# ARCHITECTURE OF CYBERSPACE AS AN EVOLVING SECURITY PARADIGM IN SOUTH ASIA: PAKISTAN-INDIA CYBER SECURITY STRATEGY

**MUHAMMAD BAQIR MALIK***

## Abstract

*This paper aims to develop a preliminary hypothesis for the South Asian region to identify the relationship between technology and national security. The paper studies the evolving trends of technology that have changed the security paradigm. To manage the security risk in a complex and dynamic digital environment, a new set of strategy and thinking is needed both in Pakistan and India to complement the traditional security approaches. Cybernetics realism is the proposed theoretical model for national security in South Asia in the age of cyber technology. The paper is divided into three sections. The first section discusses the theoretical framework of this evolving security paradigm, which examines the working mechanism of cybernetics realism in South Asia as a strategic power. The second section discusses the challenges of the new security paradigm to Pakistan and India and their policies to counter these challenges. The third section tests the proposed hypothesis, i.e., whether cyberspace is evolving as a security paradigm in South Asia. The paper ends with a conclusion and some recommendations.*

* Mr Muhammad Baqir Malik is a PhD candidate and doing research at the Massachusetts Institute of Technology (MIT), Massachusetts, United States.

*Regional Studies, 36:2, Spring-Summer 2018, pp.3-35.*

# سائبر سپیس کا قومی سلامتی نظریے کے طور پر ارتقاء اور پاکستان اور بھارت کی سائبر سلامتی حکمت عملی

محمد باقر ملک

## خلاصہ

اس مقالے کا مقصد جنوبی ایشیا کے لئے ٹیکنالوجی اور قومی سلامتی کے مابین تعلق کی شناخت کے لئے ایک ابتدائی نظریہ پیش کرنا ہے۔ مقالہ ٹیکنالوجی کے ارتقائی عمل کے تناظر میں بدلتے ہوئے سلامتی نظریے کا احاطہ کرتا ہے۔ ایک پیچیدہ اور متحرک ڈیجیٹل ماحول میں سلامتی کے خطرات کا تدارک کرنے کے لئے پاکستان اور بھارت کو روایتی سلامتی کے نقطہ نظر کو تقویت دینے کے لئے ایک نئی حکمت عملی اور سوچ کی ضرورت ہے۔ 'سائبر نیٹکس رینلزم' سائبر ٹیکنالوجی کے دور میں جنوبی ایشیا میں قومی سلامتی کیلئے تجویز کردہ ایک نیا نظریاتی خاکہ ہے۔ یہ مقالہ تین حصوں میں تقسیم ہے۔ پہلا حصہ اس ارتقاء پذیر سلامتی کے نظریے کے نظریاتی فریم ورک پر تبادلہ خیال کرتا ہے اور جنوبی ایشیا میں سائبر نیٹکس رینلزم کے عمل کو ایک تزویراتی طاقت کے طور پر جانچتا ہے۔ دوسرا حصہ پاکستان اور بھارت کو اس نئے سیکورٹی نظریے کی دشواریوں اور اُن دشواریوں سے نمٹنے کیلئے تیاری پر تبادلہ خیال کرتا ہے۔ تیسرا حصہ تجویز کردہ نظریے کو جانچتا ہے کہ آیا سائبر سپیس جنوبی ایشیا میں سلامتی نظریے کے طور پر ابھر رہا ہے۔ مقالہ ایک اختتامیے اور کچھ سفارشات پر ختم ہوتا ہے۔

The end of the Cold War changed the concept of security from traditional to non-traditional around the globe.[1] During the Cold War period, the traditional school of thought was dominating world politics. The collapse of the Soviet Union shifted this concept from traditional security to non-traditional security issues. The result was that human security, social security, environmental security, health security, etc. became the top agenda items in the post-Cold War period.[2] Currently, the concept of digital security is added to the traditional and non-traditional concepts of security. The main reasons for this are the popularity of the internet and global dependency on technologies. Cyberspace has become a hot cake in world politics of the twenty-first century. This shifting in the security paradigm is also being felt in South Asia, which has a mostly deprived and poor population of 1.7 billion, partly because of the huge defence spending of the South Asian countries.[3] The strategic location of this region gives it a special importance in world politics. Generally, when people talk about the South Asia region, it means issues pertaining to Pakistan and India.[4]

The twenty-first century is an age of globalisation and the driving force behind this globalisation is the internet. Developments in information and communication technologies are diffusing globally at an impressive speed.[5] In this digital realm, cyberspace is rapidly converting into a new conflict zone around the globe. Information Technology (IT) is playing an important role in this conversion. South Asia, sooner or later, will be engulfed in conflicts revolving around this emerging zone. It is very important for Pakistan and India to work to secure cyberspace before it becomes a new political conflict zone in the region. Both states must change their attitudes towards bringing stability to the region. Karl Deutch states, "'security community' may not be just around the corner in South Asia, the region could be more peaceful, stable and secure if the countries bring about changes in their attitudes."[6]

This paper examines this new dimension of warfare and its implications for the South Asian security paradigm. The paper is divided into two parts. The first part of the paper is the explanation of the South Asian security through a conceptual framework. It discusses how cybernetics realism works in ways similar to other theories of security studies. The second part discusses the digital space as an evolving new security paradigm between Pakistan and India. The paper ends with a conclusion and some recommendations.

## Cybernetics Realism Theory

In the security discourse, an issue is dramatised and presented as an issue of supreme priority. By labelling it as security, an agent claims a need for and a right to treat it by extraordinary means. The securitisation approach serves to underline the responsibility of actors as well as analysts who choose to frame an issue as a security issue. They cannot hide behind the claim that anything in itself constitutes a security issue.[7]

South Asia is one of the most debatable areas in world politics.[8] The foremost reason behind this debate is the hostility between the two nuclear powers in the region, i.e., Pakistan and India. Several scholars around the globe have worked on issues related to South Asia.[9] The works of these scholars help in understanding the traditional and nuclear security environment. Some of the existing theoretical paradigms could be helpful in understanding the nature of the security environment in this region. However, there are gaps in the existing body of literature on these issues related to cyberspace and digital security. This makes it quite difficult to clearly understand the digital threats and the importance of cyberspace in South Asia. In the twenty-first century, when cyberspace has become the most important tool in world politics, it is very difficult to explain cyberspace within the existing theoretical debate. There is a need to create a separate debate to understand the nature, threat, and the challenge of

cyberspace. The following discussion is an attempt to explore the theoretical understanding of cyberspace in the context of South Asia.

For this reason, I have coined and developed the theoretical concept of 'cybernetics realism'.[10] This is an attempt to explore the security environment of cyberspace. Cybernetics realism is a combination of three terms.[11] The word 'cyber' is usually used for the virtual medium, which is the application of computer and computer-related technology.[12] 'Netics' represents the physical infrastructure of technology, and 'realism' defines the attitude for accepting the situation as it is and preparing to deal with it accordingly.[13] In political science, realism is a framework to understand and practice global politics. It emphasises the nation state's policy to protect its national interest.[14] Cybernetics realism can be described as "the construction of global and dynamic domain, which is characterised by a combination of physical infrastructures and telecommunication devices that allow for the connection of technological and communication system networks to transfer the borderless information from one place to another without any hierarchical principle and its relationship with national security."[15] The communication systems broadly refer to the computer network system.

The term cybernetics was used for the first time by Plato as "the study of self-governance."[16] Norbert Wiener defined cybernetics in 1948 as, "the scientific study of control and communication of the system with machine."[17] Another early pioneer of this term was Lois Couffignal, who described the term as "the art of securing efficient operation."[18] In short, cybernetics realism can be defined as, "The art to establish the computer network system and to control the communication system of computer network and to use this network to protect the national interest by the use of cyberspace domain."[19] Cybernetics realism involves the following main features:[20]

1. Exploitation of cyberspace for military purposes by the states;

2. The defining point of a computer network, which has changed security paradigms from means to ends;[21]
3. Importance of a virtual medium for states in the contemporary security environment;
4. The relationship between a communication network and national security; and
5. The use of a computer network system in a crisis and in the power competition of states.

Why cybernetics realism is important in South Asia and will it work in the current security environment scenario? In the twenty-first century, cyberspace has emerged as a new political zone. This domain has changed the security environment around the globe. These trends of changing the security environment can also be observed in South Asia. With more and more users active in cyberspace, security issues are increasing. Pakistan and India are the main actors in this region. The stability and security of this region depend on the relations of both states. This region has already faced three wars.[22] Studying India-Pakistan politics gives an idea that the military objectives are always on top of the policy agenda.[23]

In the age of information technology, cyberspace is also developing as a conflict zone between Pakistan and India. One of the basic reasons is that after their nuclear tests, both states want to avoid any conventional conflict because it could escalate into a nuclear war. To avoid any physical clash and gaining the military objective, the virtual medium becomes the best alternative option for Pakistan and India. To explain this evolving security paradigm, cybernetics realism is applied to the current security environment for the following reasons:

First, the internet has become the most important medium for spreading ideology, funding, recruiting, planning, operating, training, meeting, and many more activities. The internet provides an easy means to interact and coordinate with each other without crossing the security check posts of any state. Pakistan and India both have

suspected each other historically. The internet provides an ideal opportunity for both states to carry out their activities without the knowledge of the other. In this context, the internet is providing a platform to achieve strategic goals. The nuclear and missile arms race clearly indicates that the balance of power is measured in terms of their military capability. On the internet, the equation of power is undecided.

Second, in the age of cyber technology, the most important use of cyberspace is for propaganda. This will become more important when states are facing some ideological, cultural, and military clashes. Since Pakistan and India have such clashes passed on from generation to generation, the importance of cyberspace for propaganda increases. Propaganda is always considered a very important tool in military strategy.[24] Many strategists believe that 50 percent of war can be won by using effective propaganda strategy.[25] This is very helpful to demoralise the military and people without fighting. According to the famous military strategist Sun Tzu, "The best weapons are that which enemy does not know." In the present situation, cyber weapons fall in this category. Cyber weapons can be easily hidden and remain unidentified. Historically, this is an accepted reality that propaganda changes the equation of war. In the age of cyber technology, this propaganda tool becomes very important for individual states.[26] It can be utilised more effectively and efficiently through the use of cyberspace. Cyber technologies are very easy to use in any form against adversaries. Pakistan and India are not enjoying good relations since their independence. This hostility not only exists between governments, but sentiments of hatred are also found among the people. Cyber technology is providing an opportunity to exploit the emotions of the people.

Third, social media have emerged as amongst the most influential propaganda tools in the twenty-first century. Social media penetrate into the minds of people and influence with very fast speed.

This increases the importance of cyberspace in military strategy. Social media in Pakistan and India are quite popular. The youth and professionals are quite active on social media. In both states, social media websites are mostly used to share pictures, jokes, religious material, political post, etc. Social media is a space where anyone can post anything without any investigation. The role of social media becomes very crucial when states are avoiding any physical confrontation, but they are not ready to minimise tension.

Fourth, social media always has space for new actors to use the campaign against the military and other institutions. There are many examples in Pakistan and India where social media play an important role during conflicts. For example, in Pakistan, during the Abbottabad operation against Osama Bin Laden, military operations in the tribal areas of Pakistan, military operations in Swat district of the Khyber Pakhtunkhwa (KP) province of the country, Lal Masjid Operation in Islamabad, and many others incidents, a malicious campaign was started against Pakistan's political leadership and military forces.[27] This has not only demoralised the security forces but could also possibly tarnish their image in front of the people. This was the reason that the people of Pakistan were confused about the use of force against militant groups.

Fifth, in 2014, the Pashtun Tahafuz Movement started from the Federally Administrated Tribal Areas (FATA), KP, and Balochistan in Pakistan.[28] The initial purpose of this movement was to protect the rights of the Pashtuns who were affected by various military operations in Waziristan and its surrounding areas. They demanded clearing of landmines and a stop to the killing of innocent people and to clearly distinguish between the Taliban and Pashtuns. The movement received attention in Pakistan after Naqeebullah Mashud was killed in Karachi.[29] Several Pakistanis supported the demands of PTM. This was also an open space for India and Afghanistan. They were operating different fake social accounts and posting material against

Pakistani forces. According to an ISPR press conference, almost 5,000 fake email IDs and Facebook accounts were operated from Afghanistan, where the only purpose was to defame the security forces.[30] This kind of activity has created a distance between the people and the security forces of the country. On another hand, however, the same social media exposed the PTM when some anti-state and anti-forces slogans were used.[31] This shows the importance of the role of cyberspace, especially in the region where terrorist and separatist movements are prominent.

Sixth, Pakistan and India are both increasing their nuclear capability and improving their missile technologies. In the age of information technology, both states are modernising their systems.[32] The digital technology can be used in the nuclear command, control, and communication systems. In this regard, there are a number of ways that these systems can be under threat. For example, malicious computer code may penetrate into a nuclear weapon system, exploiting design vulnerabilities and system failures. Cyber-attack concerns may include digital spoofing and jamming, which may create problems in communication, data manipulation, etc. This could lead to greater uncertainty in decision making and accuracy of weapons. Cyber technology in peacetime and wartime (crisis) can be used with different approaches. For instance, in peacetime, the states do not know that their nuclear weapons are under a cyber-attack. This is an example of offensive cyber activities. This unknown situation has serious implications for military decisions, particularly pertaining to the weapon deterrence policy. In the case of wartime or heightened tension situations, cyber-attacks on nuclear weapons could bring escalation. This could increase the probability of a launch of a nuclear weapon within one's own territory due to false information and target set through the use of cyber technology.

To conclude, the cybernetics realism theory is the most suitable approach to explain the evolving security paradigm in South

Asia. The following reasons could be given for the assertion:

1. States are continuously maximising their military power and in the age of technology. The military is getting more modernised and strategy getting more dependent on technology. Thus, technology is becoming an important tool in military doctrines to expand influence in the region without investing much and avoiding any physical clashes.
2. There is no economic competition in the region. Therefore, cyber technology is used to reap maximum economic benefits, so that liberalism, interdepended approach or other approaches of international relations fail to address the evolving security paradigms.
3. South Asian states are facing some common problems. For example, border issues, terrorism, extremism, separatist movements, and security issues. In this context, the role of cyber technology becomes very important in exploiting situations to achieve strategic objectives.
4. Hostile relations and spy policies are important agenda items of many states in this region. The use of cyber technology makes it easy to achieve goals without any physical confrontation.
5. This is the age of globalisation and states are avoiding going to war. But, at the same time, they are continuously using interference policies in different forms. The flexible nature of cyber technology and internet are providing the best opportunity to use different interference policies for their strategic purpose.
6. Nuclear weapons have become a major reason for security and stability in the region. Deterrence usually works between two nuclear states. States having nuclear weapons do not easily go to war with each other for the fear of it escalating into a nuclear conflict. In this context, cyber technology can be used for military purposes. The purpose of technology is not the same as nuclear technology, but it could be used for monitoring, damaging, or

destroying code. Such an act could open the zone for a physical war. Cyber technology is becoming a very important phenomenon in this region and in the new paradigm this technology determines the chance of war and the power of the state.

## The Challenge of the Evolving Security Paradigm in South Asia: Pakistan and India Security Strategy

Pakistan and India have fought three major wars. The major outcome of these wars was the loss of precious human lives.[33] IT has evolved in the mid of 1990s in this region[34] but at the time no one could have predicted that one day this technology will become a serious problem in South Asia. The history of the digital war in South Asia can be traced back to May 1998, when India tested nuclear weapons.[35] Soon after these tests, some unknown hackers penetrated into the Indian Nuclear Research Centre.[36] Indian computer security experts admitted that hackers broke the Bhabha Nuclear Research Centre site. They claimed that the hackers were from Pakistan.[37] This was the first reported incident of the beginning of a cyber war in South Asia. Although this incident did not bring any serious harm to the Nuclear Research Centre, it dismantled its communication system.[38] The next section will further discuss the challenge of cyberspace both for India and Pakistan and their approaches.

### Indian Cyber Security Strategy

India is one of the fastest growing countries in the IT sector.[39] This growing capacity and dependency on IT is becoming a challenging task for the Indian government to secure its cyber domain. Following are India's main challenges in cyberspace:[40]

1. India is a leading information technology exporter. This has created a challenge for its data security and privacy. This challenge is defined as cyberspace design.
2. Legal and technical data security standards and security issues between low-end and high-end smartphones have exposed

millions of citizens to cyber hackers. This is known as cyberspace density.

3. India is importing its digital equipment and these are tampered, which increases the vulnerability of critical Indian sectors. This needs market regulation and safety processes.
4. Another most important challenge for India is the transition of its economy into a digital economy[41] and growing Chinese cyber capability and its engagement in cyberspace.[42]

Indian security officials started working on cybersecurity strategy in 1998.[43] Indian security experts, with telecommunication experts, held several meetings for drafting the cybersecurity strategy.[44] In August 2010, the Indian government decided to form a cyber wing in their military institutions.[45] The purpose of this cyber wing was to defend against any digital attacks from any side of the world. A procedure was drafted on 29 August 2010, led by the Indian National Security Advisor Shiv Shankar Menon. It went on to be approved by the high ranking officers of the Indian Intelligence Bureau (IB) and additionally the senior authorities of the telecom section, IT service, and RAW.[46]

After three years, India released its National Cyber Security Policy on 2 July 2013.[47] The main features of this policy were as follows:

1. A National and sectoral mechanism by the name of National Critical Information Infrastructure Protection Centre (NCIIPC) was established to deal with cyber threats.
2. India formed a Computer Emergency Response Team to deal with any cyber crisis. This centre was established to coordinate and operate with different sectors and to act as an umbrella organisation for cybersecurity matters.
3. A system was proposed for obtaining strategic information regarding threats to Information and Communication Technology (ICT) infrastructure. This system was proposed for prevention, response, and recovery action.

4. For the next year, more than five hundred thousand professional computer experts were scheduled to partake in different government and private organisations.
5. The policy emphasises strong relations and cooperation between public and private organisations to address the cyber threat.
6. The Indian army's cyber command wing is to be established and cybersecurity defence is to be improved.

This policy was drafted around the following three main principles:

1. Digitalise India to boost citizens' connectivity;
2. Establish digital delivery systems in government departments; and
3. Ensure the security of personal and government data.

To achieve the objective of this policy in a broader sense, it is very important for India to create a secure cyberspace environment and to work to strengthen the regulatory system.[48] For this purpose, the target was to train 500,000 professionals and to establish a separate cyber army command unit. The timeline for this target was 5 years. According to the latest reports, a total of 10 percent of skilled people are inducted and trained.[49] However, India not only established the cyber army command but also modernised its army to deal with cyberspace issues. Interestingly, the Indian cyberspace approach is to go from regional to global level. This is the reason it is investing intensively in its space program.[50] Moreover, India is also improving coordination between the government and private companies. The following three main organisations are working to fill this gap:

1. Information Systems Audit and Control Association (ISACA),
2. The National Association of Software and Services Companies (NASSCOM); and
3. The Data Security Council of India (DSCI).[51]

**Indian Cyber Security Policy: Theory to Practice**

India is setting up its own Cyber Operation Centre. This is jointly run by the National Technical Research Organisation (NTRO)

and the armed forces. Following are India's major cybersecurity implementation projects:[52]

1. National Cyber Coordination Centre (NCCC) is working against hackers and espionage to track terrorist activity online. The structure of this centre is akin to the functioning of cyber centres in the US, UK, France, and Germany. Cyber intelligence sharing is also in its mandate.
2. The Botnet Cleaning and Malware Analysis Centre is tasked with removal and limiting of the threat due to botnets. India has the largest number of botnets in the world. Therefore, Botnet Cleaning and Malware Analysis Centre aims to provide safety and security in cyberspace.
3. Central Monitoring System (CMS) is used to monitor phone calls, text messages, and social media.
4. The NCIIPC is created under the technical intelligence agency, the NTRO. The NTRO is responsible for providing cover to 'critical information infrastructure'. Its functions are to roll out counter-measures in cooperation with other security agencies.

The release of cybersecurity policy in 2013 and all other steps adopted by the Indian government are considered important breakthroughs in South Asian security paradigm. This also indicates that new cyberspace is entering a new political and strategic zone in this region.[53] Previously, traditional and non-traditional security issues created disturbance in South Asia. This new medium will possibly have implications similar to other mediums of war in the past. Indian cyber security policy was the first step towards cyberspace as a new political zone in South Asia, but cyberspace zone is borderless. Identification of problems and dominant position of the attacker in cyberspace without attribution is a challenge. In traditional security approaches, the defenders enjoy the deterrence, retaliation, early warning, balance of power, etc. In cyberspace, the offence is easier than defence.

## Pakistan's Challenge with regard to Cyberspace and its Cyber Security Strategy

In the 21st century, the issue of cybersecurity is becoming alarming for all states. Cyberspace has created an equal challenge whether the state is developed or less developed. Pakistan is also facing the same challenge for its digital security. India has already declared its cyber strategy doctrine in 2013. The Indian cyber doctrine provides insights into understanding its strategy of countering the digital threat—the use of cyberspace to protect its national interest and maintain hegemonic power. A low-intensity cyber conflict has started between Pakistan and India.[54] The policymakers are convinced that Pakistan is less dependent on technology and cyberspace is not a serious problem for Pakistan.[55] But the emerging challenges of cyberspace are developing day-by-day. This section discusses the major challenges of cyberspace for Pakistan and analyses Pakistan's approach towards cyberspace.

First, the challenge is the psychological impact of cyberspace and its importance for Pakistan. Psychological warfare is one of the leading tools in modern warfare.[56] This involves the application of specialised information and media. The combination of media and information is used in accordance with the situation. This can be used to achieve a strategic goal or achieve political and military objectives.

The working principle of psychological war depends on the following three factors:

1. Collection of information;
2. The ability to degrade this information; and
3. Transmission of this information as per desire.[57]

The challenge for Pakistan is to manage cyberspace. Pakistan is not only facing this challenge regionally but also globally. Regionally, India is the major challenge for Pakistan. India is using all of its resources to demoralise Pakistani forces and create a distance between the people of Pakistan and its security forces. Cyberspace

creates an opportunity to spread disinformation against Pakistan. India and its allies understand the importance of the psychological war on cyberspace. This is the reason India and some major powers are investing huge amounts of resources on cyberspace against Pakistan.

The second challenge is the war on terror and the role of cyberspace. In the global war on terror, Pakistan became the frontline state. The common perception about Pakistani security agencies has changed. Cyberspace has played an important role to build perception. Hate literature, fake audios and videos, and fake statements are creating challenges for Pakistani security agencies. There are many situations where cyberspace was used against Pakistan with proper campaigning.[58] Interestingly, whenever there is political unrest in Pakistan, the first impression of the public is that the military is behind it.

The third and most important challenge for Pakistan is the recent defence agreement between India and Israel.[59] It should also be noted that Israel was the first state in the world to create a digital army.[60] The concept of the digital army is not only indicating the use of digital technologies but also provides the mechanism of coordination between different departments to share the information. The reason for creation of a digital army is to monitor adversary states. The Indian cyber strategy is similar to Israeli cyber strategy. The Indian cyber doctrine is not only aimed at setting up a digital army but also at the use of the digital mechanism inside and outside the geographic boundary. In 2015, India launched its Digital Army Programme (DAP). For this purpose, the Israeli experience in building and running a robust DAP can give the required push to India's Digital Army initiative.[61]

Israel became a close partner of India in establishing its cyber force. This was discussed in the recent visit of Indian Prime Minister Narendra Modi in Israel. As per the agreement, both states have used more than 300 cybersecurity startups. This has approximately $6.5

billion of cyber product exports. This shows that Israel has become a cyber-security powerhouse and the best option for India. In a joint statement issued during Prime Minister Modi's Israel visit, both sides asserted their desire to institutionalise cooperation on cyber issues through a joint framework. And as Isaac Ben-Israel, Chairman of the ISA and National R&D Council and head of the Cyber Research Centre at Tel Aviv University has said, "We have developed a lot of Technology but there is just not enough of a market. India has a huge market and there is a lot of potential for cooperation between the two countries."[62]

The fourth challenge is the US Personal Record Information System Methodology (PRISM) programme, which was disclosed by Edward Snowden in June 2013.[63] According to documents leaked by Edward Snowden, Pakistan is included as one of the most targeted countries in the world for US espionage. The National Security Agency (NSA) is using the internet as a spy medium against Pakistani civilians, military, private, and nongovernmental organisations. Snowden disclosed that more than 12.5 billion emails were being monitored by the US.[64] This data is collected from different social websites, for instance, Google, Skype, Facebook, Twitter, YouTube, and several others. Other classified documents proved that the NSA program is not only targeting military officers but also politicians. This surveillance strategy is also used to eavesdrop on the Pakistan nuclear program.

## Pakistan's Way Forward for Developing a Cyber Security Strategy

In response to cyber espionage or detection of intruders, Pakistan is not prepared to show an effective response. A serious appreciation of this threat is missing among the policy circles of Pakistan and they appear unable to establish a defence shield against it. It is not only neglected in civilian government but the military itself ignores the dangers of cyber threats. The major reason behind this negligence is that the entire government system of Pakistan is not

digitised. Therefore, it is believed that there is no need to establish any cyber command force.

There was a slight shift of policy on cyberspace post-Snowden revelations. In this regard, on 8 July 2013, the first-ever meeting for a cyber-secure Pakistan was arranged in the parliament. It was chaired by Senator Mushahid Hussain along with senior military officers and the head of the Pakistan Information Security Associations (PISA). In this meeting, the national cybersecurity policy was discussed in detail. Interestingly, the participants of the meeting did not include computer security experts. They were viewing it as a policy problem rather than a technical one. However, they concluded that Pakistan needed a proper cyber strategy to handle cyber threats.[65]

On 11 July 2013, a seminar was held at the Pakistan Institute of Parliamentary Services (PIPS), Islamabad. In his welcome address, the Chairman of the Senate's Standing Committee on Defence said, "Given the security threat posed by snooping and spying by the US through their secret agencies like CIA and NSA, especially of Pakistan which is the second highest in their list of countries being spied online, funds should be allocated in the budget for a Cyber Security Strategy since Pakistan is a victim of cyber warfare and cyber aggression. This should be entrusted to a Cyber Security task force, specially constituted for the purpose that can propose countermeasures. Its Secretariat should be in the Ministry of IT."[66] In this seminar, a seven-point agenda was also provided, which declared that 2014 will be celebrated as a cyber-secure Pakistan.

The Cyber Security Bill was approved from both houses after a three-year gap. This also gives an idea of how Pakistani politicians are looking into the dangers of cyberspace. The main points of this bill are as follows:

1. Pakistan must induct computer professional in various sensitive organisations.
2. The administration will use secure internet services.

3. A computer emergency response team will be established to counter this threat.
4. National Computer Crimes Centre will be made more effective.
5. Coordination among private, governmental, and security organisation should be made possible.
6. A separate office will be established for cybersecurity matters, which will work under different ministries.
7. Pakistan will raise this issue on the forum of SAARC to formulate a cooperative strategy to secure South Asia and make this zone as free from cyber-attack.[67]

If we analyse all these developments regarding Pakistan's policy on cyberspace, there is no clear strategy. Recently, some steps have been taken, which indicate the seriousness of Pakistani policy makers towards cyber policy. On 21 May 2018, Pakistan opened its first cyber centre in Air University.[68] There are three main agenda items for creating this cybersecurity centre: protect the digital economy, protect sensitive data, and secure cyberspace. The federal minister in the inaugural session stated, "We made the National Action Plan (NAP) and launched a full-fledged operation against terrorists in the country, which will continue till complete annihilation of terrorists and extremists."[69] This cyber centre will work in collaboration with different research institutions and universities.[70] Cybersecurity encompasses technologies, processes, and controls that are designed to protect systems, networks, and data from cyber-attacks. The former National Security Adviser Nasser Khan Janjua said that cyber attacks posed an enormous threat to the national economy, defence, and security. One week prior to the inauguration of the cyber centre, the Pakistan National Counter Terrorism Centre also established its separate wing of cyber security to counter digital terrorism.

## Is the Security Paradigm Evolving in South Asia?

Cyberspace has emerged as a new political zone around the globe. This is the reason several states have taken this zone very

seriously, including revisiting their security policies. So, is cyberspace the evolving security paradigm in South Asia? Whenever there is some change around the globe, its impacts are seen in South Asia. Both Pakistan and India have changed their policy according to the global environment. As cyberspace is emerging as a new political and security zone, this is also evolving as the new security zone in South Asia.

How can one say that cyberspace is an evolving security paradigm in South Asia? It is an accepted reality that this region changes its security policy according to global scenarios. Here are some chosen historical facts: First, Pakistan and India gained their independence during the Cold War period. This was the period when the realist school of thought was dominant in world politics.[71] Military power was considered the most important factor in world politics. Military power was defined as the equation of power in world politics.[72] Pakistan and India also followed the same policy in this region. Economically and politically, both states were not in a stable position. They used most of their budget for gaining military power. Pakistan and India signed the agreement to fulfil their military requirement. Economic matters were not important in their policy. The US became the strategic partner of Pakistan and the Soviet Union signed a strategic agreement with India.

Second, from 1945 to 1960, there were only two declared nuclear powers, i.e., the Soviet Union and the US. But when the trend of nuclearisation started around the globe, China, France, and the United Kingdom also joined this nuclear coalition. Nuclear weapons became the reason to shift the military paradigm form conventional weapons to nuclear weapons. South Asia was not kept isolated from the influence of this nuclear race. In South Asia, India tested its nuclear weapons in 1974.[73] Although India claimed that its nuclear program was only for peaceful purposes, the Indian nuclear tests shifted the equation of power in the region. As a reaction, Pakistan also started its

nuclear program. For Pakistan, this was a question of survival because Pakistan was dismembered in 1971 with Indian intervention. Pakistan was economically weak, politically unable, and the tragedy of separation of Bangladesh was a blow to national pride and integration. Therefore, Pakistan started its nuclear program. The famous statement of Zulfiqar Ali Bhutto, "We eat grass but Pakistan will make a nuclear bomb,"[74] shows the passion to counter the Indian nuclear threat.

Third, missile technology and its role in world politics also influenced South Asia. Both Pakistan and India started their missile programme in the late 1970s. The missile competition between Pakistan and India moved from conventional missile technology to nuclear to intercontinental to laser-guided missile technology.[75] The missile race modernised as the other states were devolving their missile technology. Pakistan and India both are following the international regime and their policies are the reflection of the global strategic and political environment. Both states are reacting according to the global environment.

The beginning of 1990s brought many new things in the world politics. The long Cold War period ended with the disintegration of the Soviet Union. America became the sole superpower in world politics and a wave of globalisation ensued. The Internet was considered a public domain and started gaining popularity with the introduction of different search engines and internet tools. Technological advancement started improving and economic policies became an important core in foreign policy agenda. There was also shifting of alliances from strategic to economic. These changes could also be observed in South Asia. Importantly, the end of the Cold War was also a serious challenge for India. Therefore, India shifted its policy to build strong relations with both China and America. Indian policy became more focused on economic relations with China and strategic relations with the US. Pakistan also improved its economic relations with China, America, and the Muslim world. Pakistan also gave importance to the

newly created Central Asian states in its foreign policy. As the world was becoming more concerned with economic issues, South Asia was also following similar approaches.

In May 1998, there was a dramatic shift in South Asian security environment.[76] India conducted five more nuclear tests. This shifted the equation of power in the region. The Indian nuclear tests created a serious challenge for Pakistan's security and stability. The public media, and security establishment was on one page to give a strong response to the Indian nuclear test. In response, therefore, Pakistan also conducted six nuclear tests. Soon after nuclear tests, the Kargil war started, but the conflict was resolved with the involvement of major powers. It is because the international community realised that if there was any escalation between Pakistan and India, it could go nuclear, introducing a global nuclear threat.

The 21st century witnessed a new wave of security challenges.[77] The Global War on Terror (GWOT) began against terrorist and their affiliated organisations. In the first phase, Afghanistan was the first country to face US military action. Al-Qaeda Chief Osama Bin Laden was in Afghanistan and America considered him the mastermind of 9/11[78]. Owing to this war, South Asia once again got special attention in world politics. This has become challenging for India and Pakistan to play their cards wisely to protect their national interests.[79]

This is the era when many social websites were introduced. After 9/11, many social networking sites such as Facebook, Twitter, YouTube, Hangout, Skype, Instagram, etc. become very popular to communicate and share views. These social websites brought a revolution not only in technology but, at times, in politics as well. State and non-state actors are all active on the internet. This transformed cyberspace as the new zone in world politics. Pakistan and Indian are both using the social media against each other. Now, direct physical confrontation is not necessary. Effective use of social media can help you achieve your goals. In Pakistan, the recent phenomenon of the

Pashtun Tahafuz Movement (PTM) is a sign of the power of this media. According to Pakistan's military spokesman, more than 5,000 accounts are operated from India and Afghanistan to support the PTM.[80] Similarly, when anti-state slogans were raised in a PTM procession, someone posted them online and people realised that it was not a movement for Pashtun protection but was against Pakistan and its forces.[81] This lost support for it inside Pakistan. In political activities, this medium has more influence and changes voter mindset. Pakistan and India are facing a security challenge from each other on the use of cyberspace. Tension is increasing day-by-day. The foregoing supports the claim that social media has evolved as a security paradigm in South Asia.

## Conclusion

The popularity of the internet and the use of social media with advanced technologies have unquestionably added to the challenges of state security. Cyberspace changed the nature of conflict and the nature of interests. It provides an equal opportunity to small or powerful states, as well as non-state actors, to conduct their activities relatively freely. The primary issue with digital threats is that they are still unrecognised as potential risks. Furthermore, resolving national policy challenges is not straightforward in today's globalised world. Moving towards digital security issues in South Asia in the age of technology, clear distinctions must be made between the politics of threat and the politics of protection. No doubt, both approaches are interconnected with each other, however, both politics of threat and politics of protection concern agenda-setting, cooperation, and conflicts of interest.

The intensity of cyber-attacks between Pakistan and India is increasing day-by-day, which indicates that in future, this low-intensity war can possibly convert into a major conflict. The active engagement of India in cyberspace demonstrates how this zone is evolving as a security paradigm in South Asia. Interestingly, India is not considering

Pakistan as a competitor in cyberspace. The Indian cyber strategy and cyber alliance politics indicate that India is the dominant actor in cyberspace. The challenge of cyberspace is creating problems for all South Asian states. Pakistan must concentrate on an effective national cybersecurity policy. Pakistan has made some progress in formulating national cybersecurity, but there is still a long way to go. One thing Islamabad should understand and accept is that cyberspace has emerged as a new political and security zone. Instead of thinking about Pakistan as a less technology-dependent state, it needs to realise the use of cyberspace and its increasing impact on daily lives. In the 21st century, states cannot separate or isolate themselves from the international community. The fast-moving trends of technology are compelling states to fully utilise its application. A positive sign is that Pakistan is moving to create a proper cybersecurity strategy. It has established the National Cyber Security Centre and Research Program. The creation of the institution itself is not important, but the induction of professional people is. Without technical knowledge, it is very difficult to formulate a proper cybersecurity strategy as per the need of the time. On the other hand, India has declared some parts of its cybersecurity doctrine and is using cyber alliance politics. India has started different research programs in various fields, especially in artificial intelligence. These steps from Pakistan and India indicate that both the countries understand the evolving security paradigms in this region. But the architecture of this new paradigm depends on the resources of cyberspace. This also imposes a multifaceted problem and must be dealt with separately, as both states have previously dealt only with the conventional security threat. However, the road to this new security paradigm is still hazy.

The following conclusions may be drawn from the use of digital technology:

1. Technology could be utilised for the benefit of people.
2. Some legal mechanisms should be adopted in cyberspace to curb

cyber terror and South Asian states must be legally bound to cooperate with each other.

3. To counter this new threat, information/computer security expertise from all states must be shared.
4. It is time to understand the challenge of digital security as a global problem, not only as a regional one. Moreover, all states have to come forward to cooperate with each other to make the cyberspace a zone free of war, so that all states can enjoy equal rights to explore new horizons for the betterment of the people in this region.
5. There is a need to have a mutual agreement to solve the cyber threat issues and to stop the non-state actors in the space.

It is very important to take practical actions to implement these steps so that new security environments stabilise the region, and cyberspace does not become a new zone of conflict. South Asian states, especially Pakistan and India, must understand the challenges of this evolving security paradigm. Both states should resolve their conflict with mutual understanding because tomorrow's keyboard could be more dangerous than a bomb.

## Notes and References


1 Harvey M. Sapolsky, Eugene Gholz, and Allen Kaufman, "Security Lessons from the Cold War," *Foreign Affairs*, July/August 1999

2 Ibid.

3 Kamran Yousuf, Defence budget up by around 20%, *The Express Tribune*, 28 April 2018.

4 Joseph Benjamin (ed), Indo Pak Relations, Prospect and Retrospect (New Delhi: Reference Press, 2004), 2.

5 George Gilder, "The Scandal of Computer Security," *Wired*, 25 July 2013.

6 Karl W. Deutsch, et al, Political community and the North Atlantic area; international organization in the light of historical experience (Princeton: Princeton University Press, 1957). 12.

7 Barry Buzan, Ole Waever, and Jaap de Wilde, *Security: A New Framework For Analysis* (London: Lynne Rienner Publishers, 1998), 21.

8 Yasmeen Khan, *The Great Partition: The Making of India and Pakistan* (America, Yale University Press, 2007), 42.

9 Bernard Brodie, *The Absolute Weapon: Atomic Power and World Order* (New York: Harcount Brace & Co., 1946); Lawrence Friedman, *Deterrence* (Cambridge: Polity Press, 2004); Lawrence Friedman, *The Evolution of Nuclear Strategy,* Third Edition (New York: Palgrave, 2003); Scott D. Sagan, Kenneth N. Waltz, *The Spread of Nuclear Weapons: A Debate Renewed* (New York: W.W. Norton, 2003); Peter R. Lavoy, Scott D. Sagan, and James J. Waltz, *Planning the Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons,* (London: Cornell University Press, 2000); Sir Michael Quinlan, "India-Pakistan Deterrence Revisited," *Survival*, Vol. 47, No. 3, Autumn, 2005; Rifaat Hussain, "Nuclear Command/Control and Deterrence Stability," *Strategic Issues,* No. 3, March 2000; Rifaat Hussain, "Nuclear Doctrines in South Asia." *SASUU Research Report*, No 4, December 2005; Feroz Hassan Khan, "Nuclear Proliferation Motivations: Lessons from Pakistan," *Nonproliferation Review,* Vol.13, No.3, November 2006; Naeem Ahmad Salik, "Pakistan's Ballistic Missile Development Programme

— Security Imperatives, Rationale and Objectives," *Strategic Studies, Vol. XXI, No.1*, Spring 2001.

[10] The term gives an idea that technology is related to national security. The term is used after discussion with Professor Nazli Choucri of the Political Science Department of the MIT.

[11] An idea shared by Leilani Gilpin, a Research Associate at Internet Policy Research Initiative (IPRI), in MIT.

[12] Definition extracted from the British Dictionary.

[13] Definition extracted from the Oxford Dictionary but in Political Science the realism is a broad concept and most commonly represents military power.

[14] Jack Donnelly, *The Ethics of Realism*, in Christian Reus-Smit, Duncan Snidal (eds.), (*The Oxford Handbook of International Relations*, Oxford University Press, 2008), 150.

[15] This is the author's own definition of cybernetics realism, the definition was extracted after several discussions with Leilani Gilpin.

[16] Albert Müller, A Brief History of the BCL, *Heinz von Foerster and the Biological Computer Laboratory, (*Note: Originally published in *Österreichische Zeitschrift für Geschichtswissenschaften* in 2000 German-to-English translation 2005 by Jeb Bishop).

[17] Norbert Wiener, *Cybernetics, or Control and Communication in the Animal and the Machine* (Cambridge: MIT Press, 1948). This term was first used by the French physicist André-Marie Ampère in the mid of the 19th century. He called cybernetics the science of the control of governments. The term became more popular when American mathematician Norbert Wiener published his book with the title *Cybernetics* in 1948. In this book, Wiener used the reference of the British physicist James Clerk Maxwell article which was published in1868, Maxwell on governors and pointed out that the term *governor* is derived, via Latin, from the same Greek word that gives rise to *cybernetics*. The word 'cybernétique' was also used in 1834 by physicist André-Marie Ampère (1775–1836) to denote the sciences of government in his classification system of human knowledge.

[18] Couffignal, Louis, "Essai d'une définition générale de la cybernétique," *The First International Congress on Cybernetics*, Namur, Belgium, 26–29 June 1956, Gauthier-Villars, Paris, 1958, 46-54.

[19] This is the author's ongoing project to explain the cyberspace with a theoretical framework. This theory aims to address the social science perspective as well as technological perspective. Cybernetic realism is part of the author's theory.

[20] Discussion with Professor Nazli Choucri. Some points are extracted from the assumptions of cybernetics realism, which is part of the author's work.

[21] Means to ends refer action to achieving. It means how states use different tools to achieve their short- and long-term goals.

[22] Jyotindra Nath Dixit, *India-Pakistan in War & Peace* (London: Routledge, 2002), 13.

[23] Devin Hagerty, South *Asia in World Politics* (London: Rowman & Littlefield, 2005), 161.

[24] Bruce L Smith, 'Propaganda'. *Encyclopædia Britannica*, 17 February 2016.

[25] Everett Dean Martin, "Are We Victims of Propaganda, Our Invisible Masters: A Debate with Edward Bernays," *The Forum*, 142-150.

[26] "Propaganda as a weapon? Influencing international opinion," *The British Library*.

[27] "Pakistan is fighting a war on all fronts, including the media warfare," *Pakistan Defence*, 21 May 2009.

[28] Ali Wazir, "What Does the Pashtun Tahafuz Movement Want?" *The Diplomat*, 27 April 2018.

[29] "Young Pashtuns have shown the mirror to 'mainstream' Pakistan," *Daily Times, 2 February 2108.*

[30] "We have enough evidence to prove PTM is being used to create trouble: ISPR," *Daily Times*, 4 June 2018.

[31] "Case registered against PTM workers over anti-army slogans," *The News*, 5 May 2018.

[32] "Cyber security of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences," *Chatham House*, 11 January 2018.

[33] "India-Pakistan: Troubled Relations (Timeline)," *BBC*, 4 June 002.

[34] Asif A Siddiqi, "Technology in the South Asian imaginary," *History and Technology*, Volume.31, Issue.4, (2015), 341-349.

[35] Gary McGrawa, "Cyber War is Inevitable (Unless We Build Security In)," *Journal of Strategic Studies*, Vol. 36, Issue 1, 2013, 109-111.

[36] Adam L. Penenberg, Hacking Bhabha, *Forbes*, 16 November 1998, (https://www.forbes.com/1998/11/16/feat.html#492ecf25618e).

[37] Ibid.

[38] "Cyber war between Pakistan and India," 16 July 2009, http://sec.only-4u.info/page/61/, (accessed 10 March 2018).

[39] India ranked 23rd out of 165 countries on the Global Cybersecurity Index 2017 released by United Nations' International Telecommunication Union (ITU). Moreover, India was listed under the "maturing" category alongside 77 other countries that have developed complex commitments to cyber security. According to A.T. Kearney, the cost of cybercrimes in India currently exceeds $4 billion. The Forbes estimates the figure to grow at 9.8% every year and in 2022 it will reach reach $170 billion. These figures highlight the growing importance of strong cyber security architecture with the rising digitalisation in India. World Economic Forum also points out, that after land, water, and air, cyberspace is the new frontier in warfare.

[40] Ashley J. Tellis & Subimal Bhattacharjee, "Cyberspace in India: Growing and Maturing," *Carnegie Endowment for International peace*, 22 April 2013.

[41] Arvind Gupt & Philip Auerswald, "How India is Moving Toward a Digital-First Economy," *Harvard Business, Review*, 08 November 2017. Arvind, is the head of technology for Indian Prime Minister Narendra Modi's BJP party, and has been for the past seven years. His views on digital transformations include his experience as a member of the research team that developed the first web browser (Mosaic, the predecessor to Netscape) in the early 1990s and as a technology entrepreneur. Philip, is an economist whose

most recent book traces processes of digital disruption over the long arc of human history.

[42] Lu Chuanying, "China's Emerging Cyberspace Strategy," *The Diplomat*, 24 May 2016.

[43] "New War Ground between Pakistan and India: Cyber War," 02 August 2011, http://digitalmedia.strategyeye.com/2011/08/02/new_war_ground_between_india_and_pakistan_cyber_warfare/, (accessed 10 March 2018).

[44] "India readies cyber army to spy on hostile nations," *The times of India,* 5 August 2010, http://articles.timesofindia.indiatimes.com/2010-08-05/india/28322993_1_computer-systems-bpos-cyber, (accessed 10 March 2018).

[45] Ibid.

[46] "New War Ground between Pakistan and India: Cyber War," *Digital Media,* 02 August 2011, http://digitalmedia.strategyeye.com/2011/08/02/new_war_ground_between_india_and_pakistan_cyber_warfare/, (accessed 10 March 2018).

[47] Sanjiv Tomar, "National Cyber Security Policy 2013: An Assessment," *Institute for Defence Studies and Analysis,* India, 26 August 2013, http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813, (Accessed on 17 March 2018).

[48] Dale Peterson, "Offensive Cyber Weapons: Constructive, Development, and Employment," *Journal of Strategic Studies*, Vol. 36, Issue 1, (2013): pp.120-124.

[49] Aman Thakker, t's Time For India to Update Its Cybersecurity Policy, *The Diplomat*, 10 October 2017.

[50] Ibid.

[51] A group of eighty leading defence, strategic and intelligence officials, ranging from former Director of the Intelligence Bureau PC Haldar, former Admiral Arun Prakash, former Chief of the Air Staff PV Naik, and former Foreign Secretary Shyam Saran called upon Prime Minister Modi to "take urgent steps" to improve India's cyber security standards. In particular, they highlighted the need for "more regular, more formalised interaction" between the civilian and military branches of government. The government's

updated policy must go beyond the vision of greater collaboration outlined in the 2013 policy.

[52] Davinder Kumar**,** "India's Cyber Security: Architecture and Imperatives," *Indian Foundation Journals*, Vol.V, Issue No. 5, (September-October 2017), 7-11.

[53] Sanjiv Tomar, "National Cyber Security Policy 2013: An Assessment," *Institute for Defence Studies and Analysis,* India, 26 August 2013.

[54] "India and Pakistan at war in cyberspace ahead of Independence Day," *Business Today*, 4 August 2017.

[55] Umair Jamal, "The Trouble With Pakistan's Cybercrimes Bills," *The Diplomat*, 27 April 2016.

[56] Chekinov, S. C & Bogdanov, S. A. *The Nature and Content of a New-Generation War*, United States: Military Thought, 16.

[57] Béla Szunyogh, Psychological warfare; an introduction to ideological propaganda and the techniques of psychological warfar*e* (United States: William-Frederick Press, 1955), 13.

[58] Kiran Hasan, "Social Media, Media Freedom and Pakistan's War on Terror," Commonwealth Journal of International Affairs, Vol. 107, issue.2, (March 2018), 189-202.

[59] Adhulika Srikumar "India and Israel's cyber security partnership could be a potential game changer," Observer Research Foundation, 10 June 2017.

[60] In the year 2004, Elbit Systems signed an agreement with the Defence Ministry for the Digital Army Program (DAP) for a period of 10 years (2004-2014). Rafael Armament Development Authority Ltd. and Tadiran Systems Ltd partnered with Elbit Systems for DAP. In 2014, the IDF concluded the deployment of the Tzayad (Digital Land Army) system in all of its field formations and now they are working to build the next generation of the Israeli army's digital C4I network.

[61] Gavriel Fiske, "India, Israel set to team up on cyber-defense," *Time of Israel*, 30 September 2014.

[62] "Future prospects of the India-Israel defense cooperation," *The Jerusalem Post*, 1 January 2018.

[63] Ben Dreyfuss and Emily Dreyfuss, "What is the NSA's PRISM program?" *CNET News*, 7 June 2013.

[64] "NSA Reportedly Mines Servers of U.S. Internet Firms for Data," *NPR*, 06 June 2013.

[65] "Mushahid chairs meeting of Senate Standing Committee on Defence" *The Frontier Post*, 09 July 2013.

[66] "Mushahid for joint Asian strategy to counter cyber threats," *Pakistan Today*, 08 July 2013.

[67] "7-point Action Plan for a Cyber Secure Pakistan," *Dawn*, 12 July 2013.

[68] "Air University to open first-ever centre for cyber security," *Daily Times*, 21 May 2018.

[69] "Pakistan's first-ever Cyber Security Centre launched," *Gulf News Pakistan*, 22 May 2018.

[70] The headquarter of the National Centre for Cyber Security will be based at Air University Islamabad with labs at different universities of Pakistan including Bahria University Islamabad, National University of Science and Technology (NUST), Information Technology University Lahore (ITU), Lahore University of Managment Sciences (LUMS), University of Peshawar, University of Engineering and Technology Peshawar, University of Nowshera, Pakistan Institute of Engineering and Applied Sciences (PIEAS), NED University Karachi, University of Engineering and Technology Lahore and University of Engineering and Technology Taxila.

[71] Stephen Biddle, Military Power: Explaining Victory and Defeat in Modern Battle (USA, Princeton University Press, 2004), p.38.

[72] Ibid, p.45.

[73] Khushwant Singh, "Foreign Affairs Pakistan, India and The Bomb," *New York Time*, 01 July 1979, https://www.nytimes.com/1979/07/01/archives/foreign-affairs-pakistan-india-and-the-bomb.html.

[74] Ibid.

[75] Syed Riffat Hussain, Missile Race in South Asia: The Way Forward, South Asia Survey, Volume: 11 issue: 2 (1 September 2004), pp.273-286.

[76] Ibid.

[77] Matthew J. Morgan, *The Impact of 9/11 on Politics and War: The Day that Changed Everything?* (England, Palgrave Macmillan, 4 August 2009). p.222.

[78] Keppel, Gilles; Milelli, Jean-Pierre; Ghazaleh, Pascale (2008). *Al Qaeda in its own words* (USA, Harvard University Press, 2008), p.19.

[79] Dan Caldwell, Robert Williams, *Seeking Security in an Insecure World* (2nd ed.) (United States of America, Rowman & Littlefield, 2011), pp.103–104.

[80] "Social media being used against Pakistan, institutions: DG ISPR," *ISPR Press Conference*, 04 June 2018, (https://www.geo.tv/latest/197971-dg-ispr-briefs-media-on-ceasefire-violations-by-india accessed date 10 June 2018).

[81] "Anti-army slogans: PTM workers booked" *The News*, 10 May 2018.