Journal of Historical Studies
Vol. VIII. No. I (Jan-Jun 2022) PP 177-195

New Challenges for Pakistan's War Against Terrorism in the Cyber Space Era

Mohsin Raza
Ph.D Scholar
Bahauddin Zakariya University Multan
Mohsinmahni495@gmail.com

Rao Imran Habib
Assistant Professor
Bahauddin Zakariya University, Multan
raoimran@bzu.edu.pk

Naureen Akhtar
Assistant Professor
Bahauddin Zakariya University, Multan
Nauree.akhtar@bzu.edu.pk

Abstract:

Cyber terrorism is wreaking havoc on the national and worldwide communities. Businesses, industries, and governments are losing billions of dollars as a result of the rise in cybercrime. Pakistan is committed to combat cyber terrorism and has enacted a number of laws to that end. However, due to the changing character of these crimes as a result of extensive technological progress, the outcomes were not productive. Existing laws are only applicable to traditional crimes, and as a result, they are unable to tackle modern crimes owing to their evolving nature. As the world becomes more electronic and the economy becomes more individualized, cyber space is praised as critical to a country's growth. This article examines how cyberspace and the internet is being used for cyber-attacks. Pakistan is committed to establishing cybercrime legislation in the digital age, but enacting unclear and ineffective cybercrime legislation is not the answer. By bringing legislation up to international standards, the evil of cyber terrorism can be combated. To make people aware of the threat of cyber terrorism, awareness campaigns is also required. Pakistan must

design and execute cyber security rules that are in line with current technology. To fend off such attempts, the enforcement process should be overhauled. This study employs descriptive technique and employs a qualitative doctrinal research design that is more dialectic and hermeneutic in nature. The data for this study was compiled from a variety of international and national magazines, as well as published cases and conference proceedings.

Keywords: Cyber Terrorism, Causes and Reasons, Cyber Space, Cyber Security, Digital era. Cyber Laws.

Introduction:

While many people throughout the world are working tirelessly to find the most efficient and effective way to communicate with modern techniques and technology, they face several obstacles, including the ongoing abuse and enhancement of technology. Hence, the communication between different cyber terrorist from different countries is carried out with the aid of the cyberspace.[1] Terrorists use such particular media to transmit their encoded communications in order to achieve their goals. Secrecy, psychological influence, and the possibility of considerable harm make cyberspace an attractive platform for terrorists of the computer-savvy generation. Cyberspace is a meeting place for cyber terrorists.[2] The extensive use of the internet, which has been reinvigorated either by the internet and social networking sector, which includes social media and internet networking sites, has had an impact on commerce, politics, and corporations.[3] An increasing number of modern states have open and diverse infrastructures and a greater reliance and vulnerability on automated networking, which increases the risk of cyber terrorism.[4]

Academics, authorities, and government officials are all targets of terrorist groups. At its core, the goal of this campaign is to undermine public trust in institutions such as intelligence agencies and governments.[5] Cyber-attacks have the ability and power to disrupt people's daily routines. As an example, if all ATMs in a country were down, there would be a pandemonium-like situation. Modern communication technologies, which

allow global financial institutions to connect, increase the possibility of this happening.[6] Most social media and networking sites are designed to help people keep connected and up-to-date with the people and things they care about in other parts of the world. Keeping in touch with loved ones, friends, colleagues, businesses, and other like-minded organisations and media sources is one of the primary reason people log on to social media sites like Facebook and Twitter. In many countries around the world, the use of Information and Communication Technology (ICT) has increased their dependence on the Internet (ICT).[7] The role of ICT is ambiguous. Despite the fact that advances in information and communication technology (ICT) have led to enormous improvements in competence and productivity, they have also provided a platform for those with malicious intentions to wreak harm. The perpetrators, such as rebels and terrorist groups, can also use it as a tool to promote propaganda and extremist ideologies and to instill fear in the population by causing destruction to assets that are dynamic to countrywide security.[8]

To carry out any form of these attacks against a specific target, terrorists can use the ICT if they merely follow the hacker's trail. Insertion of viruses into vulnerable networks, attacks on denial-of-service, defacing of websites, going to hack into computer systems and misapplication of various digital systems are among the most emerging crimes in the current digital world. Electronic fraud and terroristic threats made through the use of electronic communication are also among the most emerging crimes in this digital world.[9]

The primary aim of this article is to explore the reasons and causes of cyber terrorism and to explore the damages that it causes. Moreover, this article examines the legislation enacted by Pakistan and at the end this study suggest how this evil can be combated.

What is meant by cyber-terrorism?

It is commonly accepted that to alter and indulge falsehoods and retain interior communications the cyber terrorists commonly

use the internet services. In this context, cyber-terrorism is defined as using connected devices to decode infrastructure (like telecommunications, organisations, politics, businesses, and transport) or to manipulate or harm the general populace, social, or civilian population.[10] The term "cyber terrorism" refers to the use of code attacks by individuals to cause fear and chaos to accomplish managerial or communal purposes.[11]

Denning demonstrates Cyber-terrorism as:

> *"Cyber terrorism is unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."*[12]

The cyber terrorism is described by Mshvidobadze in the following phrase:

> *"Cyber acts designed to foment terror or demoralization among a target population for some purpose of the perpetrator, most likely this will be some kind of attack on critical infrastructure. Cyber terrorism should be involving computer technology and means as a weapon or target by terrorist groups or agents."*[13]

The aforementioned descriptions suggest that key infrastructures, including computer networks and the general people would have become attractive targets in respect of cyber terrorist tyranny, contributing to the distinctiveness of electronic criminal intimidation. As a result, essential computer network infrastructure and civilian populations will be directly harmed as a result of these attacks.

Factors leading towards Cyber-Terrorism

Myriad of reasons are considered by cyber-terrorists to become tangled in terrorism.[14] Cyber-terrorists frequently have a number of anxieties and purposes. Nevertheless, the primary elements behind cyber terrorism are economics, politics including ideology.[15] Terrorists are propelled to carry out their acts of violence by a variety of internal and external forces. When a single person or group of people join forces with a certain political or religious cause in order to advance their own objectives, that is considered an act of cyber terrorism.[16] In the Irish democratic army, for instance, you'll find that they engaged in acts of terror in order to maintain their position of power.[17]

Threats to a country's key infrastructure feed cyber terrorism. It is possible that some losses will occur in the specifically oriented industry. Corporate losses can be disastrous, resulting in document damage and destruction, stolen money, accusations of attempting to steal editorials, lost quarterly profits, theft of elevated assets, theft of mystery and financial information, larceny fraud and threat assaults, interruptions to the regular business course material, forensic analysis and many more. Cyber terrorism is expected to cost the world $10.5 trillion every year by 2025, as per cyber security initiatives.[18]

This represents a 100 % increase above the $3 trillion caused in 2021.[19] Hundreds and thousands of dollars in revenue and employee productivity would be wasted. However, the most costly intangible costs borne by a corporation are those related to its repute and image. These setbacks can sometimes be perpetual, even deadly. Furthermore, the losses can include the forfeiture of data which is stolen through an assault. These impalpable values were accurate as corporations had typically underestimated the consequence of a breach of security and protection. Prior investments made before the attack will not yield any profit.[20] Companies used to be indifferent with cyber security, but today that is something that managers will focus from the outset.[21] Many other reasons, such as radicalisation and fanaticism in cyberspace, contribute to cyber terrorism, which is getting more prevalent by the day.[22] From a psychological

standpoint, a disgruntled employee poses a threat to the company where he works. In Australia, for example, a sewerage control system was in the hands of an employee, who destroyed the ecosystem and killed wild animals.

According to the inquiry, the person had previously worked for the company and had all of the necessary information and experience to run systems. Aggression and feelings of unfairness from the administration were the driving forces for his attempts. For cyber terrorist purposes, this group of people can be planted or purchased, and their personal information sold.[23]

Pakistan and Cyber World

This unacceptable situation is due to a lack of measure, lawful, specialised, and authoritative, limit construction and collaboration to strengthen the nation's digital security, according to research. A number of approaches can be used to identify Pakistan's shaky network security plans. Through Snowden's leaks, Gatekeeper revealed that, in March 2013 behind Iran, the second most targeted country was Pakistan as per report by the US National Security Agency (NSA).[24] In the same month, the Government Communications Headquarter (GCHQ) of the United Kingdom attacked the Pakistan Central Communications Framework to get access to regularly used sites in the same month.[25]

Pakistan received the highest overall number of malware attacks in 2015, according to Microsoft, the country remained among the most attacked nations under the unaware comprehension. The National Association for Data Retrieval and Analysis (NADRA) is the primary organisation that collects and store data on the general public.[26] According to the findings of the study, NADRA is one of the greatest networks in the world for the use of craftsmanship advancements by government agencies (Threat Track Security 2014). NADRA is by far the most critical and key public organisation that gathers public profile reports on Pakistani individuals who were targeted by Indian attackers between 1999 and 2008.[27]

The financial industry appears to be particularly vulnerable to these attacks. Attacks against Habib Bank Limited (HBL) ATMs resulted in 579 accounts being hacked and Rs.10 million in losses in late 2017, as a result of a massive cyber-criminal attack using skimming gadgets. FIA discovered that, digital programmers attacked nearly all of Pakistan's banks, causing money to be lost in accounts in 2018. As a result of cyber-attacks, Pakistani citizens and infrastructure are at risk, as are the country's security systems.[28]

In 2013 during his time as chairman of the Senate Committee on Defense and Defense Production, Senator Mushahid Hussain stated that:

> *"The warning of cyber security can influence Pakistan's national defense, protection, espionage, diplomacy, nuclear and missile program, economy, energy, education, civil piloting as well as industrial and constructing units both in the private and public part. Cyber security is a problem of chief importance for Pakistan's establishment and progress."*[29]

Taliban zealots attacked an army school in Peshawar on December 16, 2014, killing over 150 students and professors. This incident sparked a shift in consciousness that allowed people to avoid the dangers of radicalism. Following the assault, Pakistan devised a "National Action Plan" that outlined 20 steps the country would take to combat radicalism.[30] The Government emphasised that, country need to pass legislation granting the government unrestricted authority to screen, detect, and arraign alleged terrorists. While the goal of speedily eradicating radicalism is commendable, the demand for free access has spread further than the National Action Plan to certain further laws currently being debated which affect Pakistan general public directly. One of the most well-known and important model is the Prevention of Electronic Crimes Act of 2015. The

deterrence of digital offence legislation has its origins in General Musharraf's presidency.

The PECO Ordinance of 2007 and 2009:

The Prevention of Electronic Crimes Ordinance was introduced by Musharraf (PECO 2007).[31] The government could use the PECO 2007 statute to prosecute numerous types of cybercrime. In general, The Prevention of Electronic Crimes Ordinance 2007 rejected criminal admission, tampering, or harm to electronic records and frameworks. The management aired PECO 2007 to increase the secrecy of Information technology industry. As a result, experts accepted Musharraf's silent resistance and used the internet to spread mockery against him. The law would be used to put a stop to free presentation because it barred the use of the cell phones and internet to use incongruity on experts or sort them out. In summary, PECO 2007 exploited the guise of "public security" to impede a variety of blogs that were critical of government policy.[32] PECO 2007 gave the FIA the authority to look into alleged crimes. FIA, on the other hand, is well renowned for keeping the pundits of high-ranking government officials secret. The FIA, for example, stated that it will expose "antidemocratic" forces circulating YouTube videos and instant messaging targeted at denigrating government officials. When PECO 2007 failed (after three amendments) and it became clear that it would never receive legislative approval, then-President Asif Ali Zardari issued another proposal in July 2009 as “The Prevention of Electronic Crimes Order of 2009”. This newly enacted order was based on the provisions PECO of 2007 which addressed identical topics. Same was cancelled in November 2009 due to a lack of parliamentary approval.[33]

The Prevention of the Electronic Crimes Act, 2016:

The National Assembly enacted the Prevention of Electronic Crimes Act of 2016 on August 11th, 2016. PECA was passed by the Senate unanimously in July. On the 18th of August 2016, Pakistan's president signed the bill into law.[34] The legislation was enacted to protect the secrecy, privacy, and information of persons who are the victims of illegal activities, as well as to establish a mechanism for investigating, prosecuting, and trying those who are charged with related offences. A provision for cyber terrorism is included in this act. Under this regulation, "cyber terrorism" refers to a cyber-attack or cybercrime aimed at causing damage to key infrastructure and inciting terrorism.[35] There were also some penalties as a result of it. For such an offence, the penalty is 14 years in imprisonment and a fine of 50 million (approximately US$47,450), or both.[36] The exaltation of the acts linked with such a category is the glorifying of hate speech, the planning, funding, or any deed which constitutes such an offence.[37] A law enforcement department can be established or delegated by the federal government. The FIA's mission is to investigate offences committed in violation of the act's provisions. On September 9, 2016, the federal government designated the (FIA) as the inquiry department.

Criticism on PECA

Human rights, free speech, and unfair prosecution were all issues raised PECA 2016. This statute has been attacked across the board for its vague language and the fact that it gives PTA unfettered powers (Pakistan telecommunication authority). Section 37 of the PECA has given the PTA unrestricted jurisdiction to censor and remove web-based information, limiting the right to free expression guaranteed by the Constitution of Pakistan 1973 article 19. The number of applications made by PTA to overseas platforms to block, restrict, or remove the user's content is extremely high. Furthermore, adding provisions of this act along with sections of such PPC violates superior court judgements by interfering with the courts' authorities. Section 20 of PECA, for example, is regularly added to Pakistan penal code section 500. The

mechanism for imposing the punishment is unclear. Another concern is that the FIA does not charge private litigants (that are not government officials) with violating the Pakistan penal code.[38]

The problem lies in this act PECA is the interpretation of section 34, as it restricts internet content for arbitrary reasons.[39] In accordance with this clause, the FIA has the authority to ban any content that is deemed to be detrimental to Islam, the country (Pakistan) or friendly ties with other countries, decency, ethics and public order, as well as the security or defence or honour of the state. Here, the problem is there are no defined terms for "necessity" and what appears to be anti-Islamic, anti-Pakistani, or anti-morality content or practises.[40] This section contains no exceptions or exclusion, and even more shocking, there is no appeals mechanism. Political opposition and government critics can be effectively targeted by Section 34 since there are no standards, procedures and guidelines for dismissing them from office. Limits content that doubts the administration's foreign policy given the favourable relations conditions. Two of most frequently criticised international ties of Pakistan with the United States and Saudi Arabia could be severed. Those who are uninformed of the requirements and punishments of the PECA are vulnerable.

Digital Rights Foundation founder Nighat dad has stated that.

> *"The overly broad language used in the bill ensures that innocent and ignorant Pakistani citizens, unaware of the ramification of what the bill entails, can be ensnared and find themselves subject to very penalties."*[41]

Due to the lack of rigour in the investigation and punishment process, the vast majority of criminals are not prosecuted. In Karachi, for example, only one individual has been convicted as of Aug. 31, 2019. Karachi is the scene of several high-profile incidents.

Court	Total Cases	Jail	Bail	Acquittals	Convictions	Absconder
Central Karachi	9	1	7	-	-	-
East Karachi	26	4	14	5	1	2
South Karachi	11	2	8	1	-	-
West Karachi	2	-	-	2	-	-
Malir Karachi	5	-	5	-	-	-
Total	54	7	34	8	1	2

This figure shows numerical figures of pending cases in various districts of Karachi. In Karachi, there are 54 cases still pending. There are seven inmates in custody, while 34 defendants are on bail. There have been 8 acquittals and 1 conviction in this case. In two of these situations, suspects have vanished without a trace. Other than that, it's not clear what is going on.[42]

Pakistan in Cyber Security so Far:

We live in a world so exposed to new risks that no government or state can claim to be completely safe from them or to have achieved complete proof and efficient cyber protection. When it comes to network security, Pakistan is a developing country, yet an exhibition diagram paints a helpless picture. Given the magnitude of the country's digital threats, this is especially true.[43] As a result of the Electronic Transactions Ordinance, 2002, (ETO 2002), passed in 2002, e-commerce was given a level of constitutional protection. ETO's inability to protect against other types of cybercrime has been viewed as its worst flaw. As a result, the Prevention of Electronic Crimes Ordinance (PECO) of 2007 was repealed in 2009 since it did not receive the necessary approval to become a law.

Resultantly, The Prevention of Electronic Crimes Bill (PECB 2015) enacted in Pakistan and it covers a wide range of issues, including but not limited to: cyber terrorism; hate speech; spamming and digital tracking; electronic fabrication and

extortion. That being said, it has been censured from that point on due of its tendency to manage the ability to talk freely, employ ambiguous language, and grant PTA continuous powers. Pakistan Information Security Association-Computer Emergency Response (PISA-CERT) and Pakistan Computer Emergency Reaction (PAK CERT) are two organisations in Pakistan that specialise in network security measures. As an aid and a source of capacity building, their services play an important role in delivering information on cyber dangers for the management of cyber security.[44]

The Senate Defense Committee also established a Research institute in Pakistan for Cyber Security under the supervision of cyber security task force. Furthermore, Pakistan established its first National Cyber Security Center in May 2018 at Air University Islamabad (NCCS). Regrettably, the country desperately needs an effective cyber security protocols along with cyber security plans to effectively apply international cyber security protocols. Furthermore, it fails to meet the requirements of a credential system for cyber protection and security. Additionally, Pakistan needs to build an administrative body or a sufficient number of cyber security personnel in accordance with internationally recognised standards. In a word, the country's attention, legislative framework, and policy on capacity building and information assurance are all woefully inadequate.[45]

Pakistan's performance in terms of organisational steps was once again dismal. Despite adopting a Digital Pakistan Policy in 2017, the country still lacks a cyber security plan and policy. In truth, there is no full-fledged cyber security agency or department. The Financial Intelligence Agency (FIA) is a section that deals with cybercrime under the supervision of the National Response Center for Cybercrime. The organised competency is now again the issue. The National Cybercrime Response Centre now lacks the means and capabilities to monitor the hacker's private operations. Furthermore, despite the fact that the country has devoured a number of white hats or ethical hackers, their skills and abilities have remained untapped.

Conclusion

It is suggested that establishing a legal framework is a challenging task because the nature of crimes, hacker inventiveness, and technological breakthroughs evolve at a far faster rate than the law. Malicious code (malware) can be developed anywhere in this digitised era by anyone with sufficient awareness and ability. These skills are not difficult to acquire, and malware-making toolkits can be obtained easily and at a low cost anywhere in the world. Noncommercial issues such as extremist communications and ideas can be hatched using cyberspace and the internet, and neither can protect e-commerce with the help of ostensibly enacted legislation. There are numerous obstacles to overcome in order to defeat cyber terrorism; for this reason, training and public awareness are critical. It is commendable that Pakistan is committed to drafting cybercrime legislation in this digital age, but implementing a vague, harsh, and illegal cybercrime law under the guise of doing so is not the solution. As the world becomes increasingly digital, it is more important than ever to build a legislative structure and push legislation to combat cyber terrorism, which is getting more dangerous as technology advances.

Departments and institutions have been established, but their efficiency in operation has not proven to be sufficient. Pakistan requires a unified institutional framework that connects the services of many key agencies and infrastructures in order to achieve harmonisation and coordination. Although, a strong legal framework and suitable regulations are urgently needed to combat cyber terrorism on a worldwide scale, basic liberty, including basic human rights must not be sacrificed in the process.

Notes

1. Azimi Bolourian, Ali, Yashar Moshfeghi, and C. J. van Rijsbergen. "SugarCube: quantification of topic propagation in the blogosphere using percolation theory." In *Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval*, pp. 786-787. 2009.
2. Alvi, *supra* note 19. PECO 2009 as an ordinance.
3. Anup Kaphle, *Pakistan Announces a National Plan to Fight Terrorism, Says Terrorists' Days are Numbered*, The Washington Post, (Dec 24, 2014):
4. Bambauer, Derek E. "Censorship v3. 1." *IEEE Internet computing* 17, no. 3 (2013): 26-33.
5. Bolo bhi, "PECA: A THREE-YEAR REVIEW", <<https://bolobhi.org/wp-content/uploads/2019/11/Summary-of-Report-updated-18.10.2019.pdf>>
6. Beggs, Christopher. "Cyber-terrorism in Australia." In *Encyclopedia of Information Ethics and Security*, IGI Global, (2007), 108-113.
7. Bergin, Anthony, Sulastri Osman, Carl Ungerer, and N. Yasin. "Countering internet radicalisation in Southeast Asia." Rajaratnam School of International Studies and Australian Strategic Policy Institute: *ASPI Special Report* 22 (2009).
8. British E-Spy Agency Hacked Network Routers To Access Almost Any Internet User In Pakistan | The Express Tribune", *The Express Tribune*, 2022, <https://tribune.com.pk/story/908732/british-e-spy-agency-hacked-network-routersto-access-almost-any-internet-user-in%20%20%20%20%20pakistan>
9. Bieda, David, and Leila Halawi. "Cyberspace: A venue for terrorism." *Issues in Information Systems* 16, no. 3 (2015): 33.
10. Baggili, Ibrahim, and Marcus Rogers. "Self-reported cyber crime: An analysis on the effects of anonymity and pre-employment integrity." (2009): 974–2891.
11. Cavusoglu, Huseyin, et al. "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers." *International Journal of Electronic Commerce* 9, no. 1 (2004): 70-104.
12. Cavelty, Myriam Dunn. "Critical information infrastructure: vulnerabilities, threats and responses." In *Disarmament Forum*, 3 (2007), 15-22.
13. Cassidy, John. "Why Edward Snowden is a hero." *The New Yorker* 10 (2013) <https://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero>
14. Denning, Dorothy E. "Cyberterrorism: Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism." (2000).
15. Flemming, Peter, and Michael Stohl. "Myths and realities of cyberterrorism." In *Countering Terrorism through International Cooperation: Proceedings of the International Conference on*

"Countering Terrorism Through Enhanced International Cooperation". Milano: ISPAC, (2001), 70-108.

16. Farieha Aziz, "Pakistan cybercrime law: boon or bane", *Heinrich Boll Stiftun, the green political foundation,* (February 14, 2018), <<https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane>>
17. Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." *Journal of Computer and System Sciences* 80, no. 5 (2014): 973-993.
18. Kostov, Nick, and Costas Paris. "Companies try to contain fallout from global cyberattack." *The Wall Street Journal, Dow Jones & Company* 28 (2017).
19. Lewis, James Andrew. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies, 2002.
20. Matusitz, Jonathan. "The role of intercultural communication in cyberterrorism." *Journal of human behavior in the social environment* 24, no. 7 (2014): 775-790.
21. Matusitz, Jonathan. "Cyberterrorism: Postmodern state of chaos." *Journal of Digital Forensic Practice* 3, no. 2-4 (2010): 115-123.
22. Mantel, Barbara. "Terrorism and the internet. Should web sites that promote terrorism be shut down?" *CQ researcher* 3, no. 1 (2009): 129-152.
23. Mehreen Zahra-Malik, "Pakistan passes controversial cybercrime law", *world news,* (August 12, 2016)
24. Mohammed, Furqan. "PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill." *UCLA J. Islamic & Near EL* 15 (2016): 71.
25. Mehwish Khan, "7-Point Action Plan Proposed For Cyber Secure Pakistan", *Propakistani.Pk,* 2022, https://propakistani.pk/2013/07/09/7-point-action-plan-proposed-for-cyber-secure-pakistan/.
26. Orman, Levent V. "Technology as risk." *IEEE Technology and Society Magazine* 32, no. 2 (2013): 22-31.
27. Pakistan | Opennet Initiative, *Opennet.Net*, 2022, <<https://opennet.net/research/profiles/pakistan>>:
28. Osman Husain, "Is the New Cyber-Crime Bill Akin to Banning the Internet in Pakistan?",*The express tribune* (blogs), Apr 20, 2015, <<http://blogs.tribune.com.pk/story/27245/is-the-new-cyber-crimebill-akin-to-banning-the-internet-in-pakistan/>>
29. Serge Krasavin, "What Is Cyber-Terrorism?" *Crime-Research.Org*, 2022, <https://www.crime-research.org/library/Cyber-terrorism.htm.> (accessed on 18th march 2022).
30. Schweitzer, Yoram, and Sari Goldstein Ferber. *Al-Qaeda and the internationalization of suicide terrorism*. Tel Aviv University, Jaffee Center for Strategic Studies, 2005.
31. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", *Cybercrime Magazine*, 2022, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.>

32. Salman Siddiqui, "Beware - Hackers Are Going After Atms In Pakistan | The Express Tribune", *The Express Tribune*, 2022, <https://tribune.com.pk/story/1574702/2-bewarehackers-going-atms-pakistan.>
33. The prevention of electronic and crimes act 2016, § 12.
34. R. Heickero, "Terrorism Online and the Change of Modus Operandi," Swedish Defence Research Agency, Stockholm, Sweden, (2007), 1-13.
35. Tariq Ahmad, Global legal monitor: "National Assembly passes new cybercrime law", Library of congress law, (September 21, 2016) <https://www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law>
36. The Prevention of electronic crimes act, 2016 § 10.
37. United Nations statistic division, ITU statistics "Cyber wellness Profile Islamic Republic of Pakistan," (December 2013) <<https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Pakistan.pdf>>
38. Kamal, Daanika. "„Policing Cybercrime: A Comparative Analysis of the Prevention of Electronic Crimes Bill‟." *Jinnah Institute, Policy Brief* (2017): 3-8.
39. Wardin, Katarzyna. "Book Review: Yoram Sweitzer, Sari Goldstein Ferber. (2005). Al-Qaeda and the Internationalization of Suicide Terrorism. Jaffe: Center for Strategic Studies, Telaviv University, Memorandum No. 78." *Rocznik Bezpieczeństwa Międzynarodowego* 2 (2007): 369-371;
40. 2016 SCMR 447.

References

[1] Bieda, David, and Leila Halawi. "Cyberspace: A venue for terrorism." *Issues in Information Systems* 16, no. 3 (2015): 33.

[2] Matusitz, Jonathan. "The role of intercultural communication in cyberterrorism." *Journal of human behavior in the social environment* 24, no. 7 (2014): 775-790.

[3] Azimi Bolourian, Ali, Yashar Moshfeghi, and C. J. van Rijsbergen. "SugarCube: quantification of topic propagation in the blogosphere using percolation theory." In *Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval*, pp. 786-787. 2009.

[4] Matusitz, Jonathan. "Cyberterrorism: Postmodern state of chaos." *Journal of Digital Forensic Practice* 3, no. 2-4 (2010): 115-123.

[5] Baggili, Ibrahim, and Marcus Rogers. "Self-reported cyber crime: An analysis on the effects of anonymity and pre-employment integrity." (2009): 974–2891.

[6] Orman, Levent V. "Technology as risk." *IEEE Technology and Society Magazine* 32, no. 2 (2013): 22-31.

[7] Bambauer, Derek E. "Censorship v3. 1." *IEEE Internet computing* 17, no. 3 (2013): 26-33.

[8] Ibid.

[9] The prevention of electronic and crimes act 2016, § 12.

[10] Lewis, James Andrew. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies, 2002.

[11] Mantel, Barbara. "Terrorism and the internet. Should web sites that promote terrorism be shut down?" *CQ researcher* 3, no. 1 (2009): 129-152.

[12] Denning, Dorothy E. "Cyberterrorism: Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism." (2000).

[13] Serge Krasavin, "What Is Cyber-Terrorism?" *Crime-Research.Org*, 2022, <https://www.crime-research.org/library/Cyber-terrorism.htm.> (accessed on 18th march 2022).

[14] Wardin, Katarzyna. "Book Review: Yoram Sweitzer, Sari Goldstein Ferber. (2005). Al-Qaeda and the Internationalization of Suicide Terrorism. Jaffe: Center for Strategic Studies, Telaviv University, Memorandum No. 78." *Rocznik Bezpieczeństwa Międzynarodowego* 2 (2007): 369-371; Schweitzer, Yoram, and Sari Goldstein Ferber. *Al-Qaeda and the internationalization of suicide terrorism*. Tel Aviv University, Jaffee Center for Strategic Studies, 2005.

[15] Cavelty, Myriam Dunn. "Critical information infrastructure: vulnerabilities, threats and responses." In *Disarmament Forum*, 3 (2007), 15-22.

[16] Beggs, Christopher. "Cyber-terrorism in Australia." In *Encyclopedia of Information Ethics and Security*, IGI Global, (2007), 108-113.

[17] Flemming, Peter, and Michael Stohl. "Myths and realities of cyberterrorism." In *Countering Terrorism through International Cooperation: Proceedings of the International Conference on "Countering Terrorism Through Enhanced International Cooperation". Milano: ISPAC*, (2001), 70-108.

[18] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", *Cybercrime Magazine*, 2022, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.> (assessed on 24th March 2022)

[19] Ibid.

[20] Cavusoglu, Huseyin, et al. "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers." *International Journal of Electronic Commerce* 9, no. 1 (2004): 70-104.

[21] Kostov, Nick, and Costas Paris. "Companies try to contain fallout from global cyberattack." *The Wall Street Journal, Dow Jones & Company* 28 (2017).

[22] Bergin, Anthony, Sulastri Osman, Carl Ungerer, and N. Yasin. "Countering internet radicalisation in Southeast Asia." Rajaratnam School of International Studies and Australian Strategic Policy Institute: *ASPI Special Report* 22 (2009).

[23] R. Heickero, "Terrorism Online and the Change of Modus Operandi," Swedish Defence Research Agency, Stockholm, Sweden, (2007), 1-13.

[24] Cassidy, John. "Why Edward Snowden is a hero." *The New Yorker* 10 (2013)

[25] "British E-Spy Agency Hacked Network Routers To Access Almost Any Internet User In Pakistan | The Express Tribune", *The Express Tribune*, 2022, (Assessed on 5th March 2020)

[26] Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." *Journal of Computer and System Sciences* 80, no. 5 (2014): 973-993.

[27] National Identity and Registration Authority (NADRA), which is Pakistan's most critical and key public agency, was attacked by Indian hackers in 2010.

[28] Salman Siddiqui, "Beware - Hackers Are Going After Atms In Pakistan | The Express Tribune", *The Express Tribune*, 2022, <https://tribune.com.pk/story/1574702/2-bewarehackers-going-atms-pakistan.> (Assessed on 06th March 2022)

[29] Mehwish Khan, "7-Point Action Plan Proposed For Cyber Secure Pakistan", *Propakistani.Pk*, 2022, https://propakistani.pk/2013/07/09/7-point-action-plan-proposed-for-cyber-secure-pakistan/.

[30] Anup Kaphle, *Pakistan Announces a National Plan to Fight Terrorism, Says Terrorists' Days are Numbered*, The Washington Post, (Dec 24, 2014)

[31] "Pakistan | Opennet Initiative", *Opennet.Net*, 2022, <<https://opennet.net/research/profiles/pakistan>>: Osman Husain, "Is the New Cyber-Crime Bill Akin to Banning the Internet in Pakistan?",*The express tribune* (blogs), Apr 20, 2015, <<http://blogs.tribune.com.pk/story/27245/is-the-new-cyber-crimebill-akin-to-banning-the-internet-in-pakistan/>>

[32] Mohammed, Furqan. "PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill." *UCLA J. Islamic & Near EL* 15 (2016): 71.

[33] Alvi, *supra* note 19. It is unclear why Zardari and his predecessor did not re-promulgate PECO 2009 as an ordinance in November 2009 when it lapsed.

[34] Tariq Ahmad, Global legal monitor: "National Assembly passes new cybercrime law", Library of congress law, (September 21, 2016) <https://www.loc.gov/law/foreign-news/article/pakistan-national-assembly-passes-new-cybercrime-law> (accessed on 29th Feb 2022).

[35] Prevention of electronic crimes act, 2016 § 10.

[36] Ibid

[37] Ibid § 10A, 10B.

[38] Farieha Aziz, "Pakistan cybercrime law: boon or bane", *Heinrich Boll Stiftun, the green political foundation*, (February 14, 2018), <<https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane>> (Accessed on 19th march 2022)

[39] 2016 SCMR 447.

[40] The "glory of Islam" basis is further problematic because it could be used to target religious minorities (*i.e.*, Christians and Ahmadi and Shia Muslims)

practicing their religion. Such an outcome would not be surprising because Pakistan officials already severely misuse the country's blasphemy laws against minorities

41 Mehreen Zahra-Malik, "Pakistan passes controversial cybercrime law", *world news,* (August 12, 2016)

42 Bolo bhi, "PECA: A THREE-YEAR REVIEW", <<https://bolobhi.org/wp-content/uploads/2019/11/Summary-of-Report-updated-18.10.2019.pdf>> (Assessed on 15th March 2020)

43 United Nations statistic division, ITU statistics "Cyber wellness Profile Islamic Republic of Pakistan," (December 2013) <<https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Pakistan.pdf>> (Accessed on 28th Feb 2022)

44 Kamal, Daanika. "„Policing Cybercrime: A Comparative Analysis of the Prevention of Electronic Crimes Bill‟." *Jinnah Institute, Policy Brief* (2017): 3-8.

45 Ibid.