 2012, people started receiving messages that included dangerous and threatening content in India,[33] and India has done the same to make things worse in an already-divided society of Pakistan. The Sunni-Shia divide is eminent in Pakistan, and India took advantage of this divide in 2019 when things escalated between Sunni and Shia communities because of several Shia killings. Later, the investigation traced the origin of the tweets containing trend Shia Genocide back to India. Moreover, India has been making use of Twitter to run anti-Pakistan propaganda since 2018. It was claimed that 80% of accounts spreading anti-Pakistan and anti-Shia propaganda were traced back to India.[34] Indian media was also seen

exaggerating the killing of Hazara Shias back in 2019. In one of the articles, an Indian author writes, "The unabated persecution of the Hazara Shia community, with the state failing to take any visible action, underlines the reality that there is no place for religious minorities in Pakistan."[35] Such is the use of cyberspace, which leads to domestic instability and insecurity. At the same time, such statements are ironic considering the treatment of occupied Kashmir's Shias, who were fired with pallet guns and tear gas on the holy day of the 10th of Muharram in 2020.[36]

- **Radicalisation of People**. The weaponisation of internet is also increasing, because of which the internet can become a source of radicalising people.[37] Many terrorist organisations seed people through the internet. The violent use of cyberspace to promote hate speech and anti-state propaganda can exploit the religious sentiments of Pakistan's population.[38] Balochistan militants are backed by foreign actors, especially India, in finance and training. These actors are also seen causing law and order situations now and then.[39] Cyberspace can serve as a psychological platform for the propagation of such agendas.

c) **Political Ramifications**

Cyberspace can be used to influence the political decision-making and political outcomes of a state as well. A notable example is the 2016 US elections. There have been accusations on Russia for interfering in the US elections in 2016 by conducting a disinformation campaign on social media and the internet. This influence was successful using different online methods, including hacking, strategic leaks and state propaganda.[40] Russia achieved its foreign policy goals using the internet for its objectives. Similarly, Indian cyber capabilities can also influence elections within Pakistan and help the party of its own choice win the polls. It undermines state sovereignty and is a threat to state democracy.

Cyberspace and social media can run propaganda warfare against the opponent and humiliate it internationally to achieve political goals. For example, after the Taliban took over Afghanistan and started to fight for Panjshir, Indian officials claimed that Pakistan was involved in the Panjshir battle. The accusations were preposterous because India used video clips from video games and portrayed Pakistani celebrities as commanders in Panjshir.[41] The allegations were also unconvincing when the Taliban and Pakistan denied Pakistan's involvement. During

a press conference, Zabihullah Mujahid, the Information Minister of Afghanistan, turned down the indictment of Pakistan's involvement by saying, "The interference from Pakistan is a rumour that has been propagated during last 20 years."[42]

In addition, the international community recognises the role of Pakistan as a significant mediator between the US, Afghan Taliban and the Afghan government. India acted as a peace spoiler and then conducted disinformation campaigns to disgrace Pakistan internationally. Reports showed that more than 50% of the information conveyed by Indian media regarding Afghanistan and Pakistan was fake. Pakistan has struggled a lot to wipe off the label of a terrorist state. Still, such disinformation could facilitate the Western media again to bring a pessimistic view of Pakistan to limelight.

d) **Social Implications**

At societal level, cyber-attacks promote hatred and instigate population to launch further attacks on the adversary. In addition, vulnerable and unregulated cyberspace can have various physical and psychological consequences. For example, cyberbullying affects mental health and can leave a person depressed.[43] Likewise, increasing cyber-attacks cause economic losses and diminish people's trust in companies. Moreover, propaganda warfare during conflict with other states has been a part of the state's objectives for a long time. Initially, the use of mass media was encouraged to spread propaganda and disinformation among the population. In contemporary times, this role is played by social media,[44] and propaganda warfare has come to be known as information warfare.

Social media platforms have become a significant source of information warfare rather than entertainment platforms. States use social media platforms to propagate their agendas to shape public opinion.[45] Twitter is a prominent example of how a social media platform has become an essential part of politics that tends to draw the attention of the public and world leaders towards a particular issue using everyday trends. In interviews, all academics agreed that social media platforms like TikTok, Twitter, etc., can be used as sources for cyber warfare.

What Can Be Done?

Because of the complexity of cyberspace and the type of actors involved, states' sovereignty has been undermined, and states do not have control over their cyberspaces. Because of this reason, it is not possible for even the most powerful

state to fully protect its cyberspace. However, for Pakistan, a few things can be done domestically to decrease the threats posed by cyberspace.

- ***Cyber Security Policy Implementation:*** It is impossible to fully secure cyberspace because of its simultaneous exposure to thousands of actors. However, efforts made to secure cyberspace by Pakistan have been minimal. At domestic level, the most important thing for Pakistan was to develop a robust cyber-security policy that entails cyber security as important as military security. Since Pakistan came up with a National Cyber Security Policy in July 2021,[46] its implementation should be given foremost importance before the policy becomes obsolete in this rapidly changing cyber environment.

- ***Budget Allocation:*** The budget should be allocated to the IT sector and R&D to enhance youth's capabilities in this domain. Besides budget allocation, law enforcement must be ensured to maximise the outcomes of efforts.

- ***Establishment of Institutes:*** Training institutes that focus primarily on strengthening cyberspace should be formed where students can learn more and more about this field. A proper cyber security workforce consisting of cyber security experts is the need of an hour. Similarly, cyber cells should be established where people can report cyber incidents. Many incidents go unreported because no specific body addresses cyber-related issues and attacks.

- ***Awareness Campaigns***: Awareness campaigns should be run where people should be made aware of the importance of cyberspace; their online rights and privacy concerns should be addressed.

- ***Cyber Agreements:*** To counter India's intentions of waging cyber war, a balance of power would play a key role for Pakistan. India has strengthened its cyberspace by signing agreements with states like the US, Russia and Israel. Likewise, agreements should be signed with technologically developed states to help Pakistan improve its IT sector. In this regard, China, which aims to become a cyber superpower in the coming few decades, could greatly assist. Pakistan and India can also sign a bilateral cyber agreement which will serve as a confidence-building measure between both states and might reduce future cyber-attacks from both sides.

- ***Self-sufficiency in the Technological Domain:*** Even though cyber agreements can help Pakistan improve its cyber security, the dependency and reliance on external support in cyberspace comes with its repercussions. One can never predict if the other state is trustworthy or not. Thus, total dependence on foreign technological partners should not be as crucial as self-reliance. Pakistan should try to become an exporter of technology rather than an importer and should facilitate the production of computers and other technological equipment in domestic industries by subsidizing them.

Conclusion

The technological evolution of the 21st century has shaped the modern world order and given rise to a new digital domain of conflict, i.e., cyberspace. Because of its anomalies and variation from traditional warfare, cyberspace has become a serious security concern for states worldwide. Securing cyberspace is a global challenge, and initiatives must be on an international and state level to mitigate cyber threats. Considering South Asia, India has long been trying to strengthen its cyber warfare capabilities to counter Pakistan in the region. For that, Pakistan needs to ensure the implementation of national cyber security policy, develop multiple institutions, educate its people on cyberspace and its vulnerabilities, and engage in cyber diplomacy to counter India in this 5th operational domain of warfare. Only then will Pakistan have the potential to mitigate the cyber-threats to its national security in a comprehensive manner and stand alongside the rapidly evolving world.

References

[1] Ramesh Subramanian, Historical Consciousness of Cyber Security in India. *IEEE Annals of the History of Computing*, *42*(4), 71-93. https://ieeexplore.ieee.org/abstract/document/9112688?casa

[2] Buzan, Barry, Ole Wæver, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998.

[3] Anthony J.S. Craig and Brandon Valeriano. "Realism and cyber conflict: Security in the digital age." *Realism in Practice* 85 (2018). https://www.researchgate.net/profile/Anthony-Craig-3/publication/323935798

[4] Barry Buzan, Ole Wæver, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis*. (Lynne Rienner Publishers, 1998).

[5] Lene Hansen and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International studies quarterly* 53, no. 4 (2009): 1155-1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

[6] Rachel E. Yould "Beyond the American Fortress: Understanding Homeland Security in the Information Age." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, edited by Latham Robert. (New York: The New Press ,2003)

[7] R. A. Clarke, & R. K. Knake .*The Next Threat to National Security and What to Do About It.* HarperCollins Publishers. 2010.

[8] Cameron H. Bell "Cyber Warfare and International Law: The Need for Clarity." *Towson University Journal of International Affairs* Vol. LI, No. 2. (2018). https://cpb-us-w2.wpmucdn.com/wp.towson.edu/dist/b/55/files/2018/05/SPRING-2018-ISSUE-1zf1eiz.pdf#page=27

[9] Ramesh Subramanian. "Historical Consciousness of Cyber Security in India." *IEEE Annals of the History of Computing* 42, no. 4 (2020): 71-93. https://doi.org/10.1109/MAHC.2020.3001215

[10] Elizabeth White Baker, A Model for the Impact of Cyber security Infrastructure on Economic Development in Emerging Economies: Evaluating the Contrasting Cases of India and Pakistan. *Information Technology for Development,* 20(2), 122–139, 2013, doi:10.1080/02681102.2013.832131

[11] E Dilipraj, "India's Cyber Security 2013: A Review." *Centre for Air Power Studies* 97, no. 14 (2013): 1-4.

[12] Anwesha Pathak, and Rohit Sharma. "Cyber Crime and Information Warfare-The New Arenas for WAR." *IITM Journal of Management and IT* 6, no. 1 (2015): 129-134.

[13] Subodh Kesharwani, Madhulika P. Sarkar, and Shelly Oberoi. "Cyber security in India: threats and challenges." *Cybernomics* 1, no. 2 (2019): 32-34. https://www.cybernomics.in/index.php/cnm/article/view/47

[14] Philippe Langlois, 2020 Data Breach Investigations Report. (2020). https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf

[15] James A. Lewis, "Computer Espionage, Titan Rain and China." *Center for Strategic and International Studies-Technology and Public Policy Program* 1 (2005). http://cybercampaigns.net/wp-content/uploads/2013/05/Titan-Rain-Moonlight-Maze.pdf

[16] Srijith K. Nair, "The case for an India-US partnership in cybersecurity." *Takshashila Institution, Inde* 14 (2010). https://static1.squarespace.com/static

[17] Sumaira Jajja, "K-Electric struck by 'ransomware', *Dawn,* September 10, 2020, https://www.dawn.com/news/1578882

[18] Summar Iqbal Babar, Muhammad Nadeem Mirza, and Irfan Hasnain Qaisrani. "Evaluating the Nature of Cyber Warfare between Pakistan and India." *Webology* 18, no. 6 (2021): 6973-6985. https://shs.hal.science/halshs-03788162/

[19] Anwesha Pathak, and Rohit Sharma. "Cyber Crime and Information Warfare-The New Arenas for WAR."

[20] Asma Bilal, (Lecturer at the Department of International Relations, National Defence University), email message to the author, September 13, 2021.

[21] Paul Bracken, "The cyber threat to nuclear stability." *Orbis* 60, no. 2 (2016): 188-203. https://doi.org/10.1016/j.orbis.2016.02.002

[22] Noreen Naseer, Muhammad Fahim Khan, and Aamer Raza. "A comparative view of India and Pakistan's defence capabilities: Historical evolution and future trends." *Asian Journal of Comparative Politics* 8, no. 1 (2023): 214-227. https://doi.org/10.1177/20578911221124384

[23] Saqib Khan, and Khalid Manzoor Butt. "Cyber Technology, Radicalization and Terrorism in Pakistan." *Journal of Indian Studies* 3, no. 2 (2017): 119-128. https://www.prdb.pk/uploads/publications/1539243517803.pdf

[24] Adam Saud, and Nehal Kazim. "Disinformation and Propaganda Tactics: Impact of Indian Information Warfare on Pakistan." *Journal of Indian Studies* 8, no. 2 (2022): 335-354. http://pu.edu.pk/images/journal/indianStudies/PDF/9_v8_2_22.pdf

[25] Pulkit Mohan, *Ensuring Cyber Security in India's Nuclear Systems*. Observer Research Foundation, 2020.

[26] Elizabeth White Baker, "A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan."

[27] Doreen Horschig, "Cyber-weapons in nuclear counter-proliferation." *Defense & Security Analysis* 36, no. 3 (2020): 352-371. https://doi.org/10.1080/14751798.2020.1790811

[28] E Dilipraj, "India's Cyber Security 2013: A Review."

[29] Nayef Al-Rodhan, Hypersonic Missiles and Global Security. *The Diplomat*. 2015, https://thediplomat.com/2015/11/hypersonic-missiles-and-global-security/

[30] Rachel Williams, Hypersonic Missile Technology Combined with Cyber Attacks on Nuclear Infrastructure Could Undermine Nuclear Stability. *College of International Studies.* 2021, https://www.ou.edu/cis/sponsored_programs/cyber-governance-and-policy-center/blog/hypersonic-missile-technology

[31] Anwesha Pathak, and Rohit Sharma. "Cyber Crime and Information Warfare-The New Arenas for WAR."

[32] Denial of Service (DoS) attack can be defined as a situation in which an authorized user is not able to access the resource. For example, send too many requests to a computer resource than it can handle, so that it will get crash or unresponsive.

[33] E Dilipraj, "India's Cyber Security 2013: A Review."

[34] News Desk, Bombshell data reveals sectarian trends on Pakistani social media originate from India, *Global Village Space*, 22 September 2020, https://www.globalvillagespace.com/sectarian-pakistan/

[35] Tushar Ranjan Mohanty, The unabated persecution of Hazara Shias in Pakistan. *League of India.* 2019, https://leagueofindia.com/india-world/the-unabated-persecution-of-hazara-shias-in-pakistan/

[36] Raashid Maqbool, Why the Indian state is now scared of the Kashmiri Shia. *Aljazeera*. 2020, https://www.aljazeera.com/opinions/2020/9/20/why-the-indian-state-is-now-scared-of-the-kashmiri-shia

[37] Arun Sukumar, and R. K. Sharma. "The Cyber Command: Upgrading India's National Security Architecture." *ORF Special Report* 9 (2016). https://orfonline.org/wp-content/uploads/2016/03/SR_9_Arun-Mohan-Sukumar-and-RK-sharma.pdf

[38] Muhammad Imad Ayub Khan, "Cyber-warfare: Implications for the national security of Pakistan." *NDU Journal* (2019): 117-132. http://111.68.99.125/website/ndu-journal/pub-new/06-Cyber-Warfare.pdf

[39] Prof Dr Umbreen Javaid, and Javeria Jahangir. "Balochistan: a key factor in global politics." *South Asian Studies* 30, no. 2 (2020). http://journals.pu.edu.pk/journals/index.php/IJSAS/article/view/3007

[40] Aditya Bharadwaj, Assessing India's Preparedness. *Wild Blue Yonder*. (2020). https://media.defense.gov/2020/Jul/21/2002460417/-1/-1/1/BHARADWAJ.PDF

[41] Shershah Nawabi, Taliban deny foreign interference claims by Iran; Pakistan rejects role in Panjshir capture. *Arab News*, (Sep 8, 2021). https://www.arabnews.com/node/1924781/world

[42] Shafek Koreshe, New Afghan government rubbishes claims of Pakistan's involvement in Panjshir. *Associated Press of Pakistan,* (Sep 6, 2021). https://www.app.com.pk/national/fake-news-indian-media-goes-berserk-shares-pix-of-downed-f-16-in-panjshir/

[43] Muhammad Imad Ayub Khan, "Cyber-warfare: Implications for the national security of Pakistan."

[44] Shahira S. Fahmy, "Media, terrorism, and society: Perspectives and trends in the digital age." *Mass Communication and Society* 20, no. 6 (2017): 735-739. https://www.tandfonline.com/doi/full/10.1080/15205436.2017.1382285; Also see Shabir Hussain, Farrukh Shahzad, and Adam Saud. "Analyzing the state of digital information warfare between India and Pakistan on Twittersphere." *SAGE Open* 11, no. 3 (2021): 21582440211031905

[45] Adam Saud, and Nehal Kazim. "Disinformation and Propaganda Tactics: Impacts of Indian Information Warfare on Pakistan." *Journal of Indian Studies* 8, no. 2 (2022): 335-354. http://pu.edu.pk/images/journal/indianStudies/PDF/9_v8_2_22.pdf

[46] MINISTRY OF INFORMATION TECHNOLOGY & TELECOMMUNICATION Government of Pakistan, *NATIONAL CYBER SECURITY POLICY 2021,* July 2021, https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf