3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare

Muhammad Nadeem Mirza[*]
and Muhammad Shahzad Akram[**]

Abstract

This qualitative exploratory and embedded case study deliberates the nature of 3-Cs of cyberspace — cybercrime, cyber terrorism, cyber warfare — against Pakistan. What is the nature of mentioned threats associated with cyberspace and how are they impacting the state and society in Pakistan. How Pakistan has been dealing with these threats related to its cyberspace. While taking cue from cyber realism – which provides the basic lens to conduct this research – this study notes that states and state-sponsored individuals, groups and organisations remain the main actors in the cyberspace who are active against each other. The perception that the cyberspace has diminished the role of state is an exaggeration. States still are the most important actors in the cyber world order animated by the typical great power politics. Pakistan remained a prime target of the cybercrimes, cyber-terrorism, and cyber warfare launched by the regional and extra-regional states. Though, it has implemented Prevention of Electronic Crime Act (PECA) and passed National Cyber Policy, yet it still has to go a long way in order to protect itself against the 3-Cs of the cyberspace.

Keyword: Cyber Crime, Cyber Terrorism, Cyber Warfare, Cyber Realism, Cyberspace, Pakistan.

Introduction

After land, air, sea, and space, cyberspace has emerged as the fifth domain of warfare.[1] Though information technology (IT) has brought about many

[*] *The author is faculty member at the School of Politics and International Relations, Quaid-i-Azam University, Islamabad. Email: mnadeemmirza@qau.edu.pk*
[**] *The author is MPhil scholar at the School of Politics and International Relations, Quaid-i-Azam University, Islamabad. Email: mshahzada22@gmail.com*

positive changes in the world, yet it is also posing some serious security threats to the individuals, states, and societies.[2] On one hand advancements in cyber technology and IT have made individual life easy and augmented state institutions' efficiency and performance because of the enhanced interconnectedness. On the other, it has opened a pandora box of vulnerabilities by posing threats to individual privacy and national security.[3]While the states have been relying more on the tools and activities transpiring in the outer-space in order to ensure successful, steady, and secure communication between different organisational structures — such as military commanders in the field and in the headquarters — the hackers may disrupt the communications, thus damaging states' capacity to even conduct the daily businesses. Similarly, advancements of the unmanned aerial and other combat vehicles,[4] automation of the war machinery, and reliance on C4ISR (command, control, communication, computers, intelligence, surveillance, and reconnaissance) have expanded the vulnerabilities of states that can be exploited by other states and non-state actors using the cyber-technological tools.

Pakistan's reliance on the cyberspace being a developing state has been increasing rapidly especially for the e-governance. UN Conference on Trade and Development's *Information Economy Report* ranked Pakistan at the ninth number in the world for its booming digital economy. As a comparison, India held the first position, China second, and Iran the seventh.[5] The report notes that more than half of Pakistan's internet users went online for the very first time in the last three years.[6] Moreover Pakistan Telecommunication Authority (PTA) notes that there

---

[1] Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin Press, 2019).

[2] Muhammad Nadeem Mirza, Lubna Abid Ali, and Irfan Hasnain Qaisrani, "Conceptualising Cyber Sovereignty and Information Security: China's Image Of A Global Cyber Order," *Webology,* Vol. 18, no. no. 5 (2021): 598-610.

[3] Mirza, Ali and Qaisrani.

[4] Muhammad Nadeem Mirza et al., "Unmanned Aerial Vehicles: A Revolution in the Making," *South Asian Studies* 31, no. 02 (December 2016): 625-38.

[5] FizzaAtique, "Pakistan Ranked 9th Globally for Its Booming Digital Economy-UN Reports," *Phone World Pakistan*, October 4, 2017, https://www.phoneworld.com.pk/pakistan-among-top-10-economies-in-terms-of-its-internet-users/.

[6] UNCTAD, *Information Economy Report: Digitalization, Trade and Development*, 2017 (United Nations Conference on Trade and Development, 2017).

are 113 million 3G/4G subscribers (with a penetration of 51.43%) and 116 million Broadband subscribers (with a penetration of 52.79%) in Pakistan.[7]

A Karachi based research company *Google* and Kantar's 2021 *Journey to Digital* report notes that 'one-third of all internet users in Pakistan made a purchase online.'[8] These figures, while giving hope for a digital revolution and opening new avenues of development in the technological and economic sectors, enhance the vulnerabilities of the individuals and state to cyber-attacks launched by hostile actors lying at different levels of the system, state, and society. The modest understanding of the cyberspace and hostile regional and international political environment further aggravate the situation.

Federal Investigation Agency (FIA) noted in 2021 that the cybercrimes — financial frauds, harassments, fake profiles, defamation, and hacking — have increased eighty-three per cent in the three years.[9] Social media provided the biggest platforms on which cyber-attacks were carried out. Moreover, the enhanced connectivity of the governmental institutions with the cyberspace, especially their opening of the social media accounts, aggravated the already precarious situation. This is akin to inviting the cyber-attacks categorised into 3-Cs cybercrime, cyber terrorism, and cyber warfare.

In order to counter the threats, Pakistan passed Prevention of Electronic Crimes Act, 2016, amended in 2022.[10] Similarly, in 2021 it passed its Natioanl Cyber Security Policy with the ultimate objective 'to establish governance and institutional framework for a secure cyber-

[7] PTA, "Telecom Indicators," Pakistan Telecommunication Authority, March 2022, https://www.pta.gov.pk/en/telecom-indicators.
[8] APP, "Country's Internet Penetration Stands at 54%," *Express Tribune*, July 30, 2021, sec. News, http://tribune.com.pk/story/2312994/countrys-internet-penetration-stands-at-54.
[9] Kasim Abbasi, "Cybercrime Increases by 83pc in Three Years," *News International*, August 28, 2021, https://www.thenews.com.pk/print/884453-cybercrime-increases-by-83pc-in-three-years.
[10] Pakistan Parliament, "Prevention of Electronic Crimes Act, 2016," (2016) https://na.gov.pk/uploads/documents/1470910659_707.pdf.

ecosystem.'[11] The need for the policy was felt after realisation that Pakistan remains the seventh worst cyber secure state in the world.[12]The policy declares that a cyber-attack against any institution of the state will be considered an act of aggression against the sovereignty of Pakistan. This policy delineated several important benchmarks, theoretically, for enhancing cyber security in Pakistan, but their effective implementation is questioned by the practitioners and scholars alike.

What are the 3-Cs of cyberspace and how are they impacting the statal and societal security? Whether the fluidity, flexibility, and openness of the cyberspace challenged the state's prized territorial dimension of sovereignty? This study while pursuing qualitative exploratory and embedded case study as research design, delineates the contours of cybercrime, cyber terrorism, and cyber warfare against Pakistan. Cyber realism provides the theoretical lens to conduct the research.

Cyberspace and Cyber Security

Norbert Wiener first coined the word cyber as a prefix in the title of his book *Cybernetics*, which he ascribed as the study of the control or communication in the animals and machines.[13] Cyber, increasingly, emerged as a prefix attached to the processes that involve Information Technology (IT), electronics, communication, virtual reality, computer networks, processors, and most importantly the internet. Cyberspace, for example, can be considered as an abstract space where flow of data transpires through communication infrastructures. The term was first coined by William Gibson in his short story *Burning Chrome* in 1982.[14] The idea further developed and now the US Department of Defense considers it as a

[11] MITT, "National Cyber Security Policy," (Ministry of Information Technology and Telecommunication, Government of Pakistan, July 2021), https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

[12] Global Strategies Index and the Global Security Index 2018 Report, quoted by Kalbe Ali, "Cabinet Gives the Green Light to Cyber Security Policy," *Dawn*, July 28, 2021, https://www.dawn.com/news/1637334

[13] Norbert Wiener, *Cybernetics: Or the Control and Communication in the Animal and the Machine* (Paris: Hermann & Cie Editeurs, 1948).

[14] William Gibson, *Burning Chrome* (Harper Voyager, 1982); William Gibson, *Neuromancer* (The Easton Press, 1984).

"global domain within the information environment consisting of the interdependent network of IT infrastructures and resident data, including the internet, telecommunications networks, computer systems and embedded processors and controllers."[15]

A related concept is the cyber security which refers to detecting, protecting and responding to any kind of cyber attack. Individuals or organisations mostly go for cyber security to restrict unauthorised accessing, changing, deleting, destroying or editing the data. It also refers to the set of precautionary measures, policies, approaches, guidelines and technological updates undertaken for data and information protection. IBM defines it as "the practice of protecting critical systems and sensitive information from digital attacks."[16] Important point to note remains that cyber security is not only limited to the protection of information but also of the critical infrastructure which is dependent on cyberspace. A well-planned cyber attack affects working, processing and decision-making of the computer systems which causes data loss, financial loss and security breaches.

Cyber Realism and Cyberspace

There exists a perception that 'in conflict-ridden times, realism has most often guided policymakers.' While 'during more peaceful periods, liberalism has more typically captured their imaginations.'[17]This assertion is challenged by realists on the ground that in peace and war alike their theory details the behaviour of states, with policy prescriptions to be followed in order to ensure national security and survival in a world lacking central authority. Rational and prudential considerations force states to pursue balance of power as the stable configuration of the international system animated by the rivalries and mistrust.[18] *Raison d'état* further enhances

[15] CRS, "Defense Primer: Cyberspace Operations," (Congressional Research Service, 1 December 2021), https://sgp.fas.org/crs/natsec/IF10537.pdf

[16] IBM, "What Is Cyber security?," International Business Machines Corporation, 2022, https://www.ibm.com/topics/cybersecurity.

[17] Charles W. Kegley and Gregory A. Raymond, "Realism in the Age of Cyber Warfare," *Ethics & International Affairs*, 26 April 2021, https://www.ethicsandinternationalaffairs.org/2021/realism-in-the-age-of-cyber-warfare/

[18] Muhammad Nadeem Mirza, "Enduring Legacy of Realism and the US Foreign Policy: Dynamics of Prudence, National Interest and Balance of Power," *Orient Research Journal of Social Sciences* 3, no. 2 (2018): 163-76.

states' positioning against the non-state actors, whom realists give relatively less importance, considering them a tool to enhance state's power and influence.[19] States' ultimate objective remains security and survival that can only be ensured by maximisation of power in every domain — hard, soft, sticky, sharp and smart powers.[20]

How do realists reconcile with the cyberspace, where individuals or groups adept with the cyber-technological tools can wreak havoc against others — individuals, institutions, or states — sitting anywhere in the world, anytime. Whether the basic conception of realism — state being the primary actor — has been challenged? Whether state's sovereignty — a prime feature of the Westphalian system — has been jeopardised because of the fluidity of the cyberspace? Whether the basic definition of the state being a 'territorial' unit has been threatened by the 'openness' and flexibility of the cyberspace? And most importantly whether realists' most prized concept of balance of power is still relevant in a world inhabited by hackers. Dmitri Alperovich while sensing the nature of the challenges posed by the cyber-domain notes that "cyberspace is not an isolated realm of its own, after all, but an extension of the broader geopolitical battlefield."[21] In geopolitics realism as a theory, deals with the challenges posed in cyberspace. Therefore, is not only relevant but required. Most of the individuals, groups, or organisations who have launched major cyber attacks against other states have largely been funded, sponsored, supported, or linked with some statal agency. In that case realism not only describes, explains and predicts the behaviour of the states, but also provides policy prescriptions — typical of the realist school of thought, such as (cyber) deterrence and (cyber) attacks.

Primacy of states, as dictated by the realists, remained visible through the Russo-Georgian and Russo-Ukrainian wars. These two wars also highlighted the importance of the cyber warfare in the times of peace as well as crisis. Russian cyber-attacks against Georgia played a critical role during the crisis. "By impeding the Georgian government's ability to react,

---

[19] Mirza.

[20] Joseph S. Nye Jr., "Think Again: Soft Power," *Foreign Policy*, 23 February 2006; Walter Russell Mead, "America's Sticky Power," *Foreign Policy*, 29 October 2009, http://foreignpolicy.com/2009/10/29/americas-sticky-power/

[21] Dmitri Alperovitch, "The Case for Cyber-Realism," *Foreign Affairs*, February 2022, https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism

respond, and communicate, the cyber-attacks created the time and space for Russia to shape the international narrative in the critical early days of the conflict."[22] Similarly, cyber-attacks between Russia and Ukraine remained a hot topic of discussion through most of the conflict period.

Moreover, cyberspace has seen a new rivalry and competition between great powers. While the US has been propagating a free and open cyberspace, China and Russia have been proposing the concept of cyber sovereignty, which denotes data localisation and extended control over the flow of information and internet users.[23] Besides China and Russia, several other states, including Pakistan, are pursuing these 'data localisation' and information protection strategies. China claims that, a free internet is akin to a US controlled cyberspace because of its technological superiority.

Realism, thus, in the cyber age remains as important as it was during and after the Cold War. History has also taught us an important lesson that the states which have not followed the realist dictates have faced the dire consequences. The United States (US), for instance, has parted way from some of the realist dictates in the immediate aftermath of the cold war.[24] It resulted in the blowback that damaged not only the American position in the international system but also resulted in the disastrous wars in different regions of the world.

Three Dimensional Threats to Pakistan in the Cyberspace: 3-Cs of Cyberspace

States' intervention to regulate the cyberspace, remains an uphill task because of its abstract nature. Russia presented a draft resolution in the United Nations (UN) in 1998 for the information security, but the movement remained sluggish because of the great power politics. This movement at the UN was strengthened by 2010 when the US co-sponsored

[22] Sarah P White, "Understanding Cyberwarfare: Lessons from Russia-Georgia War," (West Point, USA: Modern War Institute, 20 March 2018), https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf
[23] Mirza, Ali, and Qaisrani, "Conceptualising Cyber Sovereignty and Information Security."
[24] Mirza, "Enduring Legacy of Realism and the US Foreign Policy."

a similar resolution for cyber security.[25] Pakistan started taking cyber threats seriously when its first cyber related policy Electronic Transaction Ordinance (ETO) was presented in 2002. This ordinance was an attempt to regulate cyberspace and provide legal cover to online businesses.[26] Moreover, with the rapid increase in cybercrimes, government passed Prevention of Electronic Crime Ordinance (PECO) in 2007 and Prevention of Electronic Crimes Act (PECA) in 2016, which dealt with advanced cybercrimes, data theft, online frauds, forgery, cyber-harassment, and cyber-terrorism.

With the advancement of technology, cyberspace has emerged as a haven for saboteurs — both individuals and states. As early as 1993 Arquilla and Ronfeldt warned of an upcoming cyberwar.[27] Though the international system has not seen such a full-scale cyber-war, yet multi-national organisations, terrorists, criminals, hackers, and other state and non-state actors have remained engaged in cyber-attacks against their adversaries. In the realm of cyberspace, states, thus, are continually facing three-dimensional threats i.e. the 3-Cs of cyberspace — Cybercrime, Cyber terrorism and Cyber warfare.

Cybercrime

Cybercrime is related to the activities of individual hackers or groups, who carry out cyber attacks on government and private intuitions for personal financial gains. It, simply, is 'a crime related to technology, computers, and the internet.'[28] Pakistan's Federal Investigation Agency (FIA) has a separate setup to deal with the cybercrimes namely National Response Centre for Cyber Crime (NR3C). It defines a cybercrime as 'any activity commissioned via computer, digital devices and networks used in the cyber

[25] Christian Henderson, "The United Nations and the Regulation of Cyber-Security," in *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2015), 465–90, https://ideas.repec.org/h/elg/eechap/15436_22.html.
[26] Stephen E. Blythe, "Pakistan Goes Digital: The Electronic Transactions Ordinance as a Facilitator Growth for E-Commerce," *Journal of Islamic State Practices in International Law* 2 (2006): 5.
[27] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!' (RAND Corporation," 1993), https://www.rand.org/pubs/reprints/RP223.html.
[28] Bernadette H. Schell and Clemens Martin, *Cybercrime: A Reference Handbook* (Santa Barbara, Calif: ABC-CLIO, 2004).

realm, and is facilitated through the internet medium.'[29] Objective of such an activity — though remains mostly financial gains — may include theft of the data or money, cracking, cyber-bullying, cyber-harassment, cyber-stalking, cyber pornography, money laundering, piracy, and/or phreaking. Cyber criminals can lie at the domestic, regional or system levels. The tools which hackers use are mostly malicious codes and Trojan horses. Trojan horse, specifically, is the most effective means to not only destroy the software and computer system, but also transfer sensitive data back to the hackers. Pakistan has been facing high-level and low-level cyber-attacks which fall under the category of cybercrime.

Low-level cyber-attacks are carried out by domestic and international hackers. Many of these hackers are sponsored by hostile states like India. Many of them are criminals e.g., those, who hacked into Meezan Bank computer systems and stole the details of about 69,189 cards, and later put this information online for sale.[30] Similarly, some hackers threatened K-Electric administration to pay the ransom of about US$3.5 million. They threatened to sell the stolen data. K-Electric refused to heed their demands and even denied of any hacking. Resultantly the hackers leaked 8.5 GB of data about millions of users such as customer name, financial data, customer information (address, CNIC, bank account details), engineering reports, maintenance logs, unaudited profit and loss statements, engineering diagrams for turbines and the like.[31]

With the easy access to the internet and advanced gadgets, FIA notes that around 102,356 cybercrime complaints were filed in only one year (2021).[32] After verification of the complaints, 1202 cases were registered

[29] FIA, "Cyber Crime," National Response Centre For Cyber Crime (NR3C), Federal Investigation Agency (FIA), Government of Pakistan, 2022, https://nr3c.gov.pk/cybercrime.html.
[30] "Pakistani Banks Hit by Biggest Cyber Attack in Country's History – SAMAA," https://www.samaa.tv/news/2018/11/pakistani-banks-hit-by-biggest-cyber-attack-in-countrys-history/.
[31] Lawrence Abrams, "Hackers Leak Files Stolen in Pakistan's K-Electric Ransomware Attack," *Bleeping Computer*, 1 October 2020, https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/
[32] Azfar-ul-Ashfaque, "Cybercrime Complaints Topped 100,000 in 2021: FIA Chief," *Dawn*, 3 January 2022, https://www.dawn.com/news/1667248

under PECA and around 1300 arrests were made.[33] FIA further notes that the ratio of cybercrimes has increased by eighty-three per cent in over three years, with the financial frauds holding the top category.[34] Beside these reported crimes, number of the unreported cybercrimes can be very high, especially the ones dealing with harassment, bullying, blackmailing, damaging modesty of the natural person and hate speech. This is because of several reasons: First, individuals are not inclined to report the crimes considering those of minor nature, such as uploading someone else's pictures on social media without the explicit consent. Some individuals even do not know that this is a reprehensible cybercrime. Second, females facing harassment are again less inclined to report the crimes because of the societal pressures, and the fear that they will not be considered 'victims' but the ones who have invited the attacks by simply conversing with someone on the social media. Third, users of the cyber services may not even know the existence of the FIA Cyber Wing or NR3C where the complaints can be launched against the cybercrimes. In order to address these issues, Pakistan can launch awareness campaigns about the cyberspace in the society. Individuals should know their rights as well as responsibilities and it is the duty of the state to help them in this regard.

Cyber Terrorism

The US Department of State, now, considers it to be a "premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents."[35] This definition can be divided into several parts. First, Terrorism involves violence — that can be direct or indirect. Second, objective of the terrorists remains political. This part is what distinguish a terrorist from an ordinary criminal — who may pursue monetary or social objectives such as taking revenge. Third, violence is perpetrated against non-combatants.[36] This may not be the case in the contemporary environment. Terrorists now do not distinguish between combatants and non-combatants when targeting. Fourth, terrorists are

[33] Azfar-ul-Ashfaque.
[34] Abbasi, "Cybercrime Increases by 83pc in Three Years."
[35] Department of State, "Country Reports on Terrorism 2020," (Government of the United States, 2020), https://www.state.gov/reports/country-reports-on-terrorism-2020/
[36] Charles L. Ruby, "The Definition of Terrorism," *Analyses of Social Issues and Public Policy* 2, no. 1 (December 2002): 9-14, https://doi.org/10.1111/j.1530-2415.2002.00021.x

usually organised in groups which can be sub-national or can also be actors planning clandestinely to perpetrate violence — the lone wolf terrorists. It must be noted that the ultimate objective of the terrorists remains creating fear in the society. Causes of terrorism may range from psychological, religious, economic, social, ideological, to political motives.

Cyber terrorism refers to the use of computer, softwares, networks, data, and other cyber services for disrupting or damaging Information Communication Technology (ICT) infrastructures, creating fear in the state/society in order to achieve the political objectives. Veerasamy details six practices of the cyber terrorists: a) Denial of Service (DoS) attacks and Distributed Denial of Service attacks (DDoS); b) Web defacement which may include negative or derogatory comments against the government, political parties or other religious organisations; c) Misinformation campaigns; d) Theft or corruption of critical data-unauthorised access to sensitive information with the goal of accessing, stealing or destroying data; e) Exploitation of system vulnerabilities (to cause unavailability, loss of service, misrepresentation); f) Virus attacks which cause system failover, unavailability or disruption of services.'[37] Daniel Cohen, on the other hand, details three types of attacks carried out by the cyber-terrorists: 'an attack on the gateway of an organisation, mainly its Internet sites, through direct attacks, denial of service, or the defacement of websites; an attack on an organisation's information systems; and finally, the most sophisticated (and complex) category — attacks on an organisation's core operational systems for example, industrial control systems.'[38]

The cross-section of technology and terrorism has given rise to a precarious situation for states because subversive actors have made effective use of the cyberspace in order to carry out attacks against the critical infrastructures anonymously. Cyber terrorism is often considered as more lethal than the conventional terrorism. Reason being that the cyberspace has given an upper hand to the offensive attackers because of their anonymity

[37] Namosha Veerasamy, "Cyberterrorism – the Spectre That Is the Convergence of the Physical and Virtual Worlds," in *Emerging Cyber Threats and Cognitive Vulnerabilities*, ed. Vladlena Benson and John Mcalaney (Academic Press, 2020), 27-52, https://doi.org/10.1016/B978-0-12-816203-3.00002-2

[38] Daniel Cohen, "Cyber Terrorism: Case Studies," in *Cyber Crime and Cyber Terrorism Investigator's Handbook*, ed. Babak Akhgar, Andrew Staniforth, and Francesca Bosco (Syngress, 2014), 165–74, https://doi.org/10.1016/B978-0-12-800743-3.00013-X

and their exploiting the system's weaknesses. The situation is so dire that even one of the greatest technology giants like *Sony Entrainment*, or institutions of one of the greatest powers such as the US Office of the Personnel Management (US-OPM), could not protect themselves against the cyber attacks. Stealing sensitive data by exploiting the security loopholes or by attacking through different viruses, or DDoS attacks has become a routine matter now. Cripplingor sabotaging the entire systems of the institutions remains a hallmark of the cyber terrorists.

Cyberspace also provides an important medium to the terrorist groups to propagate, recruit, communicate, and plan terrorist attacks. In Pakistan terrorist organisations such as ISIS, Al-Qaeda, and Hijab-ul-Tahrir expand their radical agenda through the cyberspace, specifically through the social media. In 2015, Pakistan's agencies unearthed a group of well-off women in Karachi who had established an organisation named Al-Zikra Academy for preaching ISIS ideology, raising funds, providing financial help and matchmaking for the ISIS fighters.[39]Similarly agencies unearthed Bushra Cheema's network of recruitment for the ISIS from Lahore. She was an MPhil scholar and had also worked as honorary principal of the Noor-ul-Huda Islamic Centre. She left for Syria along with her children. Several other females and children, and even complete families — somehow connected with Bushra's network — left for Syria.[40] Important point here remains that most of these cases reported recruitment through the effective utilisation of the cyberspace and related technological tools.

Number of social media users in Pakistan has boomed in the last decade and most of the users are the young falling in the 15-35 years' age group. They are the easy targets of the terrorist influencers who manipulate them using religion as an important tool. Terrorist, extremist, and radical organisations have their social media handles on *Facebook*, *YouTube*, and

[39] AJ, "Pakistan Hunting for Network of Female ISIL Fundraisers," *Al Jazeera English*, December 22, 2015, https://www.aljazeera.com/news/2015/12/22/pakistan-hunting-for-network-of-female-isil-fundraisers.

[40] Umer Cheema, "20 Men, Women, Children from Lahore Join Daesh, Go to Syria," *News International*, December 31, 2015, https://www.thenews.com.pk/print/85370-20-men-women-children-from-Lahore-join-Daesh-go-to-Syria.

Twitter.[41] Hizbul-Islam and Jaish-e-Muhammad, for instance, use the social media platforms to expand their outreach and create attraction for the jihadists' life. Terrorist groups have also made use of cartoons for the children in order to expand their ideology and show the plight of Muslims in Palestine and other states.[42] *Twitter* and *Facebook* banned hundreds of thousands accounts for supporting the terrorist groups.

Pakistan has tried to rein in the online activities of several terrorist groups. For example, it banned Jaish-e-Muhammad and its online activities conducted mostly through Al-Qalam website and newspaper.[43] Despite bans, user fluidity and flexibility on social media provides extensive opportunities to the terrorists to re-emerge. In 2017, for example, it was reported that 41 out of the 64 banned terrorist organisations are operating thousands of pages, groups, and individual profiles on *Facebook*.[44]

Cyber Warfare

Cyber warfare involves coordinated attacks by one state or its institutions against another state or its ancillaries using the cyberspace, with the objective of causing damage and disruption. The acts may lead to the destruction of state's critical infrastructure, denial of the services (DoS), or creating chaos in the society by launching information operations. Rand Corporation considers that "cyber warfare involves the actions by a nation-state or international organisation to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."[45] US Department of Defence on the other hand considers it to be 'an armed conflict conducted in whole or part

[41] "US Designates Hizbul Mujahideen as a Foreign Terrorist Group – The Diplomat," https://thediplomat.com/2017/08/us-designates-hizbul-mujahideen-as-a-foreign-terrorist-group/

[42] Manasi Gopalakrishnan, "How Extremists Target Victims on Facebook and Twitter," *Deutsche Welle (DW)*, June 23, 2015, https://www.dw.com/en/how-extremists-target-victims-on-facebook-and-twitter/a-18535705

[43] FP, "In Face of Pakistan's Terror Ban Jaish-e-Mohammed Mouthpiece Al-Qalam Says Its Business as Usual," *First Post*, March 15, 2019, https://www.firstpost.com/india/in-face-of-pakistans-terror-ban-jaish-e-mohammed-mouthpiece-al-qalam-says-its-business-as-usual-6269191.html.

[44] Jahanzaib Haque and Omer Bashir, "Banned Outfits in Pakistan Operate Openly on Facebook," *Dawn*, May 26, 2017, https://www.dawn.com/news/1335561.

[45] "Cyber Warfare," RAND Corporation, 2022, https://www.rand.org/topics/cyber-warfare.html.

by cyber means … It includes cyber attack, cyber defence, and cyber enabling actions.' [46] Here the first definition considers states and international organisations as the main actors involved in the cyber warfare, the second considers it to be part of the military operations which can only be launched by the state and its (domestic) institutions.

Cyber espionage and thousands of low-level cyber attacks per day are a routine matter now for states. Cyber espionage relates to stealing sensitive data through digital means. Trojan horses are the most effective means available for the cyber espionage. Pegasus, for example, can infiltrate someone's smart phone through a simple missed call, an SMS, or even through simply a *WhatsApp* message. According to a *Washington Post* report, this virus developed by an Israeli organisation, has been bought by several states to spy on their own citizens and those belonging to other states. Several heads of state and government became a victim of this virus.[47] The report further noted that ten prime ministers, three presidents, and one king became targets of the Pegasus software including Pakistan's Imran Khan, France's Emanual Macron and Morocco's King Mohammad VI.[48] Besides, the list of the targets included "65 business executives, 85 human rights activists, 189 journalists and more than 600 politicians and government officials."[49] Interestingly, the list of the targets is still expanding along with the list of the clients who range from American intelligence agencies to other governments' institutions of more than forty states including that of India.[50]

China and the US have extensively engaged against each other in the cyber domain. The US, for example, alleges that China launched one of the

[46] Department of Defense, "DOD Cyberspace Glossary: Cyber Warfare," *PCMag,* 2022, https://www.pcmag.com/encyclopedia/term/dod-cyberspace-glossary.
[47] Craig Timberg et al., "On the List: Ten Prime Ministers, Three Presidents and a King," *Washington Post*, July 20, 2021, sec. World, https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.
[48] Timberg et al.
[49] Dana Priest and Elizabeth Dwoskin, "Chief of WhatsApp, Which Sued NSO over Alleged Hacking of Its Product, Disputes Firm's Denials on Scope of, Involvement in Spyware Operations," *Washington Post*, July 24, 2021, https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/.
[50] Timberg et al., "On the List."

major cyber attacks against its Department of Defence and Pentagon with the name *Titan Rain*.[51] Similarly, UK and Germany have also been accusing China of launching cyber attacks against their infrastructures, terming it a continuous problem.[52] Though China refused the accusations, yet the Americans blame that it is the individuals and organisations attached with the China's Peoples' Liberation Army (PLA) who are behind the attacks. Similarly, the Snowden Leaks revealed that the US accused China of launching *Byzantine Hades* attacks. As per the report, China remained successful in copying F-35 fighter jet designs. Besides it is also alleged that China remained successful in getting the designs of 'B-2 stealth bomber, the F-22 jet, space-based lasers, missile navigation and tracking systems, as well as nuclear submarine/anti-air missile designs.'[53]

It is not only the China which is being accused of cyber espionage. The US is one of the biggest cyber powers in the world who remained actively engaged in cyber espionage and cyber attacks against not only its adversaries but also allies. National Security Agency (NSA) of the US has specialised sections dedicated to spying, disrupting and destroying computer and related/attached infrastructures anywhere in the world. Its objective remains to strengthen already strong hold on the internet and monitor the flow of information.[54] NSA has a special unit named Tailored Access Operations (TAO) with the objective of 'getting the ungettable.' It is one of the most sophisticated units having the capacity to infiltrate anywhere in the world and launch cyber attacks, steal data, gather information, and perform any function as is demanded by the American intelligence agencies. It has conducted operations everywhere in the world. It was reported that the unit

[51] Richard Norton-Taylor, 'Titan Rain - How Chinese Hackers Targeted Whitehall', *Guardian*, September 5, 2007, sec. Technology, https://www.theguardian.com/technology/2007/sep/04/news.internet.
[52] Norton-Taylor.
[53] Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," *The Diplomat*, January 27, 2015, https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.
[54] Jacob Appelbaum et al., "NSA Preps American for Future Battle: New Snowden Docs Indicate Scope of NSA Preparations for Cyber Battle," *Der Spiegel*, January 17, 2015, sec. International, https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html.

launched operations in almost every state of the world. In 2010 only, it conducted around two hundred and seventy-nine operations worldwide.[55]

NSA also hacked Pakistan's National Telecommunication Corporation (NTC) using the SECONDDATE malware in order to spy upon the Green Line Communications used by its VIP civilian and military leadership. NSA used other viruses as well to spy on Pakistanis leadership.[56] Similarly, it is believed that an India sponsored Advanced Persistent Threat (APT) group, Confucius, deployed Hornbill and SunBird — two Android malwares — to spy on officials related with Pakistan military and nuclear infrastructure. Confucius has remained engaged in cyber-attacks throughout South Asia. Using different malwares, it extracted sensitive data such as SMS, geolocation, emails, and data even from the encrypted applications such as *WhatsApp* or *Blackberry* messenger.[57] Leyden notes that Indian capability, capacity and operations of cyber espionage have increased manifold in the recent years against Pakistan, China, and other South Asian, Middle Eastern and Southeast Asian states.[58]

Moreover, India is also using cyberspace to provoke anti-sate sentiments and launching cyber-attacks against Pakistan. In 2010, only Indian Cyber Army hacked around thirty-six Pakistan government websites,

---

[55] Staff, "The NSA Uses Powerful Toolbox in Effort to Spy on Global Networks," *Der Spiegel*, December 29, 2013, sec. International, https://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

[56] Geo, "US Hacked NTC to Spy on Pakistan Military, Political Leadership: Snowden Documents," *Geo News*, August 20, 2016, https://www.geo.tv/latest/112040-US-hacked-NTC-to-spy-on-Pakistan-military-political-leadership-Snowden-documents.

[57] News Release, "Lookout Unmasks State-Sponsored Android Spyware Tied to India-Pakistan Conflict," Lookout, February 11, 2021, https://www.lookout.com/news-release/lookout-unmasks-state-sponsored-android-spyware-tied-to-india-pakistan-conflict; Apurva Kumar and Kristin Del Rosso, 'Lookout Discovers Novel Confucius APT Android Spyware Linked to India-Pakistan Conflict', *Lookout*, February 10, 2021, https://www.lookout.com/blog/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict, https://www.lookout.com/blog/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict.

[58] John Leyden, "Indian Cyber-Espionage Activity Rising amid Growing Rivalry with China, Pakistan," *The Daily Swig: Cybersecurity News and Views*, June 30, 2021, https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan.

including those of Pakistan Navy, National Accountability Bureau, Ministry of Foreign Affairs, National Assembly of Pakistan, Government of Sindh, and the like.[59] Since then both statal and non-state actors in India have remained engaged in the cyber-attacks against Pakistan. For example, Pakistan alleges that Indian National Technical and Research Organisation (NTRO) and Defence Intelligence Agency (DIA) remained engaged in exploiting the cyberspace against Pakistan.[60] Moreover, Indians have been engaged in every effort to defame or create chaos in Pakistan. An example is the top trending hash tag on *Twitter* #Civil War in Pakistan after some political crisis in April 2021, with the objective to instigate anarchy in Pakistan.

Figure No.1

Source: Twitter (<https://twitter.com/1secalert/status/1383885933531983876>, <https://twitter.com/KhaleejMag/status/1383917914655313925>)

[59] Express, '36 Government Sites Hacked by "Indian Cyber Army," *Express Tribune*, 3 November 30, 2010, sec. News, http://tribune.com.pk/story/83967/36-government-websites-hacked-by-indian-cyber-army.

[60] Zaki Khalid, "Pakistan's Cyberspace Remains Victim to National Ignorance," *Centre for Strategic and Contemporary Research* (blog), September 10, 2020, https://cscr.pk/explore/themes/defense-security/pakistans-cyberspace-remains-victim-to-national-ignorance/

Conclusion

Cyberspace is rapidly contributing to the modern warfare. The development of technology has brought many positive changes and it poses some serious security threats as well. The 3-Cs of the cyberspace — cybercrime, cyber terrorism, and cyber warfare are posing serious threats to the states ─ being the primary actors as per the traditional as well as cyber realists. These threats affect individuals' privacy to states' national security. Individuals, groups, institutions, or states may launch cyber attacks against other states' critical infrastructures, through malwares, viruses, or other mediums. Stuxnet remains a typical example of the threats posed by states using cyberspace. It was used to target nuclear installations in Iran,[61] a precedent if pursued by other states could wreak havoc in the nuclear arena and nuclear-weapons states and ultimately the world.

Pakistan is one of the most vulnerable states facing cyber attacks in the form of cybercrimes, cyber terrorism (both sponsored by states and non-state actors), and cyber warfare. Western states and India remained the main state actors targeting Pakistan's cyberspace. India and Indians specifically have remained active in attacking the Pakistani cyberspace to disrupt, disable and destroy its computer systems and attached ancillaries. They have also remained very active in propagating fake information and trying to destabilise the state and society.

Though Pakistan through Prevention of Electronic Crimes Act (PECA) has tried to regulate its cyberspace against cybercrime and to some extent against cyber terrorism, yet its preparations against all the 3-Cs of cyberspace discussed in detail in the paper are still rudimentary. It really needs to develop its own capabilities to face the threats posed by all the possible cyber-related threats in order to protect its citizens and national interest, specifically in the domain of hate speech, propaganda, fake information, network and data security and critical infrastructures. Moreover, it needs to develop capacity and capability of different governmental institutions to help protect them against the cyber attacks in

[61] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon: Countdown to Zero Day," *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/; James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February 2011): 23-40, https://doi.org/10.1080/00396338.2011.555586

all forms. For that it may establish dedicated cyber wings (though of the smaller level) in every governmental institution and then ensure effective coordination between them through a centralised cyber institution that may coordinate all the activities transpiring in the Pakistani cyberspace and helping them prepare against all the cyber related attacks. Furthermore, Pakistan needs not only develop cyber defence capabilities but also focus upon developing cyber offensive capabilities. By developing such capabilities, Pakistan may be in a position to develop deterrence in the cyberspace. At the societal level, Pakistan needs to develop an effective mechanism to launch awareness campaigns in order to sensitise the population about the threats posed by the 3-Cs of cyberspace.