PalArch's Journal of Archaeology of Egypt / Egyptology

IMPACT OF CYBER-TERRORISM ON NATIONAL SECURITY OF PAKISTAN

Shan Ali[1], Aamir Khan Jamali[2], Syed Zaheer Hussain Shah[3], Sabira Naz Qureshi[4], Sadia Tanveer[5]

[1] LLM & Advocate High Court Islamabad, Pakistan

[2] Mphil English, LLM & Advocate High Court Islamabad, Pakistan

[3,5] LLM Scholar at Bahria University Islamabad, Pakistan

[4] LLM & Advocate High Court Peshawar, Pakistan

Email: [1]sakambohadv@gmail.com [2]aamirkhanjamali8@gmail.com

[3]zaheer.hussain.shah@gmail.com [4]mehik1323@gmail.com [5]sadiatanveer812@gmail.com

Corresponding Author Email: sakambohadv@gmail.com

Shan Ali, Aamir Khan Jamali, Syed Zaheer Hussain Shah, Sabira Naz Qureshi, Sadia Tanveer. Impact Of Cyber-Terrorism on National Security of Pakistan -- Palarch's Journal of Archaeology of Egypt/Egyptology 19(3), 1456-1468. ISSN 1567-214x

Keywords: Cyber Security, Cyber Terrorism, Laws, Threats to State, And Analysis.

ABSTRACT

This study aims to highlight the core issues of cyber terrorism in the modern world. Technology in this world has advanced dramatically and it also has given confinement to very sensitive problems. The national security of any state is based on several elements, which include the political system, government, and critical infrastructure. Since these elements rely heavily on computer systems and networks for control, management, SCADA (supervisory control and data acquisition), and communications, any disruption as a result of cyber-terrorism may cost a lot to the states, and their organizations, therefore such cyber vulnerability is considered a direct potential threat to national security. Cyberterrorism is likely to turn out an immediate threat to the country's national security. This could be the use of the internet by terrorists to plan, recruit, and communicate with other terrorists inside and outside the territorial boundaries. While terrorists may not have the advanced skills to target critical, sensitive infrastructure, they are likely to use the vulnerability of the internet or its unmonitored facilities to communicate, recruit, and plan terrorist attacks.

This world (as a global village) has now built-in problems related to technology. In this research, the researchers have discussed the concepts of cyber terrorism and how it is dangerous to the national security of any state or country. Moreover, this research also leads the reader to the impact of cyber terrorism or cyberbullying on Pakistan or on any state and analysis of laws that need improvements.

INTRODUCTION

The world has recently seen a shift in terrorism from the traditional world to the cyber world. The National security of states is in jeopardy due to the adoption of advanced skills by the terrorists, wherein they tend to target and damage the critical infrastructure of the states. The main objective behind cyber-attacks is to create terror. This paper is aimed at establishing the linkage between cyber terrorism and the national security of states and how cyber terrorism threatens or challenges the national security of Pakistan (Gordon, Sarah, & Richard Ford 2002).

In this era of globalization, the world is getting more inter-connected, which will increase the chances of cyber warfare, and our dependency on the internet will create more hurdles in overcoming this perceived threat of cyber-terrorism. The Internet has made it easy for terrorists to recruit, plan, communicate with the perpetrators, and execute their plans without being physically present at the target place.

As ongoing counter-terrorism operations squeeze the physical space for militants or terrorist groups in Pakistan, the terrorist groups are now adopting cyberspace to carry out their attacks anonymously and they prefer to use the internet to communicate with each other.

The Concept of Cyber Terrorism

Barry C. Collin of the Institute for Security and Intelligence, in the late 1980's coined the term "Cyber Terrorism". Cyber terrorism is any act of terrorism over the World Wide Web or computer network, including deliberate attacks and disruptions of computer networks, by using computer viruses, or attacks using malware, to affect individuals or government.

Computers and the internet play a vital role in our daily lives. The world has become globally integrated. Internet and computers are being used by individuals, governments, organizations, and societies for their daily life chores. They use them for storing data, communications, controlling machines, typing, editing, designing, and almost in all aspects of life.

In the contemporary era, when the world has become globalized, terrorists don't have to go to the target place but they can now easily recruit, plan, or communicate with the perpetrators and execute their plans using the internet. After the 9/11 attack, the concept of cyber-terrorism gained more importance.
The role of computers stimulated criminals and terrorists to make it their preferred tool for attacking their targets. This shift in the methods of terrorism from traditional methods to electronic methods and the dependency on the internet is becoming one of the biggest challenges to modern societies.

Denning's Testimony in her most cited paper on the issue related to cyber terrorism, "Oversight Panel on Terrorism" (2000), states that cyber terrorism is the linkage between terrorism and cyberspace. The word "cyber terrorism" refers to two elements: cyberspace and terrorism. Cyberterrorism, in general, is understood as any unlawful attack or threat of attack against computer networks to coerce a government or people to achieve political, ideological, or social objectives or generate fear. Whereas, attacks that don't cause any harm to sensitive infrastructure or disrupt non-essential services would not be categorized as an act of cyber terrorism.

Another widely used term for cyberspace is "virtual" which means a place where computer programs functions. The internet has provided a virtual battlefield for countries having problems with each other, such as Taiwan against China, Israel against Palestine, India against Pakistan, China against the US, and many other countries. (Elmusharaf, 2004). According to the United States Department of State "terrorism" means premeditated, politically motivated violence perpetrated against non-combatants by clandestine agents (Acharya S, 2010).

Therefore, a working definition of cyber terrorism is the premeditated, politically motivated attack against computer networks, computer programs, and data, which results in violence against non-combatant targets by sub-national groups or clandestine agents.

Cyber terrorists prefer using cyber methods because it is cheaper than the traditional means, the action taken by them is hard to be tracked, they can operate covertly and can hide their personalities and location, they face no physical barriers, and can operate remotely from anywhere in the world and can attack a large number of targets (Acharya S, 2010).

The Danger of Cyber Terrorism

The Homeland Security Advisor of White House, General John Gordon, while speaking at a conference in San Francisco on 25th February 2004, indicated that whether someone detonated a bomb that caused harm to innocent people or hacked into a web-based IT system in a way that could, for instance, take a power grid offline and resulted in a blackout, the result would be the same. He also stated that the potential for a terrorist cyber-attack is real.

Cyberterrorism poses an immediate and disastrous threat to the national security of any state as it can destroy the economy of the state by carrying out attacks on sensitive and critical infrastructure.

Senator Jon Kyl, Chairman of the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security stated that members of Al-Qaeda have tried to target the electric power grids, transportation systems, and financial institutions. In England, the National High-Tech Crime Unit (NHTCU) survey showed that 97% of UK companies were victims of cyber-attacks in 2003.

Cyber terrorists can endanger the security of the nation by targeting sensitive and secret information and getting access to it. In 2007, Estonia was subjected to a mass cyber-attack by hackers inside the Russian Federation which some evidence suggests was coordinated by the Russian government, though Russian officials denied it. This attack was apparently in response to the removal of a Russian World War II War Memorial from downtown Estonia. All the blame was put on the hackers from Russia. According to the authorities of Estonia, the attack had a similar impact as of the Nagasaki attack in 1945. Such a concept is termed cyber warfare when a state penetrates another state's computer networks to cause damage and disruption (Elmusharaf Mudawi M, 2004).

Another cyber-attack of similar nature was carried out by the insurgents in Iraq in 2009. They hacked the US drone communication system which helped them in watching the videos recorded by the US drones.

During the Kosovo conflict in 1999, NATO's computer network was blasted with e-mail bombs and hit by denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports.

The Tamil guerrillas in1998 tried to disrupt Sri Lankan embassies. The messages included the statements such as "We are the Internet Black Tigers and we're doing this to disrupt your communications". The Intelligence authorities characterize the attack as the first known cyber-attack against the country.

The intention of a cyber-terrorism attack varies. It could range from economic disruption through the interruption of financial networks and systems or used in support of a physical attack to cause further destruction. The aim of attackers remains to create a chaotic situation to gain attention to their cause, if not achieve objectives.

National Security Vis-a-Vis Cyber Terrorism

National security is a concept that a government and the respective authorities should protect the state's and its citizen's interests and provide protection against any kind of national crisis through different means. Earlier the concept of security was confined to the military threat but later in the 1990s, the Copenhagen school of thought proposed that the concept of security should be broadened. The debate of the 'Narrow and Wider' concept of security by the Copenhagen school of thought argues that not only the traditional aspects of security i.e. military; are important but also the other sectors of society should be added i.e. political, economic, social, and environmental threats (Hansen, Lene, Helen & Nissenbaum, 2009). The proponents were of the view that weapons were not only the reason for wars or conflicts but other aspects also contribute to it. But some cyber experts in the late 1990s argued that the cyber sector must also be considered a direct threat as it poses an immediate threat to the national security of states (Chaudhary & Sanju, 2006).

Cyberterrorism gained public interest in the late 1980s when the term was coined by Barry C. Collin. Barry C. Collin is well known for his work as a Senior Research Fellow focused on the complex intersection of computer security, emerging technologies, business, public policy, and human life.

The media of the USA in the 1990s covered the statement of John Hamre, the Deputy Defense Secretary of America that the USA was perceiving the threat of digital/ electronic Pearl Harbor and the attack would not be against the Naval fleet but it would be against the commercial infrastructure. The Defense Secretary, Leon E. Panetta in 2012 once again referred to a Cyber Pearl Harbor (Ragan, 2013).

The concerns about national security gained more importance after the terrorist attacks on September 11, 2001. The threat of terrorism has never been as prominent as it is in the contemporary era. Terrorism is a historical phenomenon that can be traced back to the 1st century AD, The Zealots, the French Revolution's 'Reign of terror' but now the methods of carrying out the attacks have been modernized. The actions of the terrorists have become more destructive and dangerous and pose a direct threat to the national security of the state.

The threat of cyber terrorism is one of the techniques used by terrorists nowadays. Cyber terrorists gain access to the computer networks to disrupt the sensitive infrastructure of a state which not only endangers the lives of the individuals but also national security itself. Most of the critical infrastructure of the Western world is linked through computer networks thus the potential threat of cyber terrorism is for sure quite alarming.

The increasing dependency of our societies on technology has made the states and individuals vulnerable, giving terrorists a chance to approach targets that would otherwise not be quite easy. The hackers break into private and government computer systems to disable or disrupt military, financial or economic advancements.

The irony is that the more a state is technologically advanced, the more it becomes vulnerable to cyber-attacks. An unknown threat is perceived to be more destructive than a known threat. This gives an edge to cyber terrorists that they can operate remotely and anonymously. There are no physical barriers or borders to cross which makes it easier for the attackers or the perpetrators to carry out the attacks.

The cyber-attacks don't have an element of direct physical violence but their psychological impact is as destructive as the effects of a terrorist bombing.

Considering the 9/11 attacks, the Federal government requested 4.5$ billion for the security and protection of the critical infrastructure. On September 11, 2001, George W. Bush believed and stated that the American forces are overused and underfunded precisely when they are confronted by a host of new threats and challenges; the spread of weapons of mass destruction, the rise of cyber terrorism, and the proliferation of missile technology. After the

9/11 attacks, President Bush created the Office of Cyberspace Security and appointed his former counterterrorism coordinator, Richard Clarke as the head. Keeping in view the techniques used by terrorists to disrupt state's activities; terrorists can sit at one computer connected to one network and can create worldwide havoc. They don't necessarily require explosive devices to cripple a sector or shut down a power grid (Chaudhary & Sanju, 2006).

A survey of 725 cities conducted by the National League of Cities in 2003 found that cyber terrorism ranked alongside biological and chemical weapons at the top of the list of fear. The 2007 digital attacks on Estonian institutions in response to the government's removal of the World War II memorial were considered to be the first war in cyberspace. The Copenhagen school of thought has been successful in gaining the center ground of the widening debate in Security Studies (Chen & Hsinchun, 2009)

According to the International Business Times ISIS is the new perceived cyber threat. "The electronic war has not yet started" was one message sent in a video released on May 11, 2015, from a hacker group that claimed to be affiliated with the Islamic State.

Threatened National Security of Pakistan

With the advent of the information age, the thinking of states and sub-state groups has been impacted. The government of Pakistan has been fighting against extremism and terrorism for many years and another front on which Pakistan is facing severe threats is cyber terrorism. It is no surprise that Pakistan has a cyberspace dilemma. Cyberspace in Pakistan is spreading on a rapid pace such as into the institutions of banking, military, education, and government sectors but Pakistan somehow lags behind in securing the critical infrastructure of the state. Pakistan fails to keep pace with technical parameters and has not developed any sophisticated security system to tackle cyber threats. The threats of such nature are becoming a menace to the national security of Pakistan because of the vulnerable person and government information.

McAfee, an internet security company, in its report of 2007 stated that approximately 120 countries had been involved in developing ways to use the internet as a tool to target government computer systems and utilities. There is evidence that Indian hackers have often hacked and penetrated the websites of the Pakistani government. The cyber analysts in Norway have claimed in the report "Operation Hangover", published by Norman Shark, that some hackers based in India had been involved in targeting Pakistan military and government networks to get access to the information of national security interest to India.

Apparently annoyed by the remarks about Kashmir given by the Chairman of Pakistan People's Party, Bilawal Bhutto Zardari, some hackers based in India, who claimed themselves to be the "Black Dragon Indian Hackers Online Squad" vandalized the official website of Pakistan People's Party in 2014 (Chandio, Khalid 2018).

The government of Pakistan has allocated very less budget for the field of science and technology; the government does not consider this field as a priority, as a result of which it is facing economic turmoil for years. The Secretary of the Ministry of Science and Technology, Kamran Ali Qureshi, gave the statement that Japan spends 25% budget on science and technology, whereas Pakistan has allocated less than 1% of its budget for the respective field and suggested that more importance should be given to this field, in the economy.

On other hand India is investing more in this field, thus creating challenges for Pakistan on this front which is considered to be more complex than the traditional threats and warfare between Pakistan and India. Israel is also suspected of helping India in the field of technology against Pakistan. This factor is one of the security dilemmas of the State of Pakistan. Indian hackers are more skilled and advanced than the hackers based in Pakistan to break the safe boundaries of the cyber world. Pakistan has to take initiatives to secure its critical infrastructure and protection of the sovereignty of the state. To deter the threat, Pakistan needs an effective cyber army.

The more dependency on cyberspace results in more digital vulnerability. Pakistan is facing several security challenges on the cyber front. The government had blocked several websites like YouTube and torrents but still, these sites were accessible using different software and applications. This shows the weak points of the government that the government of Pakistan is not strong enough to even block a few sites.

The American National Security Agency (NSA) is keeping an eye on Pakistan through the internet. Approximately 13.5 billion emails, phone calls, and fax transmissions were intercepted. Pakistan ranks second to be observed by NSA, after Iran. Pakistan should take measures to protect critical data from such activities of spying (Rasool& Sadia 2018).

Terrorist organizations operate anonymously throughout the globe and are well trained in the cyber field. No law can be enforced on them as they operate anonymously and remotely and are difficult to browse. The reasons behind the hacktivism in Pakistan are political extremism, unemployment, poverty, ethnic affiliations, and in broader sense terrorism. These groups pose a serious threat to the national security of Pakistan. Pakistan's virtual system is not quite effective to stop illegal access to Pakistani websites.

Another major challenge is the lack of awareness amongst the people. Also, the website of the National Database and Registration Authority (NADRA) is vulnerable. The personal data of citizens is easily accessible. The personal data of every individual is on this website and the vulnerability of the site of NADRA is a major security threat to Pakistan.

Cyber terrorists aim to create fear and terror among the masses. They are motivated by political, religious, or ideological beliefs. Pakistan is already fighting against extremism and now these extremists have advanced their skills and use cyberspace for the proliferation of their beliefs and notions.

Analysis of Pakistan's Cyber Terrorism Law

Due to the lack of any legislation on the issues of cybercrime in Pakistan, the activities committed within the domain of cybercrime were dealt with under the Electronic Transaction Ordinance 2002 (ETO). ETO was proclaimed considering the challenges increased by the excessive use of the internet. Section 37 of the ordinance includes the punishment of imprisonment of up to 7 years. Whereas the law had some limitations, it was also considered, somehow, flawed due to the increase in the use of computers and the internet, and, consequently, the ways to commit crimes have also got more advanced, but they were not included in the Ordinance. The Ordinance was, thus, made less effective (Khadam & Nadia, 2016)

The deficiencies in the Electronic Transaction Ordinance (2002) led to a more detailed law, i.e. Prevention of Electronic Crimes Ordinance 2007 (PECO 2007). The respective Ordinance was related to the misuse of technology. This law also proved to be ineffective as it was unable to attain the status of an Act and was nullified in 2009. Since then the activities related to cybercrime are dealt with under the provisions of ETO.

In 2014, again the cybercrime laws came under the limelight in Pakistan. Three bills were proposed in Parliament. Cyber Security Council Bill 2014 was introduced before Senate by Senator Mushahid Hussain Syed. The bill focused on making policies, governance models, and laws to analyze the challenging situation from an International perspective.

The other bill was the Protection of Cybercrimes Bill 2014 which was proposed by Senator Karim Ahmad Khawaja with an aim to stop unauthorized and illegal cyber activities and a procedure for the trial and punishment in this regard.

Whereas, the third bill presented before the National Assembly was the Prevention of Electronic Crimes Bill 2014, presented by Ms. Anusha Rehman, Minister of State for Information Technology. This bill gained more importance because of the coverage of several crimes of the respective nature in it. If the unauthorized activities are committed with an intention to create fear and terror in society then the punishment is up to 14 years' imprisonment. Unauthorized access to information related to identity would be considered a crime under the law. This comprehensive law was the need of the hour.

The aspect of cybercrimes was not taken seriously earlier but this time the authorities have dealt with the issue with much more seriousness and as a result, the bill was passed after several debates. This is a passed law and certain issues can be dealt with or removed through amendments anytime as required by the scenario or situation. When any act is passed people either criticize it just for the sake of criticism or criticize it for a more pragmatic approach (Khadam & Nadia, 2016).

The government of Pakistan had passed the law against cybercrime with amendments. The opposition had criticized the bill earlier when it was

presented in the National Assembly. The Senate Standing Committee on Information Technology proposed 47 amendments to the Prevention of Electronic Crimes Bill in 2016. The implementation will see punishment of up to 14 years imprisonment and or a fine of 50 million rupees. The cyber law of Pakistan is considered to have the capacity to control cyberspace of Pakistan as the same was not present in any previous cyber laws.

Indeed, even after the sanction of this Bill from Parliament a ton of feedback is on record. The critics of this law were of the view that this law might pose serious hurdles to freedom of information and a few provisions of the law needed elucidation since, as indicated by them, there was a perceived danger of abuse of specific provisions. In any case, wisely watching those snags, assuming any, could be dealt with by reasonable changes. That ought to be invited by the Parliament to alter and enhance the law. In the event that the same is not done this time, on the other hand, Pakistan will be in a place of lawlessness as far as cyber crimes are concerned.

An amendment was made to the clause which states that the Federal Government may establish a law enforcement agency to inquire and investigate cyber offenses. Several more amendments were made to define some vague terms. The Act also focuses on the offense of cyber-terrorism (Ahmad & Tariq, 2019). Under cyber law, detainment of up to seven years can be granted for financing a terrorist organization through the internet. Additionally, a man can be tried under the law regardless of the possibility that the offense is committed outside Pakistan. Moreover, the investigation is to be carried out with the court's consent.

According to the Ministry of IT, the cybercrime law deals with hate speech, and terrorist activities on the internet and protects critical government infrastructure from hackers. But PML-N MNA Tahir Iqbal argued that law enforcement agencies should not require a warrant from courts to take immediate actions against any illegal activity or to confiscate information and electronic devices.

Former army personnel stated "The situation of the country demands immediate actions. The Law Enforcement Agency should not need a warrant. They don't have time to get warrants and let the terrorists win. This is the only way to save society (Shahid & Jamal, 2015).

The critics pick apart the bill by considering it too harsh with the punishments that are too harsh to fit with the crimes. Moreover, the bill leaves room for Law Enforcement Agencies to misuse the powers of the provisions. The bill is considered to be flawed as it restricts the freedom of expression and access to information (Khan & Raza, 2019).

The bill does not adequately differentiate between cybercrime, cyber terrorism, and cyber warfare. All of these need specific and different laws and provisions according to their subject.

The critics argue that the mechanisms for the implementation are absent in the bill. The bill has introduced the clauses of cyber terrorism which is not the subject of the bill. The bill has to deal with cybercrimes. Thus, Pakistan still lags behind in formulating policies and mechanisms to counter the threat of cyber terrorism.

The world had seen the first digital weapon known as the "Digital Missile". The digital missile was used against Iran by the United States of America and Israel. The Stuxnet worm attacked the Iranian nuclear facility in 2010. The virus was strong enough to physically destroy the components of computer systems. Whole Iranian digital data on their nuclear program was destroyed.

Similarly, Pakistan's nuclear program is also available in cyberspace and yet needs to be highly secured. There are claims that Israelis have tried to use their money and advanced technologies to damage the nuclear program of Pakistan. Pakistan should deal with such threats and vulnerabilities seriously (Rasool & Sadia, 2015).

Ambassador Masood Khan assured the UN General Assembly in the year 2013 that the weapons stockpile was safe and secure for the entire spectrum of threats, including cyber-attacks. "Pakistan's nuclear materials, facilities, and assets are safe and secure." (Khan, 2013).

Mechanisms to Strengthen the National Security of Pakistan

Several cyber experts and authors have recognized the underlying concerns regarding cyber terrorism and have presented different strategies and mechanisms to ward off the threat to strengthen the national security of a state. O'Brien has described a set of initiatives under the standard security paradigm of Deterrence, Prevention, Detection, and Reaction. Although O'Brien gives some solutions to stop cyber terrorism by keeping the operating systems and software updated, enforcement of strong password policies, and employment of high detection systems and firewalls, but still these preventive measures are incomplete in their scope and are not enough.

The more explicit form of dealing with cyber-terrorist activities includes three stages of defense i.e. Prevention; to prevent a cyber-attack from being launched in the first place and taking pre-emptive measures, Incident management and mitigating an attack; to prepare and take defensive measures and limit the damage, Consequence management; this stage includes two primary sub-stages: recovery and response. Recovery is the passive form of defense whereas the response is concerned with the punishments imposed on the culprits and enabling the organization to defend itself in the future by taking new measures (S.E. Goodman, 2007)

Clarke argues that the cyber world is neither owned by any group or organization nor operated by a single government or a group. Such anarchic nature of the cyber world as stated by the realist school of thought is a major challenge for the states. Clarke argues that the development of a policy or a treaty would encourage the participation of the private sector. Organizations in

the private sector need to cooperate with the government and work together to avoid cyber-attacks. The involvement of the private sector would result in more financial support to fund the treaties and anti-cyber terrorism organizations.

The security plans to avoid cyber-attacks can be outlined in nine points i.e. Education, Communication, Technology, Responsibility, Funding, Commitment, and Cooperation. The plan recommends possible measures that governments, organizations, and individuals could use to avert the threat of cyber terrorism.

The development of new strategies and technologies is playing a large role to avert the threat of cyber terrorism but ironically these are also providing cyber terrorists more opportunities to exploit the critical infrastructures across the globe. The plans for dealing with cyber threats should not only consider the technical aspects but also need to incorporate the development of strategies, policies, an effective Act, and its implementation (Beggs & Butler, 2020). Several countries have given importance to national plans and policies to secure cyberspace.

Governments while taking countermeasures must keep in my mind that terrorists can easily launch attacks in a disguise. They operate covertly both in physical and cyberspace attacks. This makes cyberspace intelligence intensive. Pakistan faces several challenges on the cyber front. In a Senate Standing Committee on Foreign Affairs, chaired by Senator Nuzhat Sadiq, a committee member Mushahid Hussain Sayed stated that Pakistan is one of the top countries under foreign espionage but Islamabad does not have effective measures against cyber-attacks (Khatak, 2020).

States are recommended to go for bilateral or multilateral agreements on cyber security issues as cyber terrorism is a growing concern of the whole international community. It is not confined to one state or organization (Dogrul & Aslan, 2021).

The government of Pakistan needs to allocate more budget for the field of science and technology. The government should assist in controlling the menace of cyber terrorism attacks by establishing and revising cyber laws. There is a need for a more specific approach other than the cybercrime bill. New Acts need to be developed for more efficient cyber security practices.

CONCLUSION

Pakistan is fighting against terrorism and extremism for several years and now is threatened on the cyber front as well. Unfortunately, this emerging threat has not gained much attention from the government of Pakistan.

The conjunction of terrorism and technology is a complex issue that requires serious attention. It is nearly impossible to ignore the fact that cyber terrorism will take an extreme form in the coming future.

Pakistan was never really awake to the menace of cyber-terrorism. As it always lagged behind in the run of technology, none of the governments except the era of General Pervez Musharraf when agencies became aware of such threat, really made any effort for advancement in the IT sector. However, after that no serious thought was given to building fortified cyber territory; even the cyber-terrorism bill passed by the legislative assembly could not make things move at the desired speed. On the other hand, India is continuously enhancing its prowess in the sector. It is, now, high time that our authorities take this menace into account and should not shy away in the excuse of not being a high-speed traveler on the highway of information technology.

BIBLIOGRAPHY

Acharya, Subhojyoti. n.d. "Cyber Terrorism- The Dark Side of the Web World." *Legal service India* (2008).

Arquilla, John, David Ronfeldt, and Michele Zanini. "Information-age terrorism." *Current History* 99 (2000).

Chandio, "Cyber security/Warfare Pakistan", *Islamabad Policy Research Institute*, August 13, 2015.

Chaudhary, Sanju. "Linkages between cyber terrorism and national security", *Scholarly Research Journal for interdisciplinary studies* (2006).

Chen, Hsinchun, Wingyan Chung, Yi Qin, Michael Chau, Jennifer Jie Xu, Gang Wang, Rong Zheng, and HomaAtabakhsh. "Crime data mining: an overview and case studies." *In Proceedings of the 2003 annual national conference on Digital government research*, Digital Government Society of North America (2003).

Conway, Maura. "What is cyberterrorism?" *Current History 101*, no. 659 (2002).

Conway, Maura. "Cyberterrorism: Hype and reality" (2007).

Conway, Maura. "Cyberterrorism: the story so far." *Journal of Information Warfare 2*, no. 2 (2003).

Elmusharaf, Mudawi M. "Cyber Terrorism: The new kind of terrorism." *Computer Crime Research Center 8* (2004).

Gordon, Sarah, and Richard Ford. "Cyberterrorism?" *Computers & Security 21*, no. 7 (2002).

Frenkel, Sheera, "If You Have Windows, Update It Right Now to Keep This Massive Hack Out." *BuzzFeedNews.* May 12, 2017.

Janczewski, Lech, ed. *Cyber warfare and cyber terrorism*. IGI Global, 2007.

Keegan, Christopher. "Cyber terrorism. (Security)." *Financial Executive 18*, no. 8 (2002).

Lachow, Irving. "Cyber terrorism: Menace or myth." *Cyberpower and national security* (2009).

Khadam,Nadia "Seriousness towards cybercrime laws in Pakistan", *The News International*, August 19, 2016.

Nagpal, Rohas. "Cyber terrorism in the context of globalization." *In II World Congress on Informatics and Law*, (2002).

Petallides, Constantine J. "Cyber terrorism and ir theory: Realism, liberalism, and constructivism in the new security threat." *Inquiries Journal 4*, no. 03 (2012).

Pollitt, Mark M. "Cyberterrorism—fact or fancy?" *Computer Fraud & Security 1998*, no. 2 (1998).

Prichard, Janet J., Laurie E. MacDonald, and Lynn Hunt. "Cyber terrorism: A study of the extent of coverage in computer security textbooks." *Journal of Information Technology Education 3* (2004).

Reuters, "Cyber a top national security threat to U.S", *Intelligence director. Business Insurance*, September 2016.

Rasool, Sadia "Cyber security threat in Pakistan: causes challenges and the way forward", *International scientific online journal*, August 12, 2015.

Tariq Ahmad, "Pakistan: National Assembly Passes New Cybercrime Law", *Library of Congress*, September 21, 2016.

Tariq, Muhammad, Baber Aslam, Imran Rashid, and Adeela Waqar. "Cyber threats and incident response capability-a case study of Pakistan." *In Information Assurance (NCIA)*, 2013 2nd National Conference on, IEEE, 2013.

Westby, Jody R. "Countering terrorism with cyber security." *Jurimetrics* (2007).

Weimann, Gabriel. "Cyberterrorism: The sum of all fears?" *Studies in Conflict & Terrorism*, no. 2 (2005).

Whitehead, "Cyber-attacks threatening national security double in past year, GCHQ reveals". *The Telegraph*, November 2015.