# Evaluating the Nature of Cyber Warfare between Pakistan and India

Summar Iqbal Babar, Muhammad Nadeem Mirza, Irfan Hasnain Qaisrani

Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

# Evaluating the Nature of Cyber Warfare between Pakistan and India

**Summar Iqbal Babar[1] , Muhammad Nadeem Mirza[2] , Irfan Hasnain Qaisrani[3]**

[1]Faculty Member School of Politics and International Relations Quaid-i-Azam University Islamabad.

[2]Faculty Member School of Politics and International Relations Quaid-i-Azam University Islamabad, ORCID (https://orcid.org/0000-0002-2196-9174)

[3]Faculty Member Department of Humanities and Social Sciences Bahria University Islamabad.

---

**Abstract**

Cyber security threats are one of the primary factors revolving around modern states' national security in the twenty-first century. Cyberspace and digital networks have drastically revolutionized modern security landscape as well as threat spectrum. The growing reliance on information and communication technologies have developed digital frontier as new domain in warfare and critical national security concern. Given the nuclear deterrent as balancing act for strategic stability in south Asian region, cybersecurity has become more prudent threat, militarized the cyber space with proliferating cyber-arms culture. India's aspirations to modernize her military through equipping with cutting-edge disruptive technologies for an operational imperative has posed serious threat to Pakistan. With varying forms of targeted financial losses, hacking of state's classified data, malfunctioning of state infrastructures of critical value, phishing and ransomware are evolving potential threats in cyber domain, endangering fiscal economy as well national security of Pakistan. India is rapidly developing its offensive cyber capabilities by enhancing its cooperation with Israel and the US in this realm. Both the United States and Israel have advanced cyber capabilities. The growing Indian capabilities will thus pose a serious challenge to Pakistan in the cyber realm. This study explores on evolving cyber warfare, enhancing strategic vulnerabilities through integrating cyber-arms between Pakistan and India. It further aims in assessing Pakistan's relative capabilities to match India's fast-paced digitisation, cyber-arming, and retaliatory muscles.

**Keywords:** Cyber Warfare, Cybersecurity, Cyber-Nuclear Security, Digitisation, India, Pakistan.

## Introduction

Cyberspace has overwhelmingly transformed modern strategic thinking, conduct of warfare and essence of state security. In modern era, it is gradually replacing existing traditional means of security with cyber-arming and cutting-edge technologies with changing manner of strategic

vulnerabilities. Cyber conflicts have become a new normal in modern hybrid warfare, with nations unleashing their digital dominance on one another. It is a highly effective and low-cost weapon of warfare that has replaced soldiers and fleets with a few keystrokes that are equally capable of wreaking wide-ranging destruction on the adversary. Many countries have made it their primary weapon against their enemies. Pakistan, too, is vulnerable to cyber-attacks, particularly by her arch-rival India, which is in a continuous state of conflict against it since its independence. India has increased its efforts in recent years to enhance its potential capabilities in defensive and offensive cyberwarfare (Yaqub, 2020). As India and Pakistan, both nuclear arch-rivals see it as a possible advantage that could be used to aim for the adversary's cyberspace. However, both India and Pakistan have not launched a major cyberattack on each other. Cyberattacks of lesser magnitude and scale such as growing internet vandalism and narrative building on social media platforms are becoming more common between the two neighbours.

Some high-ranking Pakistani officials' cell phones were reportedly hacked for surveillance back in 2019. WhatsApp, a social media application was hacked using a type of malware called 'Pegasus,' which was created by the NSO Group, an Israeli spyware firm. It is one of the most advanced cyberweapon as the Pegasus malware could penetrate a phone by calling on the WhatsApp number of the targeted entity, activating the camera and microphone of the cell phone, and acquiring access to its messages, contacts, emails, and passwords. This malware can also determine its location using GPS. After discovering this hacking incident, It was reported that Pakistan is working to develop an alternative application, like Whatsapp that can guard classified and sensitive communication. (Qadeer, 2020). The preparators behind the attack on Pakistani officials are still unknown. However, when it became known that India's intelligence agencies were also making use of Pegasus to spy on different leaders of opposition political parties, lawyers and human rights activists, and civil society members who are critic of incumbent government, it became a matter of serious concern for Pakistani officials.

**Theorizing Cyber-Realism**

The rapid proliferation of Information and Communication Technology has brought the digital frontier as an increasingly significant warfare domain that has revolutionized the strategic thinking and the conduct of war (Mirza et al., 2021). It further has expanded the strategic worldview and scholarly orientation of security studies in International Relations by revitalizing the realist paradigm in the post-cold-war era (Valeriano & Craig, 2018). With varying forms of targeted financial losses and theft of restricted government information, malfunctioning of important state infrastructures and cyber security puts forward a considerable challenge to the economic and national security of countries worldwide. The Cold War security-dominated discourse by the realists is further substantiated by the evolving digital disorder and lacking central governing authority as they say, "Cyberspace has become a new international battlefield" (Petallides, 2012).

The concept of cyber-realism entails that cyber threats be considered as a geopolitical and national security priority and thus utilize all the available means to coerce the adversaries to change their behavior. A nation-state in the cyber realm is only threatened by its adversaries whether other nation-states or terrorist groups (Kegley & Raymond, 2021). For example, a

large number of cyber-attacks against Ukraine emanated from its adversary Russia. So, for a state to effectively counter cyber threat they must consider their broader geopolitical goals. Cyber-realism thus proposes that Offensive or Defensive capabilities developed by a state will not be enough for a state to counter its adversaries in the digital realm. Only, a balance of power in the digital realm much like the one in the geopolitical realm can deter states from carrying out cyberattacks against each other (Mirza et al., 2021).

**Definitional Issues**

Technology with its fast-paced and ever-changing character has revolutionized every sphere of human life. It has arguably altered the means and reshaped the future wars and strategic calculus. These technological advancements in the sphere of cyberwarfare have transformed the communication and information mediums and mechanisms which are expanding its operational domain, tactical approach, and countermeasures. It has evolved over the time with its multi-faceted character and introduced new forms of threats. As it is expanding its scope, more it requires bringing clarity in its forms, definitions for better understanding and tactful responses. This section of the study details some of the definitional puzzles relevant to cyberwarfare. "Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems" (Gibson, 1982, 1984; Ottis & Lorents, 2010).[1] Cyberspace is an artificial space made by humans and for human purposes (Mirza et al., 2021; Ottis, 2011). Cyber security, on the other hand, talks about the protection of networks, devices, programmes, and data from attack, damage, and illegal access by a variety of technologies, procedures, and best practices (Perwej et al., 2021). Cyber-attacks are 'Any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or disruption of the services or access to the information of the said national cyber asset is called cyber-attack. Intentional use of a cyber-weapon against an information system in a manner that causes a cyber-incident is also considered cyber-attack' (Jamal et al., 2021). Cyber Terrorism is 'a purposeful act, personally or politically motivated, that is intended to disrupt or destroy thestability of organizational or national interests, through the use of electronic devices which are directed at information systems, computer programs, or other electronic means of communications, transfer and storage' (Desouza & Hensgen, 2003; Hensgen et al., 2003). Cyberterrorism aims to compromise electronic systems to elicit fear. Cyber terrorism is defined as the practice of terrorist organizations and individuals using digital technology to advance their goals. This might involve the planning and execution of attacks on networks, computer systems, and telecommunications infrastructures, as well as the electronic exchange of information and the making of threats (Florakis et al., 2020). Examples include gaining access to computer systems through hacking, infecting weak networks with viruses, defacing websites or making terroristthreats via electronic communication. A cybersecurity risk is defined as any risk including potential financial loss, business interruption, or harm to an organization's reputation as a result of failure, unauthorized, orimproper usage of its computer systems. Due to the increased reliance on computers, networks, software, social media, and data internationally, organizations are becoming increasingly susceptible to cyber threats (Florakis

et al., 2020; What Is Cyber Risk?, 2021).

**Digital Frontiers of Modern Warfare**

Digitalization has been the hallmark of 21st Century. Every nation-state has a sizeable number of its population connected to the cyberspace. Digitalization has its impact on all the aspect of human life, from agriculture to communication, and medicine to military. In the realm of warfare cyber has emerged as fourth domain besides air, naval, and military. In cyberspace the threats can emanate from both, state institutions as well as non-state actors. The modus operandi can range from offensive cyberattacks to propaganda (Schia, 2018). Offensive cyberattacks can target critical infrastructure of a state whereas propaganda tools can be used to exploit existing fault lines within the state. These fault lines can be social, religious, or cultural. Also, cyberweapons are cheaper than conventional weapons. Exploiting vulnerabilities in digital systems through malicious codes or buying zero-days in the underground cyber market can empower cyber capabilities of a state (D. E. S. Perlroth Nicole & Shear, 2015; N. Perlroth, 2021; Shane et al., 2017). Also, social media is becoming a modern tool of propaganda with unprecedented impact. In past, propaganda tools could have been censored and controlled by governments. However, in present day world apps like Facebook, Twitter and YouTube are not easy to control or censor. Also, they are the platform that can be used by adversary states to exacerbate the existing vulnerabilities of a state. Fake news has emerged as a weapon of unparalleled tool in the modern warfare (Horowitz, 2019). The first instance of a digital war was observed in 2008 when Russia attacked Estonia. With a series of denial of services attacks it took much of the country's digital system offline pushing the country into a state of panic (McGuinness, 2017). Also, in the current Russo-Ukraine war cyberweapons are being utilized with impunity by the former.

**Evolving Cyber-Culture in South Asia**

Cyberculture can be defined as, 'a set of technologies, material and intellectual, practices, attitudes, modes of thought and values developed along with the growth of cyberspace, a non-place where people from several places, with pretty different cultures, values of all sorts and habits, coexist and communicate' (Gómez-Diago, 2012). In India and Pakistan, the number of cybernetics is increasing at an exponential rate. According to world bank data, the number of internet users in Pakistan was 10% of the total population in 2014, however, the number has stood at 25% in 2020 data. In India, the number of users was 14% in 2014 and has reached a staggering 43% in 2020 (WB, 2020). The growth of cyberspace, however, highlighted the need of developing a strong cybersecurity culture which means states need to protect their data and privacy.

**Cyber-Nuclear Security**

Digitalization has linked all the industries and critical infrastructure to cyberspace. It provides with immense potential to these industries however also enhancing its vulnerabilities. Every sector from transportation to telecommunication, banking and finance to defense industry and nuclear plants are digitalized. Nuclear plants are weapons are increasingly being modernized to increase their efficiencies. However, cyberthreats at the same time brings new challenges to

the tables. The threat presented by cyberattacks on the command, control, communication, computing, and intelligence (C4I) structure is the first challenge. The C4I structures' vulnerabilities are growing as digital technologies are more and more integrated into them for effective communication, evaluation, reliability, and efficiency.

A state's early-warning satellites and radars may also be in danger from cyberattacks. This could make the state more susceptible to a nuclear attack. This can be accomplished by spoofing, whereby radar systems can produce false positives and have their reliability called into doubt. This can also take the form of blindness, where the system issues false negatives and is unable to identify enemy missiles or aircraft.

Cyberweapons can pose to the adversary's operational units, delivery systems, and nuclear warheads a significant threat. Attacks on the command-and-control systems or the supply chain may lead to a failed launch, self-destruction, or inaccurate nuclear warheads. This poses a serious threat to strategic stability because it could eliminate a state's nuclear capability, making its nuclear weapons useless. Important point here remains that these cyberweapons have the least chance of getting detected by the adversaries. Here, the distinction between the developed and developing states becomes evident. While the developed states have strengthened their cyber systems in order to protect themselves against the cyberattacks and cyberweapons, the developing states are lagging far behind in the race. And even if they are trying to strengthen themselves, that is something for which they are relying upon the imports of the high-tech equipment from the developed states. in other words, they are opening up their critical infrastructure, such as the telephone networks and communications to other states, who can exploit these states with very ease.

Another potential threat to strategic stability is cyber spoofing. Spoofing is the practice of interfering with communications by posing as the original sender or source. Critical infrastructure and physical structures can also be attacked by cyberweapons over the internet (Mirza et al., 2021). They have the ability to damage actual nuclear facilities as well as assault crucial nuclear structures. A Stuxnet attack is an illustration of a cyberattack on a nuclear facility (Farwell & Rohozinski, 2011; Zetter, 2014).

Pakistan is also rapidly connecting its critical infrastructure to cyberspace. Digital banking is an illustrious example. However, its cybersecurity capabilities are nascent in comparison (Safdar, 2021). Pakistan is a nuclear weapon state and thus needs to rapidly enhance its cyber capabilities to thwart any threats to its nuclear facilities. According to Symantec, one of the leading cybersecurity firm, Pakistan is one of the most targeted states. A malware programme dubbed "Secondate" was used by the NSA to monitor Pakistan's civilian and military officials, according to Snowden papers published between 2013 and 2014 (Appelbaum et al., 2015; Desk, 2016b; Staff, 2013). Through the Rising Threat Intelligence System, the Rising Security Research Institute was able to intercept the attack carried out by the well-known Advanced Persistent Threat (APT) group "Rattlesnake" in the year 2019 (Khalil, 2020). This time, the group used the Target collision hijacking technique to attack the Pakistani Navy. The endeavour was specifically made to steal sensitive information from protected military networks while planting deceptive papers that seemed to be official remarks from the Pakistan Navy against its neighbours, namely China and India. RAW-sponsored groups have been

caught in Karachi and other parts of Pakistan which have been involved in fueling terrorist and propagation activities against Pakistan (Desk, 2016a; Mandhro, 2021; News, 2020).

India has a fixed a huge budget for the technological sector to enhance expectations in the cyberspace to counter various challengers and overcome strategic contenders in the region. The cyberspace collaboration of Israel and India has brought more dividends for the latter. India tried to maintain ascendancy in the field of technology through its National Cyber Security Policy which was established in 2013. India, in the recent years, designated a considerable amount of budget for research work in cyberspace. India allocated an 8% budget for advancement in cyberspace along with 2,58,589 crores for defense budget (Naseer & Amin, 2018). This budget has increased several folds since 2018.

In the 1990s, the Indian military went through a paradigm shift in its strategic thinking and brought cyber warfare and technological advancements in information and communication to its core policy. This policy facilitated the modernization of four military components, development of network centric warfare, the basic structure of security, information technology, and armed force flexibility. India and United States were also signatories of a memorandum of understanding (MOU) that empowers operational and technical cooperation to counter the cyber threats (Office of the Press Secretary, Department of Homeland Security, 2011).

**Cyber tit-for-tat between Pakistan and India**

Pakistan is vulnerable to cyberattacks from its adversaries. Its cybersecurity preparations are questionable. There had been major incidents of cyberattacks in Pakistan's history albeit on a low scale. So far, the damage has only been in the digital space and not in the physical space. Cyber-attacks are non-kinetic attacks, but they can trigger kinetic responses.

Pakistan is one of the top 10 most targeted countries in the world, according to Symantec, which manages the most comprehensive civilian database of events (Desk, 2019; Khalil, 2020). With publicly documented attacks on a range of telecommunications, banking, government, health, transport, utility, and ride-sharing firms, Pakistan's nuclear and other critical installations are likely the target. The NSA was deploying malware known as SECONDATE to spy on Pakistan's civilian and military leadership, according to Snowden data (Desk, 2016b; Staff, 2013).

A list of major cyber incidents in Pakistan is below. Most recently, the nation's tax collection agency experienced a cyber security vulnerability because of Microsoft Hyper-V software that was not promptly updated. The facts of the breach revealed that, despite the hackers' inability to fully exploit the system, they were nevertheless able to steal taxpayers' private information and temporarily halt FBR's activities. During the attack on the FBR data center, all official websites run by the tax machinery were down for more than 72 hours. While FBR's official website and features related to taxes were restored, hackers proposed to sell the FBR's data on a Russian forum for $30,000 (M. Z. Khan, 2021; Rana, 2021).

K-Electric, the organisation in charge of Karachi's electricity generation, transmission, and distribution, was the target of a cyberattack in 2017. Attackers threatened to release information of clients which included their names, home addresses and credit card numbers, Tax returns

and CNICs, details of bank accounts, on the dark web unless the management would pay a $7 million ransom. Millions of K-Electric customers might be exposed to internet dangers if hackers sold this data on the dark web. This attack also negatively impacted the company's internal operations, including banking and communication lines. When the KE refused to comply with the hackers' requests, they posted about 8.5 GB of the stolen data on the dark web, endangering many users (Abrams, 2020). Such attacks have also been directed at the banking industry. In February 2019, 69,189 bank cards from Meezan Bank were put on the dark web for sale. The bank lost $3.5 million worth of data due to the data breach. But according to reports, the bank's management reacted quickly and asked its clients to update their information, particularly their PIN code, as well as other security measures, to protect them from losses. Consumers were protected from financial losses, but the banking system's vulnerabilities were made clear (Ullah, 2021; Zaidi, 2019). Pakistan's banking sector experienced a distinct type of cyberattack in November 2018. Nearly 20,000 banking users were affected by the breach of data affecting almost all Pakistani banks, which resulted in considerable financial losses for the banks. For instance, according to a report from BankIslami, the attack cost the bank millions in losses and resulted in the suspension of several operations, most notably the online banking facility (Iqbal, 2018). The breach was primarily directed at debit card customers who received automated text messages from the system informing them of cash withdrawals from their accounts. Additionally, hundreds of debit card numbers belonging to bank customers were also placed for sale on the dark web. Due to this hack, the dark web received information on roughly 11,000 debit cards from 22 Pakistani banks (Iqbal, 2018; Staff, 2018).

ISPR, the spokesperson of Pakistani military in August 2020 announced that the country's intelligence apparatus had unearthed a plot by Indian intelligence agencies. According to this a cyberattack on the cell phones and other devices of Pakistani government officials and military personnel was being employed to hack them. Moreover, in October 2021, Shaukat Tarin, the minister of finance, informed the National Assembly that the Federal Board of Revenue (FBR) websites saw 71,000 cyberattacks on average per month. He stated in a written response that FBR's systems were compromised three times during the last three years (February 18, 2019, to February 22, 202; March 23, 2021; April 13, 2021, to August 19, 2021). (around 0.001pc success rate) (M. Z. Khan, 2021).

By six Indian groups of the Indian Cyber Army, thirty government websites were compromised in December 2010. Later, they claimed that websites for the National Accountability Bureau, finance, education, Pakistan Navy, and NADRA were among those that had been compromised. These websites were hosted on the same server, which made them vulnerable to hacking. The Indian hackers then posted messages to all websites that they hacked websites as a befitting counterattack for the Mumbai attacks on 26/11. Pakistan takes down websites with this kind of cyber-message (Leyden, 2021). However, after 2001, both sides carried out such attacks.

**Indian Collaborations with US and Israel**

Considering India's ever-increasing cybersecurity cooperation with Israel, the threat of Indian cyberattacks against Pakistan has grown more serious. Israeli Prime Minister Benjamin Netanyahu spoke at 9th Annual International Cybersecurity Conference and said, 'I set the goal for Israel of becoming one of the top five cybersecurity powers in the world... It's a goal we've achieved.' 'When it comes to cybersecurity, Israel has invested more than any other country proportionally,' he said (Mustafa et al., 2020). Indian policymakers are looking towards Israel's Talpiot training program, the first one in the world. The Israeli Defence Forces use this program to hire the country's most gifted and innovative youth and then teach them advanced mathematics, physics, and computer science. It is well-known for bringing up experts who support the Israeli military's R&D and cybersecurity efforts (Mustafa et al., 2020).

Despite a 'sharp increase in Chinese activity against Indian networks,' India's offensive cyber potential is 'Pakistan-focused' and 'regionally effective,' rather than being focused towards China, according to a new report by the International Institute for Strategic Studies (IISS), a well-reputed think tank with its considerable policy influence. According to Greg Austin, the head of the IISS' cyber program, 'India has some cyber-intelligence and offensive cyber capabilities, but they are regionally focused, primarily on Pakistan' (IISS, 2021; Mihindukulasuriya, 2021). It is presently attempting to compensate for its shortcomings by developing upgraded new capabilities with the assistance of important international partners such as the United States, the United Kingdom, Israel, and France, as well as by pursuing concerted international action to develop restraint norms.

Despite the South Asia's 'geo-strategic instability' and a 'keen awareness' of the cyber threat, the report claims that 'India has made only modest progress in developing a cybersecurity policy' (IISS, 2021; Nachiappan & Rajeev, 2021). It went on to say that India's reform of cyber governance has been 'slow and incremental,' with notable coordinating cybersecurity authorities in civil and military domains only being established in 2018 and 2019. 'India has a good regional cyber-intelligence reach, but it relies on partners, including the US, for broader insight' (IISS, 2021; Mihindukulasuriya, 2021). The IISS report went on to say that India's best chance of moving up to the second tier of cyber powers is 'by harnessing its great digital-industrial potential and adopting a whole-of-society approach to improving its cyber security,' noting that 'the private sector has moved more quickly than the government in promoting national cyber security' (IISS, 2021; Mihindukulasuriya, 2021).

**Assessing Pakistan's Relative Capabilities**

Hackers are encouraged to misuse and disrupt usage of the developing cyberspace, which includes greater use of telecommunications (Telecom) and information technology (IT). Hackers have now got the capability to attack and conduct sabotage activities by destroying or disrupting the national important infrastructures such as banks, electricity grid, and even military command and control systems (Mirza et al., 2021). In recent years, infrastructure and services have been the target of millions of cyberattacks. Ransomware was frequently used by hackers to demand money from its victims. Therefore, it is crucial that Pakistan acquire the capacity to both defend against and conduct counter-cyberattacks. Since it is frequently

challenging to identify the attacker, this is easier said than done. It is feasible to hide behind the internet's open infrastructure due to its nature. This specifically is the situation when states sponsored hackers launch attacks against other states' infrastructure.

Nevertheless, nations must put in place strong cyber security measures. Networks, computers, programmes, and data are all protected using a variety of technologies, procedures, and best practises known as cyber security. As technology is not stagnant but advances at an expedious pace, devices of household use will become vulnerable to hacking and disruption. As a result, cyber security is a broad field that will be difficult to master. The art of war has seen considerable modifications during the past century for both governments and non-state actors. The "information age" of our century is becoming more and more popular, but it is not without its problems. The possibility of cyber security breaches increases rapidly and can do serious harm as the world becomes increasingly dependent on the internet, interconnection, and technology. Pakistan is also susceptible to online threats. It is not surprising that Pakistan is also facing a dilemma in the online. Cyberspace has impacted Pakistan's banking, education, telecom industry, military, and governmental sectors.

**Prevention of Electronic Crimes Act, 2016**

Pakistan is mindful of the cyber threats that it faces. To counter these threats and challenges, the Prevention of Electronic Crimes Act, which proposes penalties for cyber offenders, was passed in 2016 (Syed et al., 2019). Unauthorized access to information systems, as well as unauthorized copying of any data, access to any critical infrastructure, electronic fraud, tampering with communication information, offenses against person modesty or decency, writing malicious codes or their transmission, cyberstalking, hate speech, or glorification of an offense, are all punishable offenses under the Act (Prevention of Electronic Crimes Act, 2016, 2016). For these offenses, the Act proposes both fines and jail terms (Khalil, 2021; Prevention of Electronic Crimes Act, 2016, 2016). A provision is also made for Computer Emergency Response Teams, which would consist of personnel with expertise in cyber security on critical infrastructure or information data. Similarly, officials from intelligence agencies will be included in these teams (Prevention of Electronic Crimes Act, 2016, 2016). The Act also proposes international cooperation in this area to thwart or initiate cyber security threats. The act itself has been hailed by some as a watershed moment, while others have criticized it as a draconian law that would limit citizens' rights, such as free speech, and grant additional powers to government agencies and departments (Prevention of Electronic Crimes Act, 2016, 2016). Many civil society organizations and politicians have expressed concern about the document's language, which allows agencies and departments to exploit it. Human rights experts advocate for a balance of security and human rights.

**Conclusion**

To deal with cyber threats, the government must invest in modernizing its agencies. There is no single agency or organisation focused on bolstering Pakistan's cybersecurity capabilities. Pakistan needs a full-fledged cyber-security organisation to defend the nation from digital threats. For instance, the National Cyber Security Authority (NCSA) in Israel and the Cybersecurity and Infrastructure Security Agency (CISA) in the United States both exist.

In Pakistan, the Federal Investigation Agency (FIA) has a unit called the National Response Centre for Cyber Crime (NR3C) that deals with cybercrime, but it lacks the resources, personnel, and equipment necessary to safeguard the nation's vital infrastructure.

Pakistan also lacks sufficient cyber threat protection legislation. In Pakistan, the Prevention of Electronic Crimes Act, 2016, was approved in 2016, although it does not address several important cybersecurity issues (Prevention of Electronic Crimes Act, 2016, 2016). Pakistan needs stricter cybersecurity laws that mandate companies and organisations defend their computer networks and data from hackers. Government organisations, the energy sector, as well as healthcare and financial institutions, should all be required by rules to safeguard their computer systems and data. These precautions are especially crucial today that practically all organization's systems are online and rely on big data analytics and artificial intelligence. As a result, hackers find them to be an appealing target. On the other side, cybersecurity specialists contend that businesses won't make investments in cybersecurity unless governments make them. Pakistan must acknowledge the serious threat to its vital infrastructure and take serious measures to protect the nation's linked infrastructures. It is crucial to determine whether national infrastructure is still essential for the economic and national security of Pakistan. In conclusion, it is crucial for Pakistani authorities to recognise present and potential cyber risks and create an appropriate cybersecurity plan. Without competent management of these challenges, Pakistan cannot guarantee complete national and economic security.

## References

Abrams, L. (2020, October 1). Hackers leak files stolen in Pakistan's K-Electric ransomware attack. Bleeping Computer. https://www.bleepingcomputer.com/news/security/hackers-leak-files-stolen-in-pakistans-k-electric-ransomware-attack/

Appelbaum, J., Gibson, A., Guarnieri, C., Müller-Maguhn, A., Poitras, L., Rosenbach, M., Ryge, L., Schmundt, H., & Sontheimer, M. (2015, January 17). NSA Preps American for Future Battle: New Snowden Docs Indicate Scope of NSA Preparations for Cyber Battle. Der Spiegel. https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html

Desk. (2016a, April 18). RAW network operating in Karachi University busted. 92 News HD. https://92newshd.tv/about/raw-network-operating-in-karachi-university-unearthed

Desk. (2016b, August 21). NSA used malware to spy on Pakistani civilian, military leadership: Report. Dawn. http://www.dawn.com/news/1279013

Desk. (2019, February 13). Pakistan ranked among least cyber secure countries. The Express Tribune. http://tribune.com.pk/story/1909680/pakistan-ranked-among-least-cyber-secure-countries

Desouza, K. C., & Hensgen, T. (2003). Semiotic emergent framework to address the reality of cyberterrorism. Technological Forecasting and Social Change, 70(4), 385–396.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Florakis, C., Louca, C., Michaely, R., & Weber, M. (2020). Cybersecurity Risk: Working Paper Number 2020-178. Becker Friedman Institute, University of Chicago.

Gibson, W. (1982). Burning Chrome. Harper Voyager.

Gibson, W. (1984). Neuromancer. The Easton Press.

Gómez-Diago, G. (2012). Cyberspace and Cyberculture. In Encyclopedia of Gender in Media (pp. 58–60). Sage Reference.

Hensgen, T., Desouza, K. C., Evaristo, J. R., & Kraft, G. D. (2003). Playing the "cyber terrorism game" towards a semiotic definition. Human Systems Management, 22(2), 51–61.

Horowitz, M. A. (2019). Disinformation as Warfare in the Digital Age: Dimensions, Dilemmas, and Solutions. Journal of Vincentian Social Action, 4(2). https://scholar.stjohns.edu/jovsa/vol4/iss2/5

IISS. (2021). Cyber Power—Tier Three: India. In Cyber Capabilities and National Power: A Net Assessment. International Institute for Strategic Studies. https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-three

Iqbal, S. (2018, October 30). Cyber attack costs BankIslami Rs2.6m. Dawn. https://www.dawn.com/news/1442324

Jamal, A. A., Majid, A.-A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2021). A review on security analysis of cyber physical systems using Machine learning. Materials Today: Proceedings.

Kegley, C. W., & Raymond, G. A. (2021, April 26). Realism in the Age of Cyber Warfare. Ethics & International Affairs. https://www.ethicsandinternationalaffairs.org/2021/realism-in-the-age-of-cyber-warfare/

Khalil, B. (2020, February 16). Emerging Cyber warfare threats to Pakistan. Daily Times. https://dailytimes.com.pk/558883/emerging-cyber-warfare-threats-to-pakistan/

Khalil, K. (2021). Cyber Security In Electronic Banking and Its Impact Upon Electronic Banking Financial Performance: Intervening Role of Product Innovation [Thesis, Iqra National University, Peshawar.]. http://prr.hec.gov.pk/jspui/handle/123456789/17574

Khan, M. Z. (2021, October 1). 71,000 cyber attacks made on FBR portals every month: Tarin. Dawn. https://www.dawn.com/news/1649393

Leyden, J. (2021, June 30). Indian cyber-espionage activity rising amid growing rivalry with China, Pakistan. The Daily Swig: Cybersecurity News and Views. https://portswigger.net/daily-swig/indian-cyber-espionage-activity-rising-amid-growing-rivalry-with-china-pakistan

Mandhro, S. (2021, January 14). Karachi police arrest Raw-linked terrorist. The Express Tribune. http://tribune.com.pk/story/2279936/karachi-police-arrest-terrorist-allegedly-supported-by-raw

McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia. BBC News. https://www.bbc.com/news/39655415

Mihindukulasuriya, R. (2021, June 28). India's offensive cyber capability more focused on Pakistan than China, UK think tank says. The Print. https://theprint.in/india/indias-

offensive-cyber-capability-more-focused-on-pakistan-than-china-uk-think-tank-says/685774/

Mirza, M. N., Ali, L. A., & Qaisrani, I. H. (2021). Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order. Webology, Volume 18(No. 5), 598–610.

Mustafa, G., Murtaza, Z., & Murtaza, K. (2020). Cyber Warfare between Pakistan and India: Implications for the Region. Pakistan Language and Humanities Review, 4(I), 59–71. https://doi.org/10.47205/plhr.2020(4-I)2.05

Nachiappan, K., & Rajeev, N. (2021, July 22). India as a Muddling Cyber-Power – NUS Institute of South Asian Studies (ISAS). Institute of South Asian Studies (ISAS), National University of Singapore. https://www.isas.nus.edu.sg/papers/india-as-a-muddling-cyber-power/

Naseer, R., & Amin, M. (2018). Cyber-Threats to Strategic Networks: Challenges for Pakistan's Security. South Asian Studies, 33(1), 35–48.

News. (2020, March 19). Police arrest 'head of RAW's terror wing' in Karachi. Daily Times. https://dailytimes.com.pk/579330/police-arrest-head-of-raws-terror-wing-in-karachi/

Office of the Press Secretary, Department of Homeland Security. (2011). United States and India Sign Cybersecurity Agreement. US Government. https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement

Ottis, R. (2011). A Systematic Approach to Offensive Volunteer Cyber Militia [Tallinn University]. https://digikogu.taltech.ee/et/item/e1b673b0-df9d-4afc-a9e0-a2da53af8ab6

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and implications. International Conference on Cyber Warfare and Security.

Prevention of Electronic Crimes Act, 2016, (2016) (testimony of Pakistan Parliament). https://na.gov.pk/uploads/documents/1470910659_707.pdf

Perlroth, D. E. S., Nicole, & Shear, M. D. (2015, June 20). Attack Gave Chinese Hackers Privileged Access to U.S. Systems. The New York Times. http://www.nytimes.com/2015/06/21/us/attack-gave-chinese-hackers-privileged-access-to-us-systems.html

Perlroth, N. (2021). This Is How They Tell Me the World Ends: The Cyberweapons Arms Race (1st edition). Bloomsbury Publishing.

Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 9(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Petallides, C. J. (2012). Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat—Inquiries Journal. Inquiries Journal, 4(3). http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat#:~:text=pp.%2098%2D112-,%

Prevention of Electronic Crimes Act, 2016, (2016) (testimony of Pakistan Parliament). https://na.gov.pk/uploads/documents/1470910659_707.pdf

Qadeer, M. A. (2020, June 6). The Cyber Threat Facing Pakistan. The Diplomat. https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/

Rana, S. (2021, August 15). FBR reels under a major 'cyberattack'. The Express Tribune. http://tribune.com.pk/story/2315712/fbr-reels-under-a-major-cyberattack

Safdar, A. (2021, September 23). An Overview of Pakistan's Cyber Security Policies. Centre for Aerospace & Security Studies (CASS). https://casstt.com/post/an-overview-of-pakistan-s-cyber-security-policies/469

Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. Third World Quarterly, 39(5), 821–837. https://doi.org/10.1080/01436597.2017.1408403

Shane, S., Sanger, D. E., & Perlroth, N. (2017, October 6). New N.S.A. Breach Linked to Popular Russian Antivirus Software. The New York Times. https://www.nytimes.com/2017/10/05/us/politics/russia-nsa-hackers-kaspersky.html

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

Staff. (2018, December 22). BankIslami lost $6m within 23 minutes in cyber attack. Pakistan Today. https://profit.pakistantoday.com.pk/2018/12/22/bankislami-lost-6m-within-23-minutes-in-cyber-attack/

Syed, R., Khaver, A. A., & Yasin, M. (2019). Cyber Security: Where Does Pakistan Stand? Sustainable Development Policy Institute, Think Asia, Asian Development Bank Institute. https://think-asia.org/handle/11540/9714

Ullah, M. (2021, November 28). After HBL, Meezan Bank is under Cyber Security attack? Dispatch News Desk-DND. https://dnd.com.pk/after-hbl-meezan-bank-is-under-cyber-security-attack/258803

Valeriano, B., & Craig, A. (2018, February 3). Realism and Cyber Conflict: Security in the Digital Age. E-International Relations. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

WB. (2020). Individuals using the Internet (% of population)—Pakistan, India. World Bank Data: International Telecommunication Union ( ITU ) World Telecommunication/ICT Indicators Database. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=PK-IN&name_desc=true

Yaqub, J. (2020). Cyber Warfare and Challenges for Pakistan: JCSP 46 – PCEMI 46. Canadian Forces College, 18.

Zaidi, E. (2019, February 23). Banking cards' data worth $3.5mln stolen for online sale. The News International. https://www.thenews.com.pk/print/435450-banking-cards-data-worth-3-5mln-stolen-for-online-sale

Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon: Countdown to Zero Day. Wired. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/