The Impact of Globalisation on Cyberterrorism: A Global Perspective Analyses

Dr. Subhash Patil
Associate Professor and Head
Dept of Political Science
Rani Parvati Devi College of Arts and Commerce Belagavi, Karnataka India

Abstract *This paper examines the complex relationship between cyberterrorism and globalisation, emphasising how the modern world's interconnectedness has influenced the nature of cyberthreats. This article analyses the development of cyberterrorism within the framework of globalisation, looks at the main forces that have shaped this phenomenon, and evaluates the opportunities and threats it poses for international security. Moreover, it provides perspectives on possible tactics and regulations to lessen the dangers of cyberterrorism in the contemporary globalised world.*

Index Terms- globalisation, cyber terrorism, cyberthreats, nation-states, dark web, hybrid warfare, state actors, pseudonymity, and encryption

Introduction

The emergence of globalisation has brought about unprecedented interconnectedness and technological breakthroughs, revolutionising the way economies, governments, and society's functions but in addition to these advantages, globalisation has also brought forth a number of intricate new problems, chief among them being cyberterrorism. This paper examines the origins, expressions, and consequences of cyber terrorism for international security, examining the complex relationship between cyber terrorism and globalisation. Change in cyberterrorism. The complicated and multidimensional phenomenon that is the emergence of cyberterrorism has been influenced by changes in international politics, technological advancements, and the rising interconnection of the world.

Evolution of cyberterrorism:

Initial Period (1980s–1990s): Cyberterrorism has its roots in the early years of the internet, specifically in the 1980s and 1990s. Politically driven hackers, also known as "hacktivists," started using their expertise during this time to disrupt online services, deface websites, and advance their causes. The attacks were not very sophisticated and were more intended to spread awareness than to do significant damage. The internet grew quickly in the late 1990s, becoming more widely available and networked globally. Cyber terrorists have more opportunity to take advantage of holes in online systems as a result of the expansion of the internet. Cyberattacks were carried out by more organised individuals and groups for financial, ideological, or political motives. There was a discernible change in the direction of increasingly dangerous cyberterrorism in the middle of the 2000s. Nation-states began to realise that cyberattacks may be used as a disruptive and spying technique. Prominent incidents such as the Stuxnet worm (2010) brought to light the possibility of state-sponsored cyberattacks targeting vital infrastructure. Cyberattacks became significantly more sophisticated in the 2010s, and nation-states were increasingly involved. State-sponsored cyber espionage and sabotage activities increased in frequency, with North Korea, Iran, China, and Russia being frequently implicated. Targeted attacks, zero-day exploits, and sophisticated malware development all increased in frequency.

Geopolitical tensions and hybrid warfare

Cyberterrorism is now a crucial part of contemporary hybrid warfare tactics. Geopolitical conflicts have made it possible for state-sponsored cyberattacks, such as disinformation campaigns, electoral interference, and attacks on critical infrastructure. Despite having more limited capabilities than nation-states, on-state actors like terrorist organisations have also expressed ambition in obtaining cyber capabilities.

Future Trends and Emerging Threats:

Technological advancements will probably force cyberterrorists to adjust and create new strategies. It is anticipated that threats associated with quantum computing, artificial intelligence (AI), and the Internet of Things (IoT) will present new difficulties. While still in progress, international efforts to create standards and laws governing cyberspace are beset with formidable obstacles. From relatively simple hacktivist actions to highly complex and politically motivated attacks carried out by both nation-states and non-state actors, cyber terrorism has evolved over time. Cyberterrorism will continue to be a major security problem in the near future due to society's continued digitization and growing reliance on technology. To reduce threats, governments, organisations, and security specialists must constantly adapt and collaborate. Notable cases of cyberterrorism attacks have happened all around the world, affecting different industries and organisations. Significant repercussions have resulted from these occurrences, including risks to national security, disruptions of vital infrastructure, and monetary losses. The following are some noteworthy instances of cyberterrorism and their effects:

Stuxnet:(2010)

It is believed that a nation-state, most likely Israel or the United States, was responsible for creating the highly intelligent computer worm known as Stuxnet. By undermining centrifuges used in uranium enrichment, it especially targeted Iran's nuclear project. The result was significant harm to Iran's nuclear infrastructure. illustrated how important infrastructure may be affected by cyberattacks. heightened consciousness regarding state-sponsored cyberwarfare.

Attacks on the Ukraine Power Grid in 2015 and 2016:

Cyberattacks on Ukraine's power grid occurred twice, in December 2015 and December 2016. These attacks resulted in numerous power outages that affected hundreds of thousands of people. Consequences: it exposed weaknesses in global power grid systems and disrupted vital infrastructure with real-world repercussions. Concerns over nation-states using cyberattacks for military purposes have grown.

WannaCry Ransomware Attack: 2017

A ransomware outbreak known as WannaCry spread quickly around the world, infecting hundreds of thousands of machines in more than 150 nations. It took advantage of a Microsoft Windows vulnerability that the NSA had disclosed. The consequences include the suspension of essential services, including transport and healthcare. Losses incurred from paying the ransom and fixing the system. brought attention to the necessity of prompt software patches and cybersecurity procedures.

Not Petya (2017): Another ransomware outbreak, Not Petya, started off targeting Ukraine but swiftly expanded to impact companies all across the world. For many businesses, it resulted in major operational disruptions and financial losses. Widespread financial losses for the affected organisations are the result. shown how cyberattacks might have a significant impact on the economy. More attention is being paid to supply chain security.

SolarWinds Cyberattack (2020): A supply chain attack known as the SolarWinds cyberattack involved criminal actors compromising software updates from SolarWinds, a company that provides software that is often used by businesses and government agencies. The attackers were able to penetrate private networks, including those of US government organisations.

Repercussions:

Being exposed to private company and governmental information reduction of software supply chain security trust. The United States and Russia are embroiled in continuing investigations and diplomatic disputes. The 2021 attack on Colonial Pipeline ransomware: A ransomware attack that targeted Colonial Pipeline, a significant petroleum pipeline operator in the United States, hindered petroleum distribution on the East Coast. Price hikes and gasoline shortages are the results. identified weak points in vital infrastructure. heightened awareness of cybersecurity for vital energy infrastructure. These occurrences highlight the wide range of serious effects of cyberterrorism. In order to prevent and counteract cyberattacks, they emphasise the necessity of strong cybersecurity measures, international cooperation, and policies. Cyber terrorists will probably create new strategies as technology develops; thus, it is imperative that governments and companies continue to be watchful and aggressive in tackling these dynamic issues.

Globalisation and cyberterrorism

Since globalisation has given cyber terrorists access to possibilities and difficulties that were not as common in a less connected world, it has greatly increased their reach and influence. The following are some ways that globalisation has increased the effect and reach of cyberterrorism: One of the main pillars of globalisation is the internet, which links systems and individuals worldwide. Because of this interconnection, cyberterrorists can now reach a large worldwide audience and a variety of possible victims. Terrorist organisations are able to spread propaganda, find and connect with supporters, and plan international assaults.

Cyberterrorists can now act remotely and anonymously because of globalisation. Since they can attack from anywhere in the world, it is difficult for law enforcement authorities to find and capture them. Global supply networks are intricate and interrelated, leaving them vulnerable to disruption by cyberterrorism. Platforms for safe communication and the sharing of hacking tools and information are offered via anonymizing tools and the dark web. Supply chain disruptions can have a domino effect, impacting several industries and nations. For instance, delays in the manufacturing of essential components can affect a number of industries, including manufacturing and healthcare.

Flows of Money and Money Laundering: Globalisation makes it easier for money to travel across borders, which makes it easier for cyberterrorists to finance their operations and launder money. Terrorists now have more anonymous ways to raise and transfer money through cryptocurrencies and internet banking systems. concentrating on vital infrastructure Global interconnectivity characterises critical infrastructure, including power grids, transportation networks, and financial institutions. Cyberattacks on these systems may have far-reaching and permanent effects. The phenomenon of globalisation has given rise to concerns regarding national security as it has amplified the possibility of state-sponsored cyber terrorists attacking the vital infrastructure of other countries.

Cyberterrorists are able to work abroad with other groups or individuals who share their goals, exchanging knowledge, resources, and instruments. This international cooperation may increase the effectiveness and complexity of cyberattacks. Leveraging Regulatory Omissions: Cyber terrorists could exploit national variations in cybersecurity legislation and procedures. They can carry out operations in areas with inadequate cybersecurity safeguards in order to attack targets that are elsewhere more secure.

Disinformation and Information Warfare: Cyber terrorists can conduct disinformation operations and information warfare because of the internet's global reach. They have the ability to control social media, disseminate false information, and sway public opinion both domestically and globally. The nature of threats is transnational. Cyber threats do not respect national boundaries. Cyber terrorists can operate from another nation and target individuals and groups there, making it more difficult to identify the source of attacks and bring those responsible to justice.

The causes of cyberterrorism in the age of globalisation are intricate and varied. Cyberterrorism is on the rise due to the interconnection of the modern world and the rapid growth of technology. The internet, the spread of digital technology, and the development of increasingly powerful hacking tools have made it possible for cyber terrorists to launch more severe assaults. These are the main causes of cyberterrorism in the globalised era.

The Internet of Things (IoT) and artificial intelligence (AI) are examples of emerging technologies that give cyberterrorists new ways to target weaknesses. Because of the anonymity and covertness afforded by the globalised period, it is challenging for law enforcement to identify and apprehend cyber terrorists. Terrorists are able to conceal their identities and financial transactions through the use of tools like cryptocurrency and anonymizing networks.

International Recruitment and Communication: Cyber terrorists can connect, recruit, and plan with like-minded people and organisations all across the world over the internet. Social networking sites, encrypted messaging apps, and online forums offer avenues for radicalization and cooperation. Political and ideological disputes have arisen globally as a result of globalisation, which gives cyberterrorists an incentive to use cyberattacks to further their objectives. Through their internet activities, some groups hope to spread their views or call attention to perceived injustices.

Financial Gain: Cyber terrorists may wage financially motivated operations to extort money from people or organisations, such as ransomware attacks. Cybercriminals and terrorists may find great financial gain to be an attractive motivation. Globalisation makes it possible for cyberterrorists to work together across national boundaries, exchanging knowledge, resources, and instruments. Cross-border coalitions have the power to empower cyberterrorist organisations and expand the scope of their assaults.

State-Supported Assistance: Certain nation-states aiming to further their geopolitical objectives provide assistance or support to cyber terrorists. Espionage, sabotage, or attempts to overthrow rival nations may all be part of state-sponsored cyberterrorism. Cyber terrorists may find refuge in unstable or conflict-ridden areas, where they can operate largely unhindered. Cyberattacks from these areas may be aimed at foreign targets or nearby nations.

Risks Associated with Crucial Infrastructure: Critical infrastructure systems are now globally networked due to globalisation, which has made them appealing targets for cyberterrorists. Cyberterrorism can disrupt the production and distribution of goods and services by targeting key infrastructure, which can have a cascading effect on society, the economy, and national security. The global supply chain is intricate and linked, making it an attractive target for cyber terrorists. The effects of supply chain disruptions can be felt far and wide in the economy. Cyber terrorists may spread propaganda and information swiftly through the internet, which could hasten the radicalization of people. Cyberterrorism and the proliferation of digital technologies The Internet and the widespread use of digital technology have greatly strengthened the hands of cyberterrorists in a number of ways.

Obtaining Instruments and Methods: A plethora of knowledge, guides, and hacking tools that might be exploited maliciously are readily available on the internet. Cyberterrorists can create and use advanced cyberattack methods by utilising publicly accessible materials. Cyber terrorists can work anonymously and under pseudonyms on the internet, which makes it difficult for law enforcement authorities to identify and capture them. Because anonymity protects cyberterrorists from repercussions for their activities, more daring attacks are encouraged.

Worldwide Perception and Target Choosing: Regardless of their actual location, cyber terrorists may identify and target a wide spectrum of victims. With their ability to launch assaults from almost anywhere in the world, cyber terrorists can carefully choose their targets based on political, ideological, economic, or personal objectives. This eliminates the need for them to be physically close to their targets. The dangers connected to more conventional types of terrorism, such as bombings or physical assaults, are diminished by this distant capability. Cyber terrorists can propagate their attacks across the internet, potentially impacting a huge number of people at once. Global routes for disseminating propaganda and enlisting supporters are made available by social media sites and online discussion boards.

The exploitation of weaknesses: networks, software, and systems are exposed to multiple vulnerabilities due to the Internet and digital technology. These flaws can be used by cyberterrorists to obtain unauthorised access, interfere with services, or steal confidential data. The financial investment required for cyberattacks is typically lower than that of traditional types of terrorism. Cyberterrorism is a tempting alternative for individuals or small groups with minimal funds due to its lower costs. Technological Progress: Technological advancements, such as the capacity of computers to analyse information at ever-increasing speeds and the availability of high-speed internet, allow cyber terrorists to carry out increasingly sophisticated and destructive operations. Artificial intelligence and machine learning are examples of emerging technologies that can be used to automate attacks and evade detection.

Security and Encryption in Communication: Cyberterrorists are able to coordinate and communicate in secret because of the availability of encryption software and secure communication channels. Platforms for secure communication include encrypted messaging applications and dark web forums. Cyber terrorists can carry out financially motivated actions, such as ransomware attacks and online fraud, to raise money for their operations. Individuals and organisations are drawn to cybercrime by the possibility of financial gain. Cyber terrorists can use the vulnerabilities introduced by the interconnectedness of global supply chains to disrupt the production and distribution of products and services. Supply chain disruptions can have a significant impact on the economy and society.

The Dark Web and Cyberattacks The Dark Web and encrypted communication channels are vital to the functioning of international networks involved in cyber terrorism because they offer a hidden space for terrorists to coordinate, communicate, and carry out their operations. Below is a summary of their roles: 1. security and anonymity. The "Dark Web" is the portion of the internet that is inaccessible without specialised software like Tor and that is not indexed by conventional search engines. Both users and website proprietors can enjoy a high level of anonymity with it. 2. Encrypted Communication Channels: Telegram, WhatsApp, Signal, and other encrypted messaging apps and tools offer end-to-end encryption, guaranteeing that messages can only be decrypted and read by the intended receiver. 3. Safe Interaction: The Dark Web: Forums and markets on the Dark Web are frequently used by cyberterrorists for secure communication. These forums offer a venue for exchanging hacking tools or stolen data, talking about attack strategies, and spreading malware. 4. Encrypted Communication Channels: Secure communication is provided via encrypted messaging applications, which make it challenging for authorities to intercept and interpret messages. These platforms can be used by terrorists to organise events, disseminate propaganda, and organise attacks. 5. Transfer of Resources: The Dark Web: Cyberterrorists can obtain resources, services, and tools to aid in their operations through the Dark Web. This involves buying malware, hacking tools, stolen data, and even employing hackers to do particular jobs. 6. Encrypted Communication Channels: Financial transactions, including ransom payments and the sale of stolen data, can be negotiated and arranged using encrypted messaging applications. 7. Radicalization and recruitment: The Dark Web: To enlist new members and radicalise people, certain extremist organisations use the Dark Web. They might disseminate misinformation, violent training manuals, and extremist content. 8. Encrypted Communication Channels: Terrorists can disseminate their ideology and plan operations covertly by using encrypted messaging applications to enlist supporters and adherents. 9. Exchange of Information: Cyber terrorists might share information about exploits, vulnerabilities, and hacking methods in forums on the Dark Web. They can also exchange methods and plans for carrying out cyberattacks. Encrypted Communication Channels: Terrorists can quickly and safely exchange information thanks to encrypted messaging applications. When planning attacks or giving directions to lone individuals or small groups, this is extremely crucial. 10: Law enforcement evasion: The Dark Web: Because of its anonymity, law enforcement organisations find it challenging to investigate unlawful activities, locate and detain cyberterrorists, or determine the origin of cyberthreats. Encrypted Communication Channels: Attempts to get evidence and stop cyberattacks are hampered by encrypted communication applications, which make it more difficult for authorities to monitor and intercept communications.

Combating cyberterrorism

Cyberterrorism Governments, international organisations, and players in the business sector must work together to combat cyberterrorism, which is a complicated and diverse issue. To combat the threats presented by cyberterrorism, each of these stakeholders is essential. 1. Authorities: Legislation and Regulation: Laws and regulations pertaining to cybersecurity and cyberterrorism must be passed by and enforced by governments. They create legal frameworks that specify cybercrimes, their associated punishments, and the limits of their jurisdiction. 2. Law enforcement: Governmental organisations that look into cyberterrorism-related actions, find the offenders, and compile evidence for legal action include national law enforcement and intelligence organisations. 3. National Cybersecurity Strategy: National cybersecurity strategies, which outline a government's approach to protecting critical infrastructure, securing public systems, and lowering cyberthreats like those from cyberterrorism, are created and implemented by governments. 4. International collaboration: To foster international collaboration in the fight against cyberterrorism, governments take part in diplomatic initiatives and bilateral or multilateral agreements. 5. Cybersecurity Capacity Building: Governments invest in cybersecurity capacity building programmes to train law enforcement, cybersecurity experts, and government officials in cyber defence and incident response. They collaborate with other nations to share threat intelligence and coordinate responses. 6. Worldwide Organisations: United Nations (UN): The UN contributes significantly to the fight against cyberterrorism by encouraging member states to hold discussions, by promoting standards and guidelines for responsible state behaviour in cyberspace, and by pushing for the peaceful use of ICTs. 7. Interpol: Interpol helps member nations fight cybercrime, including cyberterrorism, by offering support in the form of operational coordination, sharing of threat intelligence, and capacity building. Through initiatives like the European Cybercrime Centre (EC3) and the Network and Information Security Directive, the European Union (EU) has established a comprehensive framework for addressing cyber threats, including cyber terrorism. Regional organisations, like the African Union (AU) and the Organisation of American States (OAS), work to strengthen cybersecurity cooperation and response mechanisms within their respective regions. 8. Private Industry Players: Protection of Critical Infrastructure: Private sector companies that run key systems like electricity, finance, and telecommunications work with governments to improve these systems' cybersecurity. They exchange threat intelligence and make investments in strong cybersecurity defences. 9. Cybersecurity Businesses: Private cybersecurity businesses offer goods and services to assist organisations in fending off online dangers, such as cyberterrorism. They are essential to the development of security solutions, incident response, and threat detection. 10. Information Sharing: To share threat intelligence and best practices, private sector businesses take part in industry-specific Information Sharing and Analysis Centres (ISACs) and information sharing initiatives. 11. Supply Chain Security: To stop the entry of compromised components or vulnerabilities into their goods and services, private sector players must secure their supply chains. This is essential for fending off supply chain-related cyberattacks. Public-private collaborations: These collaborations, which facilitate cooperation in combating cyberterrorism and strengthening the overall cybersecurity posture, are an example of how governments and private sector organisations can work together.

Measures for Cybersecurity: Cybersecurity measures are vital procedures, tools, and approaches that guard computer networks, systems, and data against hacker assaults, unauthorised access, and other security risks. These precautions are essential for maintaining the integrity of digital assets, guaranteeing business continuity, and protecting sensitive data. Here are a few crucial cybersecurity precautions: 1. Barricades: Network security tools called firewalls regulate incoming and outgoing network traffic in accordance with pre-established security standards. They filter traffic to stop unauthorised access and any dangers, serving as a barrier between a trusted internal network and an untrusted external network. Software for antivirus and anti-malware: Malicious software, including Trojan horses, worms, viruses, and spyware, can be found, blocked, and eliminated with antivirus and anti-malware software. These programmes aid in preventing malware and hacking attacks on endpoints, imputers, and other devices. 2. Patch Administration: To fix known vulnerabilities and security flaws, operating systems, software programmes, and firmware must be updated and patched on a regular basis. Patch management assists in thwarting cyberattacks that take advantage of vulnerable systems. 3. Control of Access: Access control procedures guarantee that certain resources, systems, or data are only accessible to authorised users. Strong authentication procedures, user access controls, and role-based access control (RBAC) are some of the techniques. 4. Cryptography: The process of transforming data into a safe format to guard against unwanted access or interception is known as encryption. Data at rest (like encrypted hard drives) and data in transit (like SSL/TLS for web traffic) are both secured by it. Systems for detecting intrusions (IDS) and preventing intrusions (IPS): IDS and IPS keep an eye on system activity and network traffic for indications of nefarious or suspicious activities. Whereas IPS can actively block or prevent threats, IDS identifies and warns about prospective risks.

Training on Security Awareness: Preventing human error and social engineering attacks requires educating users and staff about cybersecurity best practices. Training courses increase knowledge about safe online conduct, password security, and phishing. 1. MFA, or multi-factor authentication: By requiring users to give multiple forms of authentication, such as a password and a one-time code texted to their mobile device, MFA adds an extra layer of security. Even in the event that credentials are compromised, it lowers the chance of unauthorised access. 2. Plan for Incident Response (IRP): A cybersecurity incident response plan, or IRP, describes what should happen if a cybersecurity issue occurs. It assists in minimising harm, locating the attack's origin, and resuming regular activities. 3. Disaster Recovery and Data Backups: Frequent data backups guarantee that important data can be restored in the event that hardware malfunctions or cyberattacks cause data loss. Plans for disaster recovery describe how to restore IT services and infrastructure in the case of a significant disruption. 4. Network Division: By dividing a network into separate sections, network segmentation restricts an attacker's ability to move laterally in the event of a breach. It aids in containing and lessening the effects of cyberattacks. Regular vulnerability scanning finds flaws in systems and applications. Vulnerability testing also finds vulnerabilities in systems and applications. By simulating cyberattacks, penetration testers (also known as ethical hackers) can find vulnerabilities and fix them before bad actors can take advantage of them.

Security Guidelines and Adherence: Establishing and upholding compliance standards and security rules aids firms in maintaining a stable and safe cybersecurity posture. Many industries have standards and rules that must be followed (e.g., healthcare, finance). Constant observation and threat analysis: Network traffic, system logs, and endpoints are continuously monitored, which enables enterprises to identify and address security breaches instantly. Threat intelligence helps with proactive protection methods by providing information about new threats and trends. 6. Security Measures for Clouds: Protecting data in the cloud while using cloud services requires putting cloud security measures like identity and access management (IAM), encryption, and access management (AM) into place. Introduction: With the world becoming more interconnected, cyberterrorism has far-reaching and ever-changing effects.

Conclusion

This paper has offered a thorough examination of the relationship between cyberterrorism and globalisation, highlighting the necessity of concerted worldwide action to solve this urgent security issue. As the globe grows more interconnected and technology advances, it is crucial to be vigilant and take preventative action to protect against the threats posed by cyberterrorism.

References:

1. Ahmed, N. (2016). The Effect of Globalization: Terrorism and International Crime. IOSR Journal of Business and Management (IOSR-JBM).e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 18, Issue 11. Ver. III, PP 43-49.

2. Ali, A., Anjariny, A. H., Habib, S. A., and Nyakwende, E. (2018). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies." In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 608-621. IGI Global.

3. Benson, D. C. (2014). Why the internet is not increasing terrorism. Security Studies. Volume 23, Issue 2.

4. Berger, J. M. (2015). The evolution of terrorist propaganda: The Paris attack and social media. The Brookings Institution.

5. Bretherton, C. and Ponton, G. (1996). Global Politics: An Introduction. Oxford: Black well.

6. Center for Strategic and International Studies (CSIS). (1998). Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo (Washington DC: CSIS Press).

7. Christen, H. T., Denney, J, P., &Maniscalco, P. M. (2002). Weapons of Mass Effect: Cyber-Terrorism, in Paul M. Maniscalco& Hank T. Christen (Ed.s), Understanding Terrorism and Managing the Consequences, New Jersey: Prentice Hall, 194.

8. Collin, B. (1997). Future of Cyberterrorism: Physical and Virtual Worlds Converge. Crime and Justice International, 13(2): 15-18.

9. Conway, M. (2007). Cyberterrorism: Hype and Reality. Available at: http://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf

10. Cronin, A. K. (2003). Behind the curve.Globalization and international terrorism.International Security.Vol. 27, No. 3 2003.

11. Davis, E.L. (2003). Globalization Security Implications.RAND Issues Paper.

12. Denning, D. (2001). Cyberwarriors: Activists and Terrorists Turn to Cyberspace. Harvard International Review 23:2. Available at: http://www.hir.harvard.edu/articles/index.html?id=905

13. Gordon, S. and Ford, R. (2002). Cyberterrorism?636-637 & 641.

14. Hathaway, O.A., Crootof, R., Perdue, W and Levitz, P (2012).The Law of Cyber-attack".California Law Review.Vol.100, Issue 4. Pp. 817-886.

15. Hoffman, B. (2016). The Global Terror Threat and Counterterrorism Challenges Facing the Next Administration."CTC Sentinel 9, no. 11 (2016): 1-8.

16. Karacasulu, N. (2006). Security and Globalization in the Context of International Terrorism."UluslararasiHukukvePolitikaCilt 2, No:5. ss. 1-17. p. 3.

17. Martin, S. and Leonard B. (2016). Terrorism in an era of unconventional warfare." Terrorism and political violence 28, no. 2: 236-253.

18. Mates, (2001). Technology and Terrorism. NATO Parliamentary Assembly. Sub-committee on the proliferation of Military Technology.

19. Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., and Gagnon, G. (1991).Cyberterror: Prospects and Implications. Defense Intelligence Agency Office for Counterterrorism Analysis (TWC-1).Center for the Study of Terrorism and Irregular Warfare Monterey, CA

20. Podhorec, M. (2012). Cyber Security Within the Globalization Process. Available at: http://journal.dresmara.ro/issues/volume3_issue1/02_podhorec.pdf

21. Pollitt, M. M. (1998). Cyberterrorism: Fact or Fancy? Computer Fraud and Security: 8-10.

22. Shackelford, S.J (2013). Toward Cyberpeace: Managing Cyber-attacks through Polycentric Governance. American University Law Review.62 (5),1273-1364.

23. Hoo, S. K., Goodman, S. & Greenberg, L. (1997). Information Technology and the Terrorist Threat. 143.Survival Global Politics and Strategy. Volume 39, Issue 3

24. Stuart, A. A., Jarvis, M. L., and Chen, T. M. (2017). Introduction to the special issue: Terrorist online propaganda and radicalization. Studies in Conflict & Terrorism, 40(1), 1–9. doi:10.1080/1057610X.2016.1157402: 1-9.

25. Taylor, P. A. (1999). Hackers: Crime in the Digital Sublime. London: Routledge, 44-50.

26. Urbas, G., & Choo, K. R. (2008). Resource materials on technology-enabled crime.Australian Institute of Criminology, No. 28.