Challenges of Securitising Cyberspace in Pakistan

Aamna Rafiq*

Abstract

With the rapid developments in the cyberspace domain, Pakistan has emerged as one of the fastest growing digital economies in the world. Pakistan's internet penetration and teledensity are increasing exponentially, resulting in greater global connectivity. However, this connectivity has become a tool and target of conflict, crime and crisis which varies with respect to nature, occurrence and power. Pakistan is exposed to multidimensional cyber threats like computer malware, identity theft, economic data theft, cyber frauds and espionage attempts on critical infrastructures. However, the state institutions are ineffective to formulate a comprehensive national cybersecurity framework to counter these threats. This paper provides an in-depth analysis of the nature and severity of these cyber threats to the national security of Pakistan. It identifies the incorrect media framing of cybersecurity initiatives, the absence of relevant institutions, wide scope security debates, traditional security culture and non-inclusion of the audience as the major challenges to the successful securitisation of cyberspace in Pakistan.

Keywords: Cyberspace, Pakistan, Challenges, Securitisation Theory, Cyber Threats, Cybersecurity

Introduction

According to Jason Andress and Steve Winterfeld, cyberspace is a "notional environment" or "global domain" that consists of independent networks of information technology infrastructure including telecom networks, computers, internet, controllers and embedded processors to collect,

**The author is Research Associate at the Institute of Strategic Studies Islamabad. This research paper is extracted from the author's M. Phil dissertation (2017) titled "Securitisation of Cyber threats in Pakistan: Challenges and Prospects" submitted at School of Politics and International Relations (SPIR), Quaid-i-Azam University (QAU), Islamabad.*

analyse, modify, transmit, store and secure the information.[1] It was originally designed to enhance communication and connectivity. However, the ever-increasing human dependency on cyberspace and destructive technological innovations have transformed the cyberspace into an arena where information technology and data are being used as the tools as well as the target of warfare for causing instability, destruction of critical infrastructure and espionage. For Pakistan, cyberspace has become a criminalised and militarised zone, posing threats to its national security.[2] Pakistan is exposed to extensive cyber threats ranging from computer malware, identity theft, financial data theft, cyber frauds, surveillance on critical infrastructure and critical infrastructure information. Pakistan cannot ensure comprehensive national security without effectively coping with these threats.

In this context, the objective of this paper is to highlight the nature of cyber threats to the national security of Pakistan. It also identifies the standards, patterns and attitudes within the national security culture, which are hindering the successful securitisation of cyber threats in Pakistan. It also aims to suggest the requisite changes to resolve the challenges. The paper focuses on following research questions; What are the cyber threats to the national security of Pakistan? How Pakistan's security culture is posing challenges to the securitisation of cyberspace?

Cybersecurity is relatively a new domain of research in Pakistan due to which limited literature is available. The literature review is organised in theoretical to case-study order. In their article "Digital Disaster, Cyber Security and the Copenhagen School,"[3] Lene Hansen and Helen Nissenbaum analyse the emergence of cybersecurity as a concept in the wake of the shifting geopolitical dynamics and technological revolution of the post-Cold War period through the lens of the securitisation theory; they also applied this theoretical framework on the 2007 cyber-attacks in Estonia. In their book, *Cyber War: The Next Threat to National Security and What to Do*

[1] Jason Andress and Steve Winterfeld, "What is Cyber Warfare," in *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham, Massachusetts: Elsevier, 2014), 3-5.

[2] Solange Ghernaouti, "Cyber Conflicts, Cyberwars and Cyber Power," in *Cyber Power: Crime, Conflict and Security in Cyberspace* (Lausanne, Switzerland: EPFL Press, 2013), 176.

[3] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School," *International Studies Quarterly* 53 (2009): 1155-1175.

About It,[4] Richard A Clarke and Robert K Knake provide a thought-provoking comparison between cyberspace and Pakistan. They have developed an analogy between cyberspace and tribal areas of Pakistan while deliberating on the anarchical nature of cyberspace. Furthermore, their narrative compares the nature and severity of cyber threats with the drone attacks in Pakistan. A comprehensive legal analysis on cyberspace of Pakistan is provided by Khalil-ur-Rehman Khan in "Cyber Laws in Pakistan."[5] His legal opinion gives an all-encompassing appraisal of the inevitability of the formation of a legal framework to regulate and secure individuals, institutions and the state of Pakistan in cyberspace. He further raises some of the critical questions on the absence of cyber-specific legal framework and also forecasts the possible problematic scenarios. He also analyses the compatibility of cyber laws in general and the Prevention of Electronic Crime Act (PECA), 2016 in particular. Reviewing the cyberspace of Pakistan, through the lens of the securitisation theory, provides an entirely different and modern perspective as compared to the traditional realist school of thought which dominates the security discourse in Pakistan. The paper is divided into three sections i.e., Theoretical framework, followed by cybersecurity in Pakistan and challenges of the cyber securitisation in Pakistan.

Theoretical Framework

According to Barry Buzan and Ole Wæver, securitisation is "a discursive process through which an inter-subjective understanding is constructed within a political community to treat something like an existential threat to a valued referent object and to enable a call for the urgent and exceptional measures to deal with the threat."[6] In an eclectic conceptualisation of security, anything that has sufficient significance to possess a legitimate right of survival is called the referent object. The spectrum of referent object is extensive, well-defined and all-inclusive ranging from an individual to all humanity. Yet, the actual scale and legitimacy of an object are established

[4] Richard A Clarke and Robert K Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins Publishers, 2010).
[5] Khalil-ur-Rehman Khan, "Cyber Laws in Pakistan," Supreme Court of Pakistan, http://supremecourt.gov.pk/ijc/articles/10/1.pdf.
[6] Barry Buzan and Ole Wæver, *Regions and Powers the Structure of International Security* (New York: Cambridge University Press, 2003), 491.

by the success of speech acts and facilitating conditions, which in turn determine the required allocation and mobilisation of resources.

As securitising actor refers to an individual or group who securitises an issue through speech act, they are government, bureaucracy, pressure groups and political dignitaries. An asymmetrical relation among several actors makes the identification of a securitising actor a complex process. Segregation cannot be done especially when the actors are strongly embedded into authoritative roles assigned to them as representatives of collectivities. The difference between an object and an actor is not intrinsic but contextual. It is further complicated by their existence at multiple levels of analysis in a single point of time. The process of securitisation can be studied at five levels: i.) International system; ii.) International sub-systems; iii.) Units; iv.) Sub-units and v.) Individuals. According to Buzan, Wæver and Japp de Wilde, these levels are the "ontological referents" rather than an explanation in themselves. Michel Foucault called them the "sites of judgment." The securitisation theory effectively defines the discourses, social and technical interactions by providing an easy transition among the objects, actors and sectors.[7] With respect to the concept of security, a sector is a lens used to study the particular characteristic of an interaction. Again, as stated by Buzan, Wæver and Wilde:

> …the military sector is about relationships of forceful coercion; the political sector is about relationships of authority, governing status and recognition; the economic sector is about relationships of trade, production and finance; the societal sector is about relationships of collective identity and the environmental sector is about relationships between human activity and the planetary biosphere.[8]

In International Relations, an issue must possess a set of attributes to qualify as a security issue. In the discourse of the securitisation theory, it is known as "an essential quality of security." The theory defines security as a quest for survival. Thus, the essential quality of security is an "existential threat" to the survival of the referent object. The course of determining the essential quality of security is not the process of assessing the reality of existential threats rather it is the process of understanding the practical usage and representation of the concept. An act of presenting an apolitical issue as

[7] Barry Buzan, Ole Wæver and Japp de Wilde, *Security: A New Framework for Analysis* (London: Lynne Rienner Publishers, Inc. 1998), 34-39 and 5 -7.
[8] Ibid., 27-29.

an existential threat to the specific referent object by the securitising actor is called a “securitisation move.” On the securitisation spectrum, the non-politicised is a stage where an issue has not yet become an integral part of public policy. Next comes the politicisation stage, at which an issue is admitted as a subject of a state policy, which necessitates a contribution by the government in the form of political debate, decision-making, legislation, institutionalisation and resource allocation. Securitisation is a stage where an issue is placed above politics. However, the position of an issue varies on this spectrum. The securitisation move can finish off at any stage of the spectrum.

The securitisation theory adopts a subjective approach to security. The securitising actor securitises an issue according to its own threat perception and threshold. In one political community, the successful and legitimate securitisation may appear insignificant in another community. Thus, it is crucial to understand the dynamics of units and sub-systems at an international level and sub-units within a unit. The three fundamental elements of successful securitisation are existential threats; i.) Emergency measures; ii.) Chain reactions on inter-unit relations and iii.) Already existing securitisation. However, the study of partially successful and failed moves are as important as the study of the successful cases, since they provide considerable information about the formation-process of standards, security patterns and social attitude required for determination of the security legitimacy. It also suggests the required change and direction of future discourse and practice on a particular issue.[9]

Cybersecurity in Pakistan

Pakistan’s digital economy is globally ranked ninth by the UN. In 2005, Pakistan’s internet penetration was 6.3 per cent. With the increased access to the 3G and 4G technologies, the internet penetration rate increased up to 17.8 per cent in 2016.[10] During three years from 2012 to 2015, an increase of 16 million internet users was recorded for Pakistan. These first-time

[9] Ibid., 23- 30.

[10] “Internet Penetration Rate in Pakistan from 2005 to 2016,” Statista, https://www.statista.com/statistics/765487/internet-penetration-rate-pakistan/

entrants are 47 per cent of internet users in 2018.[11] According to Pakistan Telecommunication Authority (PTA), the cellular internet penetration rate is 25.32 per cent with 51 million subscribers. The broadband penetration rate is 26.46 per cent with 54 million subscribers. The teledensity in Pakistan is 72.90 per cent with 148 million cellular subscriptions. Currently, Pakistan is ranked tenth globally with respect to unique increasing mobile subscriptions.[12] The mobile penetration in Pakistan is 39 per cent of the total population. By 2025, it is expected to reach 50 per cent and Pakistan, together with nine other countries, will form 60 per cent of the global subscriber market.[13]

With such great existing and increasing use of information and communication technologies in Pakistan, cyberspace has emerged as a new security domain. Pakistan is undertaking new initiatives to achieve an all-inclusive national cybersecurity framework. The most significant achievement is the PECA 2016.[14] This law ensures protection against the unauthorised access, interference, interception and transmission of critical data and information system. It also deals with the cyberterrorism, online glorification of offence, hate speech, electronic fraud, identity theft, cyberstalking, spamming, spoofing, offences against the dignity and modesty of natural person especially minor. In 2017, Pakistan was ranked 67th among 193 states in the Global Cybersecurity Index (GCI) by the International Telecommunications Union (ITU). According to the GCI, Pakistan is lagging behind in the areas of technical and organisational measures.[15]

[11] "Information Economy Report 2017: Digitalisation, Trade and Development," United Nations Conference on Trade and Development (UNCTAD), October 2, 2017, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

[12] "Telecom Indicators," Pakistan Telecommunication Authority, last updated February 2018, http://pta.gov.pk/en/telecom-indicators

[13] "The Mobile Economy 2018," GSM Association, February 2018, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/2/The-Mobile-Economy-Global-2018.pdf

[14] Government of Pakistan, *Prevention of Electronic Crimes Act, 2016*, August 19, 2016, http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

[15] "Global Cybersecurity Index (GCI) 2017," International Telecommunication Union, last modified October 5, 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

In 2017, the concentration of malware hosting sites in Pakistan was one of the highest in the world (15 - 20 malware hosting sites per 1,000 hosts). The world's second highest malware encounter rate was recorded for Pakistan at 27.48 per cent in the first quarter of 2017.[16] According to the Microsoft Malware Infection Index for the Asia Pacific Region 2016, Pakistan is the topmost country vulnerable to the malware infection in the Asia Pacific markets. Indonesia, Bangladesh, Nepal and Vietnam ranked second, third, fourth and fifth respectively. India is placed at the eighth position.[17] Pakistan is vulnerable to the malware like Gamarue, Skeeya and Peals, which can install other malware and steal all the personal information from the infected computer system. The second and third biggest cyber threats are the Distributed Denial of Services (DDoS) attack and identity theft respectively.[18] The banking sector of Pakistan has been a major victim of cybersecurity breaches in 2018, resulting in serious financial losses. The personal data of more than 8,000 accounts of the Pakistani banks is available on the Dark Web.[19]

In the "Cold Start Doctrine," India has integrated "cyber warfare" along with the biological, nuclear, chemical, conventional and sub-conventional warfare. It involves various tools and techniques to compromise, destroy and degrade the computer systems at tactical, operational and strategic levels. Furthermore, it also aims to destroy the critical information passed and stored in computer systems used for the nuclear Command and Control (C2).[20] In the Joint Doctrine Indian Armed Forces 2017, India included cyber warfare as an essential component of the "Hybrid or Fifth Generation Warfare." This doctrine declared cyberspace as a new domain of future war.

[16] "Microsoft Security Intelligence Report (January – March 2017, Volume 22)," Microsoft, August 17, 2017, https://www.microsoft.com/en-sa/security/Intelligence-report

[17] "Microsoft Malware Infection Index for Asia Pacific," Microsoft Asia, https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/#sm.0001c8j2ld213dupxw82ps93k6pbp

[18] Ibid.

[19] "Almost all Pakistani Banks Hacked in Security Breach, says FIA Cybercrime Head," *Dawn*, November 6, 2018, https://www.dawn.com/news/1443970.

[20] Government of India, Integrated Defence Staff, *Indian Army Doctrine 2004,* October 4, 2004, http://ids.nic.in/indian%20army%20doctrine/indianarmydoctrine_1.doc

Challenges of Securitising Cyberspace

Role of the Audience

By describing the securitisation process as an inter-subjective agreement, a substantial significance is assigned to the role of the audience which, in Pakistan, are citizens. The absence of resonance between the citizens of Pakistan and national cybersecurity narrative is the biggest challenge. Presenting something like an existential threat to the cybersecurity of citizens does not necessarily result in securitisation. The securitising actors or the credible voices of the cybersecurity have to argue the case in front of the citizens for a resolute acceptance, which generates a resonance between citizens and national cybersecurity narrative.[21] When it comes to the securitisation of cyberspace in Pakistan, the audience is largely oversimplified due to the inability of constructing a balance between the securitisation process in cyberspace as a speech act of a government and as an intersubjective process. At one particular point of a process, securitisation is an inter-subjective agreement but, at the other points, it became a speech act. The political and security institutions of Pakistan have to comprehend the necessity of reconciling these two points. In Pakistan, cyber issues are being considered as a speech act and are dealt with the traditional approach, which has a highly formal and conventional set of rules and procedures. This completely negates the inter-subjective component of the process, which in turn generates a crisis of legitimacy for the initiatives to regulate cyberspace.

Media Framing

In the last decade, electronic media emerged as one of the key power brokers and played a substantial role in the social construction of security threats in Pakistan. The media can bring to light the psychological, economic, social, cultural and political setting in which cyber securitisations are introduced. Furthermore, the media is a platform through which the audience can react towards these securitisations. With respect to the cybersecurity dynamics in Pakistan, the media becomes a part of the audience when one uses the phrase "effects in media." However, "effects of media" makes it a crucial functional actor with the ability either to play

[21] Buzan, Wæver and Wilde, *Security*, 25-30.

down or amplify the cyber securitisation moves. This is a point wherein lies the challenge. Instead of highlighting the growing existential cyber threats, the media could compel the audience to focus more on human rights violations and excessive investigative powers instead of positive protective measures.

Cyberspace is relatively a new realm of security about which the audience has limited knowledge. A securitising actor or government of Pakistan can use media framing to create a desired and suitable context by activating the positive aspects of cybersecurity initiatives. By sending credible voices, they should utilise this platform to achieve the support of the political opposition, neutral actors and human rights organisations.

Establishment of Relevant Institutions

According to securitisation theory, security culture of the state has its specific dynamics and boundaries which decide what can be securitised. A major problem arises when the newly discovered cyber threats become controversial with respect to their state of emergency, which play a crucial role in the establishment of new relevant institutions. In Pakistan, the entire cyberspace has been securitised at a general level in such a way that any cybersecurity issue automatically moves to the already securitised area of terrorism. This has compelled cybersecurity to operate in the absence of relevant institutions or under the domination of the institutions established as a result of other types of securitisations. The National Response Centre for Cyber Crimes (NRC3) was established as a result of the Electronic Crimes Ordinance in 2007 and 2008 to deal with cyber threats. However, instead of giving it the status of an independent agency, it was turned into a specialised branch under Federal Investigation Agency (FIA).

Under the PECA 2016, extensive powers have been given to the investigative officer who is authorised to access, check, use, preserve, acquire, search, seize, copy and demand data whether content or traffic which may be necessary to carry out an investigation. Moreover, he is empowered to call any person for the purpose of investigation whether charged or containing encrypted information and can demand the decryption of that information.[22] However, the issue of a relevant institution

[22] The Prevention of Electronic Crimes Act, 2016, section 36 and 32.

has not been resolved. Presently, there is a heated debate among the state officials regarding the new cybersecurity agency to be established or which law enforcement agency should be authorised to work on the matter. Keeping in view the extensive powers, the Senate Standing Committee on Information Technology is sceptical about the expertise and capacity of the FIA.

In addition to the FIA, another institution under consideration is the National Counter Terrorism Agency (NACTA).[23] The Prime Minister's office has constituted an Inter-Ministerial Committee to design and finalise the structure of the organisation in addition to rules and regulations for the operationalisation of the PECA 2016. The establishment of a Cyber Emergency Response Team (CERT) and the nomination of special courts for the prosecution of cyber offences are also pending.[24] The future of cyber securitisation will be designed by the finalisation of these matters and the extent up to which the designated organisation and court will exercise their powers. Keeping in mind the security culture of Pakistan, the securitisation of cyberspace likely become institutional when a sense of urgency is created by the persistence reappearance of cyber threats.

Securitisation on the Behalf of State vs Nation

In certain securitisations, one securitising actor is being more privileged (the acting side) while marginalising the actual/real judges of acts. In the case of state securitisations, this problem is less evident since the state has well-defined rules and hierarchies about who can speech act on its behalf. Additionally, there is no problem of legitimacy. However, this is a major fault line for the cyber securitisations in Pakistan. Cyber securitisations are done on behalf of the state instead of the nation. If one is doing a speech act on behalf of the nation then its rules will be more flexible as compared to the state. The speech act for the nation is based on the logic of identity and values. For example in Pakistan, the securitisation of terrorism is done on the behalf of the Pakistani nation. The securitising actor here was the state that successfully changed the common narrative of the US "War on Terror

[23] Tahir Amin, "Electronic Cyber Crime Bill 2016: Senate Body against Giving Unbridled Powers to FIA Officials," *Business Recorder*, July 22, 2016.
[24] Ministry of Information, Broadcasting and Heritage, Press Information Department, PR No. 61 First Meeting of IMC for PECA 2016 Rules Held at MOIT Islamabad, September 8, 2016.

(WoT)" to "Pakistan's war on terror," ending the whole confusion that divided the nation. Both the government and military establishment achieved inter-subjective agreement on almost all the excessive countermeasures for the eradication of terrorism in various parts of the country. As a result of this national consensus, violations of certain fundamental human rights became acceptable to counter the menace of terrorism as soon as possible; for example the establishment of temporary military courts, an additional Directorate of Internal Security under the command of NACTA, Federal and Provincial Rapid Response Force, special anti-terrorism courts and military operations. Hence, the prospects of cyber securitisation will be promising if carried out on behalf of the nation rather than the state.

Synthesis before Segregation

The securitisation theory proposed an analytical method that consists of segregating the "complex whole" into different sectors e.g. military, societal, economic, environmental and political in order to identify particular patterns of interaction since all these sectors lack the "distinctive quality of independent existence." The core objective of this segregation is to reduce the number of involved variables.[25] In Pakistan, the challenge is the broad scope of the cyber securitisation where securitising actors are trying to deal with the great number of variables at the same time. They are trying to introduce single securitisation to deal with cyber threats in all sectors ranging from basic cyber threats of malware attack and identity theft to much complex cyber threats to national critical infrastructure. They are defining the scope more broadly and making the process of securitisation more complex instead of manageable, clear and simple. The securitising actors are synthesising the sectors in cyberspace before even segregating them. They have failed to identify the specific patterns of relationships, subjects and objects that shape the entire threat-survival matrix which is operating in cyberspace of Pakistan.

Conclusion

There are substantial existential cyber threats to Pakistan's national security and without the securitisation of these threats, the all-inclusive national

[25] Buzan, Wæver and Wilde, *Security*, 7-8.

security is unachievable. In the last decade, governments initiated various securitisation moves but failed to accomplish success. The incorrect media framing of cybersecurity initiatives, the absence of relevant institutions, wide scope security debates, traditional security culture and non-inclusion of the audience are the major challenges to the successful securitisation of cyberspace in Pakistan. The platform of electronic media and credible voices of cybersecurity could help achieve the inter-subjective agreement among the relevant stakeholders. The reconciliation of this inter-subjective agreement with the speech acts would resolve the issues related to the role of the audience. Furthermore, it is important to identify the patterns of relationships, securitising actors and objects in military, economic, political and social sectors that design the threat-survival matrix operating in cyberspace. The issues of cybersecurity should be approached with a modern and flexible set of rules instead of rigid and traditional rules of the existing security culture.