INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 3, Issue 12, 2025

INFORMATION FLOWS, CYBER SECURITY POLICY AND HYBRID WARFARE: A THEMATIC ANALYSIS OF PAKISTAN

Hammad Ahmed[1], Mirza Nouman Ali Talib[*2], Awais Aslam Malik[3]

[1]*Securities and Exchange Commission of Pakistan*
[*2]*Department of Economics, National Defence University, Islamabad*
[3]*Bahria University Islamabad*

Corresponding Author: *
Mirza Nouman Ali Talib
DOI: https://doi.org/10.5281/zenodo.18044141

Received	Accepted	Published
25 October 2025	01 December 2025	24 December 2025

ABSTRACT

In the wake of digitalization and the proliferation of Information and Communication Technologies (ICT) in major domains of national power, incapacity to deter the cyber-attacks have brought the serious concerns of securitizing data for policy makers in developing countries like Pakistan. By highlighting the weak cyber infrastructure and its security policy, this study exhibits the relationship of insecure critical information flows and hybrid warfare posing challenges to the national security of Pakistan. To analyze the Pakistan's current cyber situation, qualitative research method is adopted in which semi-structured interviews are conducted from relevant resource civil-military officials using purposive sampling technique. By analyzing through the lens of DIME ontology, the findings of thematic analysis elucidate that Pakistan's critical information flows are insecure due to weak cyber infrastructure and delayed formulation of national cyber security policy may be responsible in making critical infrastructure prone to manifold cyberattacks. As a consequence, the threats of hybrid warfare posing challenges to the national security that are eminent due to lack of resilient measures deterring spread of disinformation and propaganda. The findings implicate by signifying the need of implementing a holistic and robust cyber security policy along with the applicability of Chinese cyber governance model with prerequisite modifications to improve the situation of cyber sector in population abundant countries like Pakistan for their best interest of national security.

Keywords: *Information flows, Cyber-attacks, Cyber security policy, Hybrid Warfare, Chinese cyber governance model, national security*

INTRODUCTION

This article focuses to ascertain the weaknesses in Pakistan's cyber security infrastructure and the information flows. As the information flows are insecure, it is taking Pakistan towards and exposing it vulnerabilities (critical elements and information) to the multifaceted threats of hybrid warfare. Besides this, the paper also highlights the threats of hybrid warfare that Pakistan is facing in the domain of cyber warfare and information warfare due to the technological evolution and weak cyber infrastructure. Moreover, it also finds the Chinese cyber governance model's applicability in the fraternity of Pakistan's cyber sector to mitigate and curb the perils of cyberattacks and hybrid warfare.

Background

With the evolution and advancement in information technology, data and information

flows have become an important part in the process of digitising and information system (Yamin, 2018). As these information flows and data are the most essential sources of the knowledge that give connotation to every sector of the world (Chenou, 2021). Today, information is considered as a pre-requisite of technological, cultural, economic and social organizations since the development of computer and internet (Da Silva, & Agusti-Cullell, 2008). The advancement and development of information technologies has created a 'cyber world' or 'cyber space' that has linked countries, organizations and people through the internet for the exchange of information to make their lives possible (Egloff, 2017). The invention of World Wide Web, the expansion and commercialization of cyberspace have increasingly made the societies and lives to become dependent on network serviceability (Sarangam, 2021; Akram et al. 2011).

Steve Winterfeld and Jason Andress have described and explained cyber space or cyber world as a 'hypothetical domain or environment' that comprises a group of independent networks that include internet, computers, telecom networks and processor to gather, alter, analyse, transmit and secure the data and information, thus making the world dependent on cyberspace (Rafiq, 2019). This dependency has increasingly pushed the critical infrastructures and societies to become more dependent on cyberspace and information technologies such as Supervisory Control and Data acquisition (SCADA) and internet-enabled devices to control the information flows and all processes (Da Silva, & Agusti-Cullell, 2008). On contrary, the ever-increasing dependence of societies and infrastructures on cyberspace has exposed the vulnerabilities to multifaceted threats of cyber-attacks and hybrid warfare due to the presence of fragile cyber security. Hybrid warfare is defined as a secret, open or joint warfare that uses the resources of diplomacy, informational, military, and economics (DIME) as well as cyber methods for the purpose of creating an influence and to achieve the political or military goals (Aptsiauri, 2017). Today, the threats of hybrid warfare are ever-changing and diverse in nature due to the inclusion of tools such as information warfare attacks and cyber security attacks which are making difficult for the states to secure their critical information flows from anti-state elements (Abdyraeva, 2020).

Pakistan: Cyber security and Hybrid warfare

Pakistan has also become a prominent member of the digital world as it is moving towards technological innovation, e-governance, and ICT based infrastructure. However, while coping up the digitising process, there has been an aggravation of cyber security threats and technological issues in the region of Pakistan (Tariq et.al. 2013). Currently, Pakistan is exposed to multifaceted cyber threats such as propaganda, disruption of services, abuse and espionage due to proliferation and reliance on ICT and cyber space (Chenou, 2021). Furthermore, the cyber space of Pakistan has also become a pivotal point for militarized actions and crimes which is endangering the national security and may create an unfavorable situation for it in the digital society (Rafiq, 2019).

There has been a lack of focus by government towards the cyber security and has paid no heed on scrutinizing the cyber space used by state and non-state actors against its interest since the inclusion of ICT and internet in the mainstream practice (Tariq et.al. 2013). Due to this, Pakistan is vulnerable to numerous cyberattacks i.e. cyber frauds, information warfare, financial theft and surveillance on critical infrastructures which is exposing it towards hybrid warfare (Rafiq, 2019). Therefore, it is in the need of hour to formulate and execute a comprehensive national level cyber security policy in Pakistan with an aim of developing and enhancing cyber security infrastructure and ICTs by recognizing and mitigating the threats of cyberattacks and the impact of hybrid warfare on masses in an effective way (Tariq et.al. 2013; Rafiq, 2019; Ali, 2021).

2. Material

Over the last decade, the world has changed into a global information society due to the

expansion and growth of the internet in all wake of lives (Lipson, 2002). Since then, business, governments and institutions have been exchanging the flow of information with their counterparts through the use of ICT and internet. Moreover, governments have also been utilising the internet for the flow of information to its citizen and to the world (Lipson, 2002). Due to this, governments have been in the continuous process of replacing the traditional methods of gathering and spreading the information with the internet.

The Importance of Information Flow

Today, information flow is considered as an essential tool for modelling, scientific discovery, technological society and ICT devices that gather, analyze and spread the information (Da Silva, & Agusti-Cullell, 2008). Among them, computer is considered as the most useful development; it facilitates the information flow as internet enabled-devices assist cross-border information flow in a concurrent manner (Meltzer, 2015). Therefore, internet has become an important part of the global information society due to its ability to give meaning to the information by acting as an intelligent agent and to disseminate the information worldwide (Da Silva, & Agusti-Cullell, 2008; Meltzer, 2015).

Currently, state and non-state actors which possess or own such information are considered as influential and powerful as through the use of this information, they can affect or influence the people of targeted countries psychologically by creating hassle and instability (Tariq et.al. 2013). Due to this, the mode of warfare has been changed into irregular or unconventional warfare through the amalgamation of information with cyberattacks.

The Perils of Cyber Attacks in Pakistan

The prevailing threats of cyber-attacks in cyberspace have the capability of creating undesirable consequences for the states, institutions and people (Tariq et.al. 2013). Due to this, the types of cyber-attacks are mostly based on resources, impacts, magnitude and motivation ranging from cybercrime, cyberwar, and cyberterrorism. Pakistan has also been encircled by the dangers and threats of these cyberattacks. As Pakistan has been in the process of transition from traditional mode of governance to digitizing (Rasool, 2015). This transition has increased the reliance and dependency of institutions and sectors such as education, military, banking and government on cyberspace, thus making Pakistan vulnerable to cyberattacks like cybercrime, cyberterrorism, cyber espionage, disruption of services and sabotage on nuclear assets (Tariq et.al. 2013). On the other side, Pakistan's lack of concern towards cyber security is giving or allowing state and non-state actors to utilise the cyberspace for the purpose of achieving their malicious social, political and religious objectives. As a result, Pakistan is on the brink of edge due to the cyberspace used by international rivals and state-sponsored terrorist groups that can endanger its authority in the global world (Tariq et.al. 2013; Rasool, 2015; Naseer & Amin, 2020).

Fusion of Cyber Attacks with Hybrid Warfare

The dawn of 21st century has changed the concept of wagging a warfare, as cyberattacks have now been considered as the most important tools of hybrid warfare (Simons et al., 2020). Advancement in ICTs and internet has reduced the physical, informational and temporal distances between the superiors and its troops (Steingartner & Galinec, 2021). Technologies are being used in the battlefield against the enemies than soldiers or hard power. It has become very important to take and comprehend the concept of hybrid warfare with cyber perspective (Devereux, 2019). In the contemporary era, in hybrid warfare, the methods of traditional warfare and cyberattacks are being used (Devereux, 2019). The international community is challenged by the threats of hybrid warfare in terms of economic crisis, energy crisis, demographic issues, access to information, and extension of non-military characteristics (Ştefănescu, 2016). Therefore, the concept of hybrid warfare exhibits the use of propaganda, disinformation, disruption of services, use of cyberattacks and media in the battle field with a purpose of creating chaos and

ultimately weakening the stability of the target state (Ştefănescu, 2016).

Today, cyberattacks are considered as lethal as nuclear attacks because it amplifies the prevalent deficit of trust between the government and its people, when a country is in the middle of other crisis (Simons et al., 2020). Such attacks are not only launched with a purpose of giving physical damage, but also to impact psychologically through the conception of uncertainty (Ştefănescu, 2016). Hybrid warfare mainly targets critical infrastructures such as national power buildings, nuclear plant etc. and people of a particular state by gaining the crucial information and by spreading disinformation, propaganda and fake news (Dowse & Bachmann, 2019). Thus, "lies spread very fast", which is a basis of hybrid warfare as figured out by scholars (Yasin, 2020).

Prevailing Threats and Challenges of Hybrid Warfare in Pakistan

International rivals and state-sponsored groups have been using hybrid warfare strategy against the interest of Pakistan. Amongst all, India has been practically implementing hybrid warfare strategy in terms of fifth generation warfare by using the amalgamation of national power with the technological elements with an aim of destabilising and endangering the sovereignty of Pakistan in the international community (Dawn news, 2020). The investigation report of EU Disinfo Lab has revealed that India has been targeting Pakistan through more than 750 websites operating in 119 different countries to weaken the position of it in the global community. There main purpose is to defame Pakistan and China through propaganda at the forums like UN and EU (Hayat, 2021). Moreover, such can also be observed at the meeting of Financial Action Task Force (FATF) where Indian lobbies are kept on targeting the information system, economy and international image of Pakistan to push it into the black list (Dawn news, 2020). Thus, weaknesses within the internal structure have provided a gap to state and non-state actors to implement the strategy of hybrid warfare against the interest of Pakistan with an effortlessness (Haider et al, 2020).

Pakistan's Cyber Security Situation

Since the emergence of internet, states have been in a continuous process of devising holistic approach and cyber policies to mitigate the prevalent threats of cyberattacks. Conversely, Pakistan has been negligent in formulating a national cyber security policy due to which it has struggled to mitigate the threats of cyberattacks (Safdar, 2021). Certain general guidelines were provided to specific sectors such banking and military, but a national level cyber security policy was not devised by the government. As a result, according to the 2018 report of Global Security Index, Pakistan was ranked seventh worst countries in terms of secure cyberspace (Ali,2021). Pakistan is taken as a weak cyber secured country in the cyber domain in terms of catering cyberattacks. However, after the struggle of almost two decades, in 2021, Pakistan's approved and devised its first ever national level cyber security policy with the assistance of Ministry of Information Technology and Telecommunication (Khan, 2021).

China's Cyber Security Initiatives

In the last two decades, China being the emerging economy of the world, has also been undergoing through the process of rapid digitising and cyber-based technologies (Li et al., 2020). Due to this, China has made the development of cyber security as an integral part of its national security (Kshetri & Kshetri, 2016). Today, China considers the enhancement in cyber security as an opportunity to develop its military capabilities as well as threat to the fabric of national security (Daricili et al., 2018). China has the most number of internet users in the world i.e. 800 million in 2019 which increased by 3584% within two decades. Due to this, in 2018, China experienced on average 800 million cyberattacks on daily basis (Li et al., 2020).

The cyber security policy of China has been based on economic, political and military objectives in order to control such massive

internet users and to mitigate cyberattacks (Daricili et al., 2018). The main purpose of China's cyber security policy is to control the internet, protect the technologies, to support the military, to consolidate the strategies of cyber and information warfare, and to develop measures against information warfare (Li et al., 2020). Moreover, China has also banned the social media networks in order to encourage the use of national social platforms to make the mechanism of cyber security strenuous. China has also implemented the great firewall model by banning the commercial websites and by regulating the usage of internet within the society for censorship and surveillance (Daricili et al., 2018; Li et al., 2020).

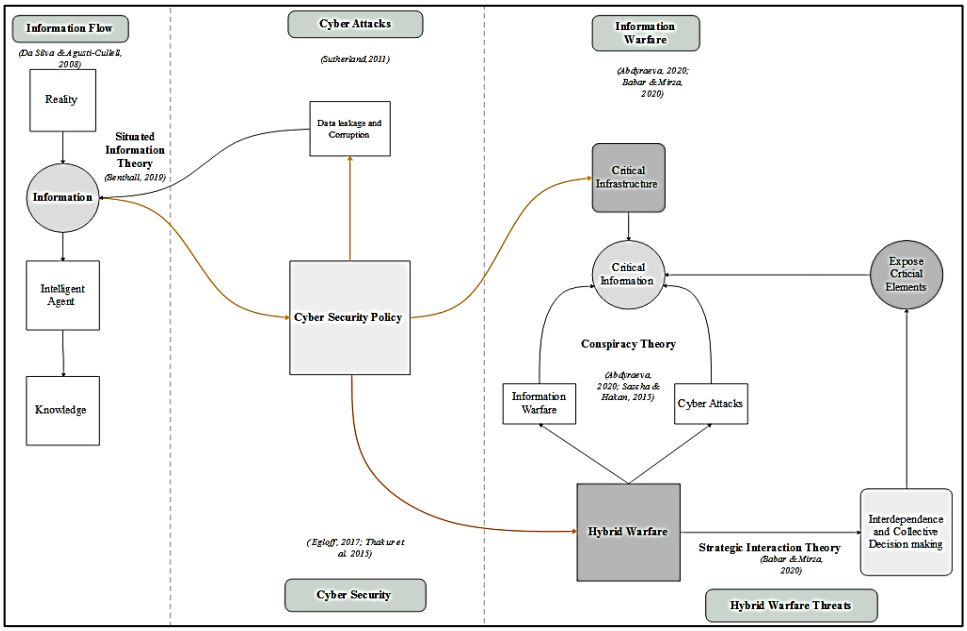
Chinese Cyber Governance Model

With the dispersion of ICTs and boom of internet, the government of China has linked national security with cyber security and has recently formulated a cyber governance model that comprises the international and domestic components. The domestic components are the unification of cyber laws, regulation, standard and strategies (Segal, 2020). As these components provide guidelines for the strengthening of ICT industry, data protection, encryption as well as protection of critical infrastructures and data. Moreover, trainings on cyber security are made mandatory for officials in an order to implement and execute the laws of personal information security and cyber security for the purpose of collecting, keeping, shielding, analysing and sharing of information and data (Segal, 2020). On the international side or level, China has introduced a cyber diplomacy concept to implement and introduce the model of cyber governance at the international forums (Segal, 2020).

Chinese cyber governance model is a model of cyber security which is not designed with the prime focus of cybersecurity only but also link it to the national security. Today, cyberattacks have become unconventional, these attacks are not only limited to land, air and water only. A single click or a cyberattack on critical infrastructure by the adversaries could hamper the stability of a country and cause an equal damage like a traditional military attack in the internal structure. Therefore, China has understood the ever-changing nature of cyberattacks and hybrid warfare due to which it has mainstreamed the challenges of cybersecurity with its national security (Sarkar, 2020).

Conceptual Framework

For the purpose of understanding the current situation and the link of information flows, cyber security policy with hybrid warfare in Pakistan, this article proposes a conceptual framework on the basis of analysis of aforementioned review of literature. The conceptual framework of this article is presented and explained below;



Conceptual Framework
Source: (Author's Information)

The threats of cyberattacks and the impact of hybrid warfare are multidimensional which involve the need of advanced cyber strategies and techniques by understanding that cyberspace has no boundaries and it does not belong to anyone. Consequently, state and non-state actors are kept on utilising the cyberspace by gathering the critical information due to fragile cyber security mechanism and infrastructure to carry out their malicious activities in the domestic arena of Pakistan via hybrid warfare strategy. Moreover, it also depicts the role of intelligent agent who gives meaning to and manipulates the stored and shared information in the cyberspace through cyberattacks i.e. corruption and data leakages. Thus, creating instability and chaos by constantly affecting the masses through disseminating disinformation and propaganda. The conceptual framework also describes the inferences of executing a comprehensive national level cyber security policy along with the inclusion of Chinese cyber governance model in Pakistan. In order to safeguard the information flows and cyberspace from every type of cyberattacks and the impact of hybrid warfare.

3. Methods

Research Methods

The foremost and basic step in research is to perform desk research- reading of all relevant events and material to have an in-depth understanding of the situation. For this, research papers, books, scholarly articles, as well as governmental and non-governmental documents are gone through.

Data Collection and Sources

In research, both the primary and secondary data are important and used for analysis. Primary data is collected through semi-structured interviews from the most relevant stakeholders i.e. civil-military leadership while secondary data is gathered through numerous resources. Initially, to have a better understanding of situation and link between information flows, cyber security policy and hybrid warfare, policy papers, published articles, books and cyber initiatives and polices of China and Pakistan are reviewed and studied thoroughly. Majority of documents are accessed through different search engines such as Google scholar, Mendeley, Elsevier, Jstor. The main purpose of using these resources is to understand the linkage of having insecure

information flows with that of fragile cyber security infrastructure and policy, and the impact hybrid warfare creates on the citizens of Pakistan hypothetically.

Semi-Structured Interviews

In this paper, semi-structured interviews are selected as a tool of collecting information from the targeted stakeholders. Semi-structured interviews also known as face to face interviews, are the interviews which have a set of developed questions. Moreover, these interviews also allow or lead to the addition of new questions during the interview. A set of 16 questions are established by dividing them into three parts for the purpose of collecting the information from the stakeholders and to understand their perspective about the current scenario through the lens of Diplomacy, Information, Military, and Economics (DIME) model.

Sampling Design

Non-probability sampling technique is used to select the sample size in this paper. In non-probability sampling, judgement or purposive sampling is applied to select the target population. The official of government and military, policymakers, academicians, and cyber security experts who have knowledge and are familiar with the current issues within the information flows, cyber security infrastructure and policy, and the impact hybrid warfare creates on the masses of Pakistan are being selected.

Sampling Size

In qualitative research, the sample size is selected on the basis of saturation point as purported by different school of thoughts and theories. Saturation point is used as an indicator for sampling acceptability that means the researcher has to end the data collection process when the point of saturation is being attained i.e. consistent information or no new information is coming after a certain number of interviews, according to O'Reilly and Parker (2013).

On the basis of different concepts and theories related to sample size, twenty interviews are conducted from civil-military leadership i.e. military officials, government officials, policymakers, academicians, and cyber security experts as after twenty interviews, saturation point is reached. In order to confirm the validity of saturation point, five more interviews are also conducted.

Data Analysis Technique

In this paper, thematic analysis is used for the purpose of data analysis, as thematic analysis technique figures out and helps to develop themes from the collected data. Thematic analysis technique is extensively used for the purpose of analysing the data in qualitative research, according to Braun and Clarke (2006). It also delivers a set of different skills for accompanying other data analysis techniques also (Nowell et al., 2017).

In thematic analysis, a set of standard steps are being followed starting from classifying, shaping, scrutinising, describing and reporting of themes and sub-themes produced from the collected data (Braun & Clarke, 2006). It is basically a six-phased process of data analysis that is interrelated to one another and repeated constantly by moving forward and backward between different phases (Braun & Clarke, 2006; Nowell et al., 2017).

4. Results

The insights and perspectives of civil-military leaderships are collected and recorded through interviews in order to understand Pakistan's current scenario of cyber security, and the linkage of insecure information flows with hybrid warfare in the presence of fragile cyber security infrastructure and policy. Moreover, their perspectives are also used to comprehend the probability of implementing Chinese cyber governance model under the comprehensive national level cyber security policy in order to mitigate and curtail cyberattacks and the threats of hybrid warfare. The perceptions of twenty-five interviews are scrutinized through the method of thematic analysis via NVIVO software.

Thematic Analysis

Thematic analysis is a process that helps to identify codes, sub-themes and themes from the collected data. Semi-structured interviews are conducted to get the responses from most relevant resource persons, as these responses are a great source of knowledge and help to bring clarity to several main themes that are related to information flows, cyber security policy and hybrid warfare. Themes that produced by moving forward and backward repeatedly, are the significance of information flows, Pakistan' cyber sector provocations, repercussions of hybrid warfare in the society, and Chinese cyber governance model's applicability

The Significance of Information Flows

Literature review has already pointed out the significance of information flows in the current globalised information society, as the extent of power of a particular state is evaluated by the degree of secured and critical information flows a state has. Thereby, all wars in future would be fought for the purpose of gaining critical information. This point is also confirmed and approved by Mr. Zahid Bashir- member of cyber security policy and chairman of cyber security task in planning commission of Pakistan. He said, "The world now is in the constant state of fifth generation warfare where all states are indulged in gathering the critical information flows to get strategic position over other states". Moreover, according to him, "Today, on the basis of information, a state is considered as powerful and authoritative, on contrary, this same information may cause a devastation to the national security too".

In modern era, the world is considered as domain of information which is one of the perspectives of resource persons. According to them, the elements of DIME model can be used through the gathered insecure information flows to target the opponents (see figure 4.1 below). Mr. Shahmeer Amir- cyber security advisor in Ministry of Finance and among top three ethical hackers also added the same. He pointed out, "Insecure information related to diplomacy, military and economics can hamper the national security of a particular country". Moreover, he also added, "Any fake new or information or coordinates related to military officials, nuclear warheads or misinformation related to stock market may paralyse the system of a country within seconds". History has been the bare witness that how DIME model has been used against Pakistan to hamper the fabric of national security. As per the report of Disinfo Lab, insecure information flows have always been used in the elements of DIME model by anti-state group against Pakistan to target its sovereignty

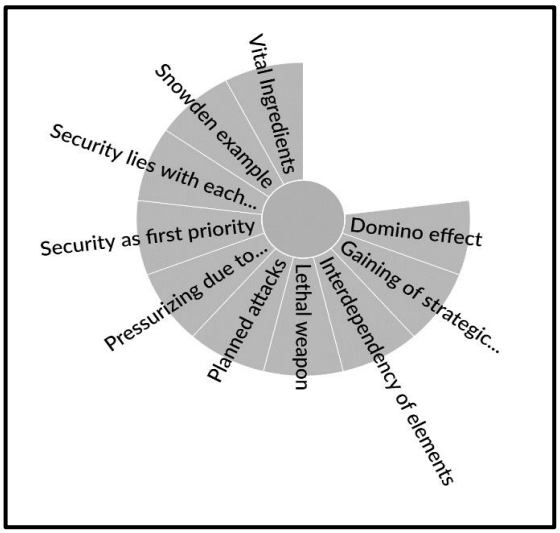


Figure 4.1 Insecure Information Flows and DIME
Source (Author's information)

Therefore, it can be concluded on the respondent's perspectives that in modern times, information flows are the core element and vital for Pakistan's national security, and proper securing of these information flows are one of the core elements of national security. As manipulation and leakage of such information flows may lead to catastrophic situation for Pakistan

Pakistan's Cyber Sector Provocations

Today, Pakistan is also undergoing the process of transition towards digitalisation. Major sectors and critical infrastructures of Pakistan such as banking, power, energy, military and financial have become dependent on internet-enabled devices and advanced ICTs for the purpose of sharing and storing information. For the same reason, Pakistan bought the use of ICTs into the mainstream, but totally neglected the part of cyber security during the transition. Brigadier (R) Dr. Ashraf Masood- CEO of Khastech solutions and Former dean of Military College of Signals agreed the situation of Pakistan. As he opined, "In start, ICTs devices were devised for the purpose of typing only, but with the emergence of internet, these ICTs devices were started to secure and store the critical information. Pakistan as a state, has embraced these devices for the same purpose, but has showed lack of concern related to the cyber security infrastructure. He further added, "Iran having a weak cyber security infrastructure for its nuclear program, has always been on the top of CIA's target list".

Pakistan is prone to all types of cyberattacks that are hampering the fabric of national security. Dr. Rafi- Director cyber wing in Ministry of IT& Telecom accepted the existence of this reality. According to him, "Every type of cyberattack is frequent, common and prevalent in Pakistan, and every sector of it, is susceptible to all types of cyberattacks". On the same lines, Mr. Ammar Jaffri- Former DG of FIA, also added that cyberattacks are launched by two groups; i) by the adversaries with an aim of dislodging the operability of the country, and ii) by cyber security experts from dark to deep dark web. Dr. Tariq Raheem- Deam of IoBM University, also explained the weaknesses and provocations of Pakistan's cyber sector. He added, "Cyberattacks are launched to affect the national security of Pakistan, and during the period of 2010 to 2016, Pakistan was among top ten countries of cyberattacks". Thus, currently, Pakistan is vulnerable to every type of cyberattacks which are launched to destruct and manipulate its critical information (see figure 4.2 below).

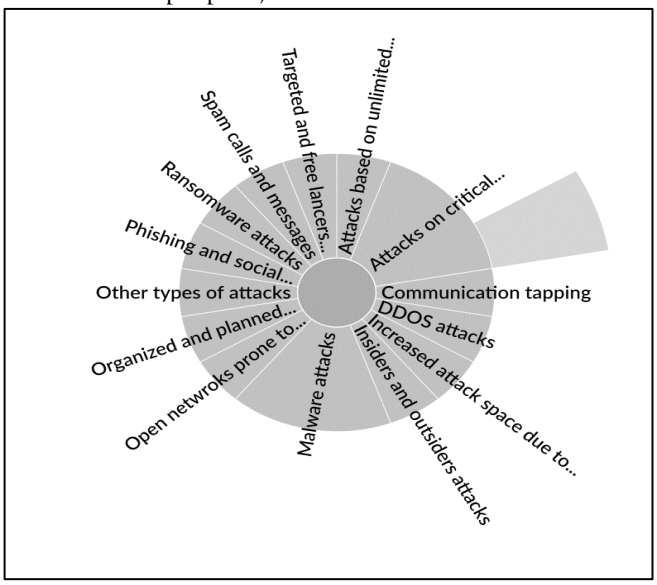


Figure 4.2 Pakistan and types of Cyberattacks
Source (Author's information)

Since the inclusion and adoption of ICTs in major sectors, Pakistan has been considered as the lowest country in terms of cyber security due to absence of cyber security policy and presence of weak cyber infrastructure for a prolonged time. Mr. Ammar Jaffri said, "Today, Pakistan is ranked as low country due to lack of resilient cyber infrastructure". He also added, "The world is heading to new form of warfare i.e. Hybrid warfare, and we as a state, are highly vulnerable to it. If cyber security strategies are not linked to national security and inclusive approach is not implemented, then our critical infrastructures and information are highly susceptible to these threats and attacks". Moreover, the vulnerabilities are also increased by the use of pirated software and by the presence of untrained employees in major sectors. As supported by Mr. Zahid Bashir. He said, "The operating system of our country is running on pirated software and there is no policy of using certified software or windows which has been responsible in making our country vulnerable to cyberattacks, thus creating challenges for cyber sector". Mr. Ahmed Manzoor- Policy maker and Network Security Advisor also opined the same. According to him, "The use of pirated software, absence of Computer Emergency Response Team (CERT) and untrained manpower are dragging Pakistan towards the perils of cyberattacks and hybrid warfare". Consequently, there are many provocations in Pakistan's cyber sector as purported by respondents which are cited in the figure 4.3 underneath.

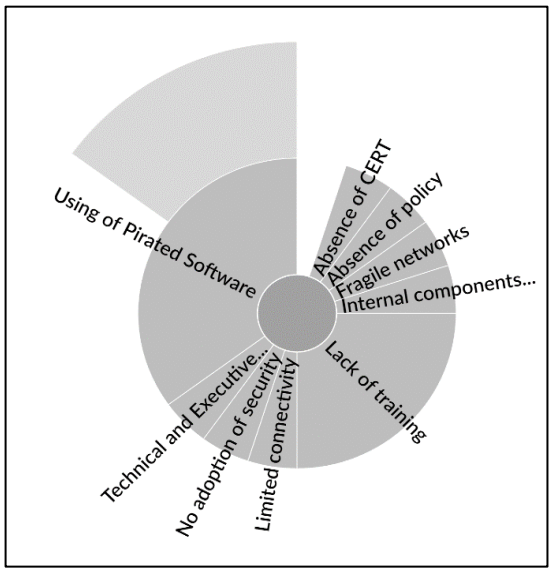


Figure 4.3 Provocation of Cyber Sector
Source (Author's information)

Therefore, it can be ascertained on the basis of responses that Pakistan is susceptible to almost all types of cyberattacks and there are numerous hassles as argued which are affecting the authority of it in the digital society and threatening its national security.

Repercussions of hybrid warfare in the Society

It is the era of unconventional or irregular warfare, as the world is moving towards non-physical warfare. As orated by Dr. Tariq Raheem, "The world will experience a data or informational war in the future, as traditional wars are becoming obsolete due to the inclusion of ICTs in battlefield". Currently, state and non-state actors are indulged in hitting the soft bellies of the opponents in order to get critical information. According to Mr. Ammar Jaffri, "Bytes before bullets scenario is actually happening in the world". Moreover, Dr. Mehreen Afzal- Chairperson of Cyber Security Department in Air University, also added that

everyone is in living in the cyber world where disinformation and propaganda are the important ingredients of hybrid warfare to affect the lives of the people.

Pakistan has been the most affected country by hybrid warfare, since the proliferation of ICTs and the diffusion of social media platforms for the access of information (see figure 4.4 below). Miss Asma Sajid- Expert in detecting fake news and Lecturer in GC University, expressed, "Social media is used as an essential tool of hybrid warfare where disinformation and manipulated information is being shared to affect the masses psychologically. As social media platforms have the highest potential of impeding the thinking process of the people". Furthermore, Mr. Mehmood ul Hassan- Deputy Director Cyber Wing in FIA, highlighted Disinfo Lab report. According to him, "India is running disinformation campaigns against Pakistan where more than 500 social media accounts are being used to defame Pakistan at the international forums".

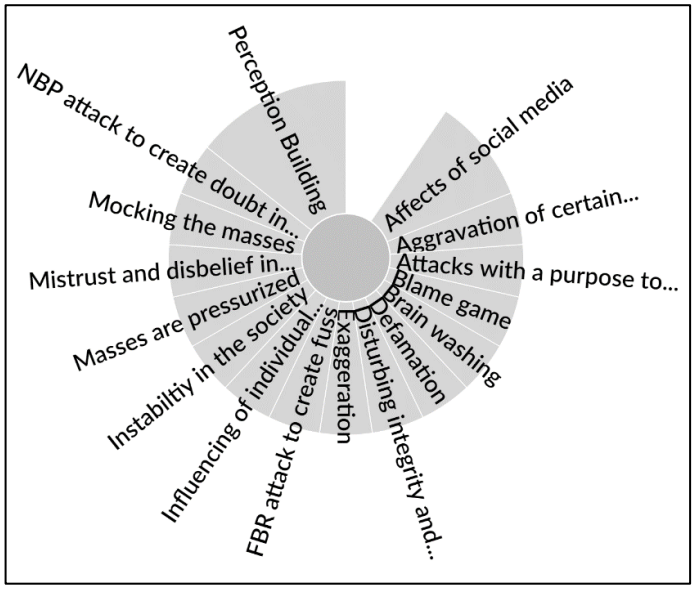


Figure 4.4 Repercussions of Hybrid Warfare
Source (Author's information)

State and non-state actors launch their cyberattacks and hybrid warfare strategy against the opponents with the help of intelligent agent. Intelligent agent is a person, bot or ransomware who collects or gathers the critical information flows with a purpose of damaging the target country. Mr. Ammar Jaffri supported the existence of this reality. He said, "State and non-state actors use artificial intelligence module to give command to the intelligent agent who by using logical algorithms exploits the loopholes in our cyber infrastructure to destruct the financial setups and the critical infrastructures". According to Mr. Rafay Baloch- Top ethical hacker, "Intelligent agents are the real problem, as intelligent agents as ransomware and bots can even bypass strong cyber security system to gain the critical information". Besides, the gathered critical information flows are used by intelligent agents to spread hatred and extremism to obstruct the stability of the society and to carryout undesirable warfare (see figure 4.5 below).

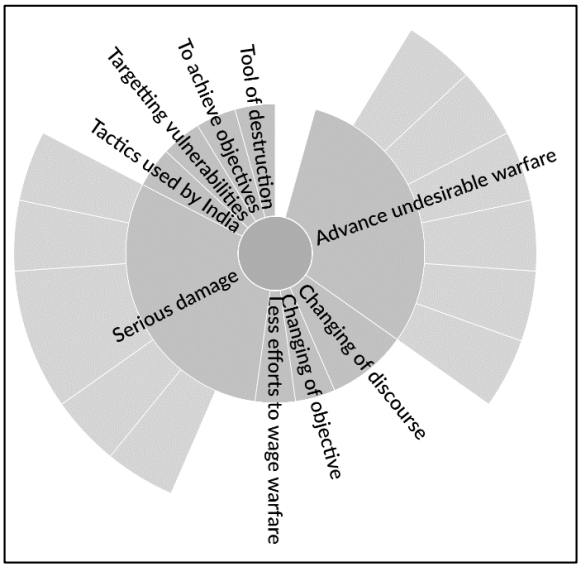


Figure 4.5 Intelligent Agent's in Hybrid Warfare
Source (Author's information)

Therefore, the participants' responses portrayed that Pakistan has always been vulnerable to the perils of hybrid warfare and the masses of Pakistan has been the main target of such warfare. Moreover, adversaries have been using intelligent agent to create chaos and fuss in the domestic arena of Pakistan to meet their malicious objectives.

Chinese Cyber Governance Model's Applicability

China has been considered as one of the top cyber security countries in the world, as it has implemented the great firewall model and is undergoing the process of implementing Chinese cyber governance model in order to mitigate, curb and to protect its masses, and critical infrastructures from advanced cyberattacks and the threats of hybrid warfare. Currently, China has initiated measures for cyber security especially Chinese cyber governance model which is taken as a signature model. So far, China has been remained successful and effective in controlling the usage of internet and in safeguarding its critical infrastructure, information flows and masses from the menace of globalised information society. According to Dr. Shahzeb Tahir, "Chinese cyber governance model is an ideal model for our cyber sector, as China has remained successful so far in limiting the threats of cyberattacks and hybrid warfare". Likewise, other respondents also supported that Chinese governance model can be applied in the cyber sector of Pakistan by bring together the required elements (see figure 4.6 below). Brig(R). Dr. Ashraf Masood also agreed and said, "There is a possibility of implementing such model in Pakistan, but the stake of government is crucial. Therefore, it is in the need of hour for government to consider this model as a base model and to implement it by modifying it according to our infrastructure".

IEER
Institute for Excellence in Education & Research

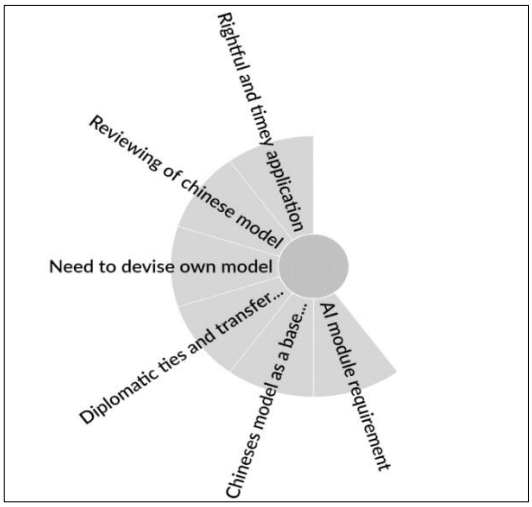


Figure 4.6 Chinese Cyber Governance Model's Applicability
Source (Author's information)

Therefore, it can be ascertained on the basis of respondents' insights that in Pakistan, the applicability of Chinese cyber governance model is possible, but with pre-requisite standards and modifications. This model can be implemented in Pakistan through; inspecting usage of internet, devising the model as per the government and political structure, formulating of cyber laws and comprehensive policy, development of indigenous protects, using necessary protocols for network protection, restricting the flow of propaganda and disinformation and lastly, allowing masses the maximum limit of using internet.

5. Discussion

Information Flows

In the contemporary era, information flows have more value than oil and gold in the world, as it is now one of the main components for effective decision making. Thereby, almost every state and non-state actor are constantly indulged in gathering the critical information flows to become powerful and to have an advantageous position over other states (Kozloski, 2009). Pakistan being the newly inducted member of cyber world, is largely becoming dependent on internet and ICTs. Due to this, the interaction of Pakistan with other states is also increasing which is giving an opportunity to anti-state groups to gather and manipulate its critical information flows due to fragile and lack of cyber security strategies, infrastructure and policy (Goffman, 1970; Babar & Mirza, 2020).

Intelligent agents are considered as an important contrivance of hybrid warfare and in cyber community for enemies, as through it, a specific meaning is given to the reality which is disseminated forward as an actionable knowledge to influence the masses as per their political objectives (Benthall, 2019). With the advancement of ICTs and internet, the role of intelligent agents has increased which has been creating problems for the members of cyber world particularly for Pakistan. The gathered critical information flows are being used in the strategy of hybrid warfare as a main tool by state and non-state actors against Pakistan to influence the perception building of the people due the absence of resilient cyber security policy and mechanisms (Da Silva, & Agusti-Cullell, 2008). Therefore, while coping up the process of digitizing, Pakistan has become a soft target of hybrid warfare, and has been among top countries in terms of cyberattacks due to the lack of government's focus and will towards cyber security.

Hybrid Warfare

Today, Pakistan is one of the top countries which is affected by the threats of hybrid

warfare, as the majority of its population is using social media platforms as the main source of sharing and gaining the information flows without checking its validity. As per 2020 report of Pakistan's internet landscape, amongst all social media platforms, Facebook is used by more than 85% of its population and twitter is used by 10% of its population for the acquisition of information (Haque, 2021). As a result of it, the masses of Pakistan is highly susceptible and exposed to manipulated information and campaigns of propaganda. The fusion of cyberattacks with hybrid warfare has intensified the influence of insecure information flows in the society, such can be seen in the cyberattacks of NBP and FBR (Abdyraeva, 2020). These attacks were carried out with an aim of generating a deficit of trust between the government and its population and to lead towards instability by anti-state groups (Baloch, 2019).

Since the boom of ICTs and internet, India has been running the main disinformation and propaganda campaigns against Pakistan to malign it worldwide, according to Pakistan's internet landscape report of 2020 (Haque, 2021). Thereby, creating chaos and instability within the internal structure of Pakistan. Furthermore, these campaigns are being used to exaggerate minor incidents into major incidents in order to create sentiments in the masses to stand out against their government. In the recent past, such can be seen in twitter where a fake news was circulated about the cyberattacks on different banks including NBP to force the masses to take out all their assets from banks to disrupt Pakistan's financial system (Baloch, 2021). Hence, the exposed critical information flows of Pakistan are gathered due to lack of resiliency in cyber infrastructure and policy intending to use it as a tool of hybrid warfare to create chaos in the domestic affairs of Pakistan by influencing the minds of the masses.

Cyber Security Policy

Pakistan as an active and new member of cyber world, has been under the process of formulating and executing cyber security approaches to curb and protect its critical information flows from cyberattacks and the impact of hybrid warfare. Since the launch of Pegasus spyware as an advanced cyberattack, Pakistan has devised and approved its first national level cyber security policy in 2021 (Safdar, 2021). This newly devised policy highlights and focuses on devising of resilient cyber measures and the promulgation of cyber ordinance and laws with the purpose of making cyber infrastructure strong (Khan, 2021). However, Pakistan as the member of cyber community, is late in devising a national level policy as compared to its counterpart India which has recently devised its fourth national cyber security policy. Though, Pakistan has devised its policy, but it only covers those measures which can only be able to curb traditional threats of cyberattacks and hybrid warfare and would be ineffective in catering advanced persistent threats (APTs) i.e. Pegasus spyware (Khan, 2021; Safdar, 2021).

Currently, Pakistan lacks essential such as certified software, indigenous protocols and products, secured communication channels and trained manpower, for resilient cyber infrastructure which is making a detrimental situation for Pakistan to devise an inclusive policy. Today, a simple cyber policy with no advanced cyber strategies is not effective enough to curb the ever-changing threats of cyberattacks and hybrid warfare. Due to which formulating and implementing a cyber governance model is in the need of hour by considering Chinese cyber governance as a base model. This model would not only curb the prevailing threats, but would also focus more on the development of indigenous IT products, as Pakistan has always been dependent on foreign IT products for the information flows to get stored and shared. Thus, providing opportunity to state and non-state actors to disrupt and manipulate information flows due to implanted bugs in these foreign IT products.

It is the right time for Pakistan to devise a cyber governance model like a Chinese cyber governance model by replicating all the points that are feasible in current socio-politico-economic structure and by modifying it in terms of linking cyber security with national security,

developing domestic industries, allowing citizens maximum use of internet, executing network gateways and promulgating of cyber ordinance and laws. Hence, Pakistan needs a holistic cyber security policy with all the prerequisite of resilient cyber infrastructure along with the modified cyber governance model as per its democratic and political structure in order to mitigate and curb the threats of cyberattacks and hybrid warfare.

6. Conclusion

Information flows are the national assets and are of immense important for Pakistan's national security, and leakage of such information through cyberattacks may lead to hybrid warfare. This article has pointed out on the basis of review different researchers and articles, the significance of information flow, the ever-changing cyberattacks, the repercussion of hybrid warfare on the masses, and possibility of Chinese cyber governance model's applicability. The respondents has shed light on the provocations that Pakistan is currently facing in its cyber sector and the influence hybrid warfare creates on the masses through propaganda and disinformation. On the basis of respondents' insights, it can be concluded that Pakistan is susceptible to almost all threats of cyberattacks and hybrid warfare due to fragile cyber infrastructure that has been main reason in creating instability and mistrust in the society.

Furthermore, the article also highlights the need of holistic approach such as cyber governance model based on Chinese cyber governance model under comprehensive cyber security policy that is feasible for socio-political-economic structure of the country. As it would be in the national interest of Pakistan due to the effectiveness this model would offer i.e. proper securing of critical information flows, establishing of domestic IT industries, and maximum usage of cyberspace, training of manpower, technological inclusion, and linking cyber security as the core element to national security.

Acknowledgements

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

REFERENCES

Abdyraeva, C. (2020). The Use of Cyberspace in the Context of Hybrid Warfare: Means, Challenges and Trends.

Akram, M. M. U., Asif, N., Abdullah, M. T., & Sarwar, M. U. (2011). Effective Enforcement of Cyber Laws in Pakistan. International Journal of Science and Technology, 1-15.

Aptsiauri, K. Social Media as an Instrument of Waging Hybrid Warfare. In 7th EURASIAN MULTIDISCIPLINARY FORUM, EMF 2017 6-7 October, Tbilisi, Georgia (p. 238).

Ali, K. (2021, July 28). Cabinet gives the green light to cyber security policy. DAWN.COM. https://www.dawn.com/news/1637334

Babar, S. I., & Mirza, M. N. (2020). The Indian Hybrid Warfare Strategy: Implications for Pakistan. Progressive Research Journal of Arts & Humanities (PRJAH), 2(1), 39-52.

Baloch, R. Cyber Warfare Trends, Tactics and Strategies: Lessons for Pakistan.

Baloch, R. (2021). NBP Cyber Attack - Insights. Facebook https://www.facebook.com/unsupportedbrowser

Benthall, S. (2019, April). Situated information flow theory. In Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (pp. 1-10).

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101.

Chenou, J. M. (2021). The contested meanings of cybersecurity: evidence from post-conflict Colombia. Conflict, Security & Development, 21(1), 1-19.

Chowdhury, A. (2016, October). Recent cyber security attacks and their mitigation approaches– an overview. In International conference on applications and techniques in information security (pp. 54-65). Springer, Singapore

Daniele, C., & Giles, H. (2009). Cloud Computing: Benefits, risks and recommendations for Information security. 2012-03-21]. http://www. enisa. europa. eu.

Da Silva, F. S. C., & Agusti-Cullell, J. (2008). Information flow and knowledge sharing. Elsevier.

Dawn.com. (2020, December 3). Pakistan being subjected to 5th-generation warfare in 'massive way' but we are aware of threats: DG ISPR. https://www.dawn.com/news/1593804

DARICILI, A. B., & ÖZDAL, B. (2018). Analysis of the Cyber Security Strategies of People's Republic of China. Güvenlik Stratejileri Dergisi, 14(28), 1-35.

Devereux, H. (2019, June). Data-Driven Cyber Prediction in Hybrid Warfare. Arts.

Dowse, A., & Bachmann, S. D. (2019). Explainer: what is 'hybrid warfare 'and what is meant by the 'grey zone'? The Conversation, 17.

Egloff, F. (2017). Cyber security and the Age of Privateering. Perkovich/Levite (Hg.): Understanding cyber conflict. Fourteen analogies. Washington, DC, 231-247

Goffman, E. (1970). Strategic interaction (Vol. 1). University of Pennsylvania Press

Haider, M. W., Azad, T. M., & Ahmad, R. (2020). A Critical Analysis of Strategies to Counter Hybrid Warfare: Way Forward for Pakistan. ASIAN Journal of International Peace & Security (AJIPS), 4(2), 295-310.

Hayat, R. (2021) Hybrid Warfare: A Challenge to National Security. PCL Student Journal of Law, Vol V:1.

Haque, J. (2021). Internet Landscape of Pakistan 2020 | Bytes for All, Pakistan. Https://Bytesforall.Pk/Publication/Internet-Landscape-Pakistan-2020

Khan*, A. (2021, August 17). Pakistan's National Cyber Security Policy 2021: What Is Achieved and What Is Yet to Achieved – OpEd. Eurasia Review. https://www.eurasiareview.com/17082021-pakistans-national-cyber-security-policy- 2021-what-is-achieved-and-what-is-yet-to-achieved-oped/

Kshetri, N., & Kshetri, D. N. (2016). Quest to Cyber Superiority (pp. 107-120). Springer.

Lenz, R. (2019). Big Data: Ethics and Law. Available at SSRN 3459004.

Lipson, H. F. (2002). Tracking and tracing cyber-attacks: Technical challenges and global policy Issues. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Li, Z., Guo, X., & He, Q. (2020). A Study of Chinese Policy Attention on Cybersecurity. IEEE Transactions on Engineering Management.

Meltzer, J. P. (2015). The Internet, Cross-Border Data Flows and International Trade. Asia & the Pacific Policy Studies, 2(1), 90-102.

Naseer, D. R., & Amin, D. M. (2020). Cyber-threats to strategic networks: Challenges for Pakistan's security. South Asian Studies, 33(1).

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. International journal of qualitative methods, 16(1), 1609406917733847.

O'reilly, M., & Parker, N. (2013). 'Unsatisfactory Saturation': a critical exploration of the notion of saturated sample sizes in qualitative research. Qualitative research, 13(2), 190-197.

Rafiq, A. (2019). Challenges of securitizing cyberspace in Pakistan. Strategic Studies, 39(1), 90-101.

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward. International Scientific Online Journal, 12, 21-32.

Sacks, S. (2021). China's Emerging Cyber Governance System. Center for Strategic and International Studies. https://www.csis.org/chinas-emerging-cyber-governance-system

Safdar, A. (2021, September 13). An Overview of Pakistan's Cyber Security Policies. Centre for Aerospace & Security Studies. https://casstt.com/post/an-overview-of-pakistan-s- cyber-security-policies/469

Sarkar, M. G. (2020, August). China's Cyber Governance: Between Domestic Compulsions and National Security. Https://Www.Icsin.Org/Publications/ Chinas-Cyber- Governance-between-Domestic-Compulsions-and-National-Security.

Segal, A. (2020, March 13). China's Alternative Cyber Governance Regime. U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. https://www.uscc.gov/

Singer, P. W., & Friedman, A. (2014). Cybersecurity: What everyone needs to know?

Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: creating legal and operational dilemmas. Global Change, Peace & Security, 32(3), 337-342.

Steingartner, W., & Galinec, D. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. Acta Polytechnica Hungarica, 18(3), 25-45.

Sutherland, B. (2011). The economist: Modern warfare, intelligence and deterrence.

Ştefănescu, D. C. Is hybrid Warfare a New Manner of Conducting Warfare? Review of the Air Force Academy, 14, 155-160.

Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013, December). Cyber threats and incident response capability-a case study of Pakistan. In 2013 2nd National Conference on Information Assurance (NCIA) (pp. 15-20). IEEE

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (pp. 307-311). IEEE.

Yamin, T. (2018). Cyberspace Management in Pakistan. Governance, 3(1), 46-61.

Yasin, B. M. (2020). Hybrid Warfare: Countering the Impending Threats

IEER
Institute of Excellence in Education & Research