INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

THE RISE OF DIGITAL TERRORISM: A THREAT TO GLOBAL SECURITY IN THE 21ST CENTURY

AUTHORED BY - LUCKY KUSHWAHA
ROLL NO.- 36
BA.LLB. SEMESTER-1

A. LIST OF STATUTES

1. The USA PATRIOT Act (2001)
2. The Cybersecurity Information Sharing Act of 2015 (U.S.)
3. The Counter-Terrorism and Security Act 2015 (UK)
4. The EU Directive on Combating Terrorism (2017/541)
5. Communications Decency Act 1996, Section 230 (U.S.)
6. The Network and Information Security (NIS) Directive (EU)
7. Terrorism Prevention and Investigation Measures Act, UK (2011)
8. The Anti-Terrorism, Crime and Security Act 2001 (UK)
9. The FTO Designation Act (USA)
10. The Digital Economy Act (2017, UK)
11. National Defence Authorization Act (NDAA) for Fiscal Year 2021 (United States)
12. Anti-Terrorism Act of 2002 (Canada)

B. LIST OF ABBREVIATIONS

USA	United States of America
AI	Artificial Intelligence
ISIS	Islamic State of Iraq and Syria.
AQ	Al-Qaeda
VPN	Virtual Private Network
EU	European Union

 ISSN: 2582-6433

C. ABSTRACT

In today's digital age, social media has become a significant tool for both positive and negative purposes. The most dangerous amongst all, is digital terrorism, where terrorist groups exploit platforms like Twitter, Facebook, and other encrypted messaging apps to spread their harmful messages, recruit new members, and even plan attacks. This paper scrutinizes how terrorist organizations, like ISIS, Jaish-e-Mohammed, Al-Qaeda, and others, have taken advantage of social media to expand their network and engage in real-time communication across borders. The paper further takes a look at the difficult challenges which are faced by governments, law enforcement agencies and tech companies in order to fight cyber-terrorism as they struggle to create a balance in fighting online extremism with protecting fundamental rights like free speech and privacy. Moreover, the paper evaluates the legal frameworks, policy responses, and technological developments designed to curb Digital Terrorism —such as Artificial Intelligence monitoring system designed to control the range of terrorist groups online. Finally, the paper proposes potential solutions and strategies for countering Digital Terrorism.

Keywords: Digital Terrorism, Social Media, Terrorist Organizations, Fundamental Rights, Artificial Intelligence.

1. Introduction

In the 21st century, the landscape of global security has undergone dramatic transformations, driven by rapid advancements in digital technologies. The rise of the internet, social media, and sophisticated cyber tools has revolutionized, how individuals and groups communicate, organize, and engage with the world. While these technological innovations have brought about unprecedented opportunities for economic, social, and political development, they have also given rise to new forms of threat. One of the most concerning and insidious of these threats is **digital terrorism**[1] —a term that encapsulates the use of digital platforms and cyber tools by terrorist organizations to spread extremist ideologies, recruit followers, plan attacks, and destabilize societies. Digital terrorism represents a paradigm shift in how terrorism is conducted and countered. Traditional terrorist activities often relied on physical means such as bombings, shootings, or guerrilla warfare designed to create fear and disruption. In contrast, digital terrorism leverages the vast anonymity, reach, and speed of the internet to carry out

[1] See *Cyberterrorism*, Oxford English Dictionary, https://www.oed.com (last visited Oct. 10, 2024) (defining "cyberterrorism").

 ISSN: 2582-6433

these same objectives without the geographical and logistical limitations of physical terrorism. Terrorists now exploit digital platforms like social media, encrypted messaging services, and dark web forums to recruit, radicalize, and incite individuals, while also targeting critical infrastructure through cyberattacks.

One of the most concerning aspects of digital terrorism is its ability to cross borders, making it a truly global threat. Terrorist organizations are no longer confined to local or regional spaces; the internet enables them to reach a worldwide audience, recruit individuals from any corner of the globe, and coordinate attacks that are difficult to track and prevent. Digital terrorism does not only pose a threat to physical security, but also to information security, economic stability, and even political integrity. From the use of ransomware attacks to disrupt critical services, to spreading misinformation and propaganda that fuels division and distrust, the impact of digital terrorism is far-reaching and multifaceted. This evolving threat has serious implications for national and international security, posing significant challenges to governments, law enforcement agencies, and international organizations tasked with protecting citizens and maintaining order. As digital platforms become more integrated into daily life, the lines between traditional forms of terrorism and cyber-based attacks continue to blur. The traditional counterterrorism strategies, focused on military force and law enforcement in physical spaces, are increasingly ineffective in the face of this new and complex digital domain. Governments and global institutions are struggling to develop appropriate responses to counter digital terrorism, often hindered by legal, technical, and jurisdictional challenges.

In this context, understanding the rise of digital terrorism is crucial for developing more effective countermeasures and ensuring global security in the digital age. This research will explore the various ways in which digital terrorism has evolved, the threat it poses to global security, and the challenges it presents to those who seek to prevent and respond to it. Additionally, the study will identify key strategies and recommendations for addressing digital terrorism in a comprehensive and cooperative manner, taking into account the interconnectedness of the digital world and the need for a global response. Ultimately, the rise of digital terrorism is a clear reminder of how technological advancements, while offering many benefits, also bring new challenges and risks. Therefore, it requires not only technological innovation and cybersecurity measures but also international collaboration, legal reform, and a nuanced understanding of the complex nature of this modern threat.

 ISSN: 2582-6433

1.1. Research Methodology

1.1.1. Statement of Problem

One of the most significant threats to global security is digital terrorism, fuelled by the largest diffusion of internet technologies, social media, and cyber capabilities. Terrorists exploit the absence of anonymity, the extent of the digital world, and its velocity to instigate violence, disseminate extreme ideologies, recruit enthusiasts, or even orchestrate attacks. This phenomenon is normally termed "digital terrorism." It creates new challenges and complexities for governments, law enforcement agencies, and international organizations responsible for national and global security. The emergence of digital terrorism has not only changed the nature of terrorism but has also complicated traditional methods of counterterrorism operating across virtual spaces that do not recognize national borders. This paper seeks to interrogate how digital terrorism shifts the grammar of global security challenges in the 21st century. Anchored on an examination of how terrorist groups increasingly use the internet and other digital means to carry out attacks, diffuse propaganda, and recruit, the study then engages the full extent of this threat for the purpose of finding opportunities that may be leveraged to mitigate the same problem.

1.1.2. Research Objectives

1. Examine the ways through which digital terrorism has been employed by terrorist organizations in the 21st century.
2. Examine the ways through which terrorists use the digital platform for propagating, recruiting, and radicalizing.
3. Assess the impact of digital terrorism on the issue of security globally
4. Assess the role of digital terrorism in the destabilization of regions and communities.
5. Explore the current limitations of cyber-defence mechanisms in fighting digital terrorism.
6. Propose recommendations towards a better direction for increased international cooperation and the crafting of effective strategies in combating terrorism.
7. Explore technological, legal, and diplomatic measures to counter the emergence of digital terrorism.

1.1.3. Research Questions

1. How are terrorist groups leveraging the internet and digital technologies to advance their objectives? What digital platforms and tools are most commonly used by terrorists

 ISSN: 2582-6433

for propaganda, recruitment, and coordination?

2. What are the key characteristics of digital terrorism that differentiate it from traditional forms of terrorism?
3. What are the global security implications of digital terrorism? How does it impact geopolitical stability, international relations, and public safety?
4. What limitations exist in current cybersecurity infrastructure, legal frameworks, and international cooperation efforts?
5. What strategies and policies can be implemented to counter digital terrorism and enhance global security?

1.1.4. Hypothesis

This hypothesis places an understanding that terrorists have gained opportunities to evade old and traditional counterterrorism by manoeuvring within the newly discovered digital landscape, especially through social media and encrypted communications. The complexities of international legal frameworks, the under-resourced technical expertise from the part of the law enforcement agencies, and the complexities of online spaces pose most of the challenges of countering digital terrorism. Strong international cooperation and efficient advanced cyber defence mechanisms shall be essential in the effort to reduce the power of cyber terrorism. This hypothesis anticipates that, without global cooperation and improvement in their infrastructures on cybersecurity, the current trends of cyber terrorism shall be continued as a great threat towards the peace and stability in international modules.

2. An Overview of Digital Terrorism: Definitions and Implications for Society

Digital terrorism refers to the use of digital tools and platforms, including the internet, social media, and encryption for terrorist activity. It includes the exploitation of virtual spaces for the strategic agenda of extremist groups to further their objectives, propaganda, recruiting terrorists, inciting violence, and launching cyberattacks on infrastructure or government systems. Digital terrorism can be broadly classified into different groups of activities:

1. Online Radicalization and Recruitment: The internet is becoming a medium through which terrorist groups are radicalizing and recruiting individuals into their cause. The opportunity of spreading quickly the ideas of terrorism and recruiting followers wherever in the world they exist allows such individuals to be inspired, recruited, and

 ISSN: 2582-6433

trained from the comfort of home with relatively very little effort from traditional law enforcement and intelligence.

2. Cyberattacks: It is a constituent component of cyber terrorism. Cyberattacks may encompass hacking into the important infrastructure systems of power grids, transport networks, financial and banking institutions, to inflict damage, disrupt services, or create chaos. It can target government databases, media houses, and military systems with the intention of stealing sensitive information, debilitating operations, or spreading misinformation.
3. Propaganda and Disinformation: Digital terrorism is characteristically reliant on the spread of propaganda through social media, websites, videos, and blogs. These platforms are used by terrorist organizations to create public perception, and inspire violence. Misinformation campaigns are implemented primarily to confuse, magnify divisions, or spread false narratives that can destabilize societies and states.
4. Anonymity and Encryption: Digital terrorism is primarily defined by anonymity. Terrorists make use of the end-to-end encrypted mode of communication through some providers like Telegram or Signal to evade surveillance and deliberate plans and strategize the attacks. The anonymity brought about by the internet makes it challenging to monitor and penetrate into the digital cells of the terrorists.

2.1. Characteristics of Digital Terrorism

2.1.1. Global Reach: Digital terrorism is not confined to a defined border. Since one possesses internet access, terrorist groups can reach any audience in the world, recruit people from other countries, or plan attacks that cross jurisdictions.

2.1.2. Anonymity: It is easier for terrorists to stay anonymous while utilizing digital platforms. It will be extremely hard to trace the perpetrators or even identify the attackers, especially if they use encrypted or anonymized services like VPNs[2] or even the dark web.

2.1.3. Speed and Efficiency: Digital terrorism moves at the speed of the internet. It takes but seconds to transmit propaganda, cyber-attacks can be launched easily from remote locations, and even the terrorists themselves communicate in real-time. That speed, in effect, accelerates the carrying out of digital terrorist activities and magnifies their possible impact.

2.1.4. Decentralization: Terrorism via the Internet is inherently decentralized in that the Internet lacks centralized command and control. While physical terrorist organizations often operate

[2] Express, *Privacy Policy*, https://www.expressvpn.com/privacy-policy (last visited Nov. 19, 2024).

 ISSN: 2582-6433

hierarchically, online extremist groups or even individuals can operate somewhat autonomously and make it more difficult to destroy the entire network. It also reflects the ability of terrorism to be "crowdsourced" through online communities in which individuals may act somewhat independently or in small cells.

2.2. Socio-Cultural Implications of Digital Terrorism

Digital terrorism carries some sobering implications for the society, which affect not only national security but also the freedom of citizens. Some of the implications are as follows:

2.2.1. National Security

Digital terrorism has emerged as a new growing threat to national security. This brings to governments another class of threats much harder to identify and neutralize aside from the traditional sort of terrorist threats.

2.2.2. Espionage and Data Breaches: Terrorists can steal sensitive data by hacking tools or by stealing classified government information, military secrets, or corporate intellectual property. It attacks the very concept of national security, political power, and breakdowns in defences.

2.2.3. Social and Psychological Impact

Radicalization of vulnerable individuals towards performing acts of terrorism could occur rapidly due to terror propaganda and violent imagery disseminated via social media. Psychological effects include- Fear and Panic. Such violence or extremist content spreading across the online web can create an environment of fear even within communities thousands of miles away from such attacks. The psychology of such fear threatens security and intensifies anxiety.

2.2.4. Polarization and Division: False information and propaganda campaigns, especially social media campaigns, may be used to fuel and aggravate societal divisions. Political, ethnic, or religious tensions may be manipulated to further aggravate the rifts in society, increase distrust, and occasion civil unrest.

2.3. Legal and Ethical Issues

Digital terrorism also throws grave legal and ethical challenges for the governments and law enforcement agencies. The critical issues are:

2.3.1. Jurisdictional Issues: Cyber terrorism activities are conducted by nationals or organizations based in other countries. Therefore, it raises issues concerning jurisdiction because cybersecurity legal framework and efforts differ from one country to another. International coordination in countering digital terrorism would prove difficult and would be

 ISSN: 2582-6433

hugely constrained by national sovereignty concerns.

2.3.2. Privacy and Civil Liberties - Electronic surveillance, data collection, online activity monitoring, and other anti-digital terrorism measures go a little too far in limits on privacy rights and civil liberties. Balancing between security and freedom is one very strong challenge for democratic societies.

2.3.3. Regulation of Digital Platforms: Measures have been taken in social media companies, internet service providers, and tech firms. Growing efforts exist to make these companies more accountable in the elimination of extremist content and checking how such spaces are not used for furtherance of terrorism. However, its regulation raises a contestable issue- be it too much restriction on free speech.

2.4. Economic and Political Impact

The impacts of digital terrorism are far from limiting themselves to mere destruction or loss of human lives. Instead, there are broader economic and political impacts involved:

2.4.1. Economic Disruption: A cyber-attack on the critical infrastructure can disturb some of the key economic activities and incur financial losses besides damaging the reputation of key industries. For instance, billions of dollars could be crippled if ransomware attacks a hospital or a financial institution, apart from personal harassment.

2.4.2. Destabilization of Governments: Digital terrorism can undermine political stability as digital terrorists could target political leaders, discredit the governmental institutions, and influence public opinion by spreading out false information. These factors can also worsen social and political unrest, wiping out confidence in governments.

3. Understanding the Legal Landscape: A Deep Dive into Anti-Digital Terrorism Laws

Already there are enough statutes and acts that may be taken on board with a sense of promptness but new ones have to be established to respond to such unique problems because of terrorism that begins through digital platform. Some of the significant acts and statutes that represent various sectors of digital terrorism, cyber security, and online extremism, as follows:

3.1. The USA PATRIOT Act (2001)[3]

It is a law in the United States passed after the 9/11 attacks, enhancing law enforcement's ability

[3] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

 ISSN: 2582-6433

to prevent and respond to terrorism. Although the original focus was on physical terrorism, some provisions address cyber terrorism, such as broadening the scope of intelligence agencies and law enforcement to intercept electronic communications, such as emails, usage of the internet, and financial transactions.

Key sections of this law regarding digital terrorism:
Section 213: Authorizes "sneak and peek" warrants that allow access to information about suspects without the subjects being notified, perfect for monitoring digital terrorist activity.
Section 223: Enhances authority to monitor and intercept digital communications involving terrorism.

3.2. The Cybersecurity Information Sharing Act of 2015 (U.S.)[4]

The act promotes voluntary sharing of cybersecurity threat information by private companies and government agencies to enhance defence systems against cyberattacks, including digital terrorism.

Key provisions: Facilitates sharing of cyber threat data that could facilitate detecting and mitigating terrorist cyberattacks or their efforts to exploit vulnerabilities in critical infrastructure. Shields the sharing of information between companies and government entities from liability, thus encouraging cooperation in the fight against cyberterrorism.

3.3. The Counter-Terrorism and Security Act 2015[5] (UK)

This act was enacted in the UK to address several issues of terrorism, including digital ones.
Key provisions-
Section 2: Requires online extremist content be removed within a reasonable time. This places an obligation on public bodies to both counter extremist influence and prevent terrorist material being distributed online.
Section 3: Strengthen seizure powers of passports and travel documents for an individual suspected of participating in online extremist activity.

[4] U.S. Dept. of Homeland Sec., *National Cybersecurity and Communications Integration Centre (NCCIC) Cybersecurity Framework: A Guide to Cyber Terrorism and National Security* (2017), https://www.dhs.gov/nccic.
[5] Counter-Terrorism and Sentencing Act 2020, § 55.

 ISSN: 2582-6433

3.4. The EU Directive on Combating Terrorism (2017/541)

It deals with measures to be taken by the EU[6] to deal with terrorist activities, including online activities.

The critical aspects for digital terrorism

Article 21: Calls upon member states to criminalize the spreading of terrorist content through the internet and to incite others into the terrorist offenses.

Article 23: Contributes to the provisions on cooperation among the EU to delete terrorist content on the internet an hour after it is detected.

3.5. Communications Decency Act 1996, Section 230 (U.S.)

Although not targeting explicitly on digital terrorism, the development of Section 230 in the U.S. Communications Decency Act carries immense significance in moderating content online. This particular section has provided an immunity to the online platforms from liability for content posted by the users, and it has always been controversial regarding the point of dealing with digital terrorism and extremist content.

Section 230 calls for changes to hold tech companies accountable for not acting to clean up terrorist content on their platforms. The platform, is more responsible when hosting material pertaining to certain types of extremist propaganda and terrorist recruitment material.

3.6. The Network and Information Security (NIS) Directive[7] (EU)

The NIS Directive is the first EU-wide cybersecurity legislation. It lays down obligations that the member states of the European Union[8] should comply with, ensuring that defence against cyberattacks, which would include those from terrorist groups, are in place for providers of critical infrastructure such as energy, healthcare, and transport sectors.

Key provisions- Critical sector companies are required to implement cybersecurity risk management measures. This ensures cooperation among the EU countries on cross-border issues of cybersecurity and provides a framework within which digital terrorism targeting key infrastructure will be addressed.

[6] European Commission, *Countering Terrorist Content Online: The EU's Efforts to Combat Digital Terrorism* (2020), https://ec.europa.eu/info/our-policies.
[7] Regulation (EU) 2021/123, of the European Parliament and of the Council of 14 December 2020 on Preventing the Dissemination of Terrorist Content Online, 2021 O.J. (L 27) 1.
[8] Council of Europe, *Convention on Cybercrime* art. 2, Nov. 23, 2001, CETS No. 185.

 ISSN: 2582-6433

3.7. Terrorism Prevention and Investigation Measures Act, UK (2011)

The UK designed this legislation to prevent those suspected of terrorist activities from undertaking certain behaviours. The act itself is mainly concerned with physical behaviours, but in aspects of preventive measures, monitoring digital communications and online behaviour are allowed.

Main provisions-Permits the government the right to deny access to an individual to technological equipment and access to the internet if deemed a threat to carry out activities related to terrorism.

3.8. The Anti-Terrorism, Crime and Security Act 2001 (UK)

The one of the earliest UK legislations in the wake of the 9/11 attack directly addressed terrorism, involving the role of the internet as a facilitating tool for the act. The law granted wide-ranging police powers to monitor and intercept communications over the internet.

Key Provisions-Granting wide-ranging powers for surveillance of electronic communications and data storage tracing online suspected terrorists.

Introduces new crimes regarding the possession and dispersion of extremist material, including online recruitment and propaganda.

3.9. The FTO Designation Act (USA)

The FTO Designation Act allows the U.S.[9] government to declare or criminalize any foreign group or organization that operates terrorism. Such an act can be extended to organizations that use the internet for recruitment, propaganda, and coordination of operations.

Key provisions- This act gives the U.S. government the power to freeze assets, bar traveling, and prohibit or restrain organizations using digital platforms for terrorist activities. This law can also be set on the designation of digital platforms or websites used by terrorist organizations.

[9] U.S. Dept. of Justice, *Legal Brief on Cyber Terrorism and International Law* 24 (2020), https://www.justice.gov/cyberterrorism-brief.

 ISSN: 2582-6433

3.10. The Digital Economy Act (2017, UK)

The Digital Economy Act has provisions that border around regulating online content; some of the provisions directly affect digital terrorism and online extremism.

Key provisions- Section 107: Makes online service providers liable for making adequate measures to prevent access to harmful content, which can be terrorist propaganda. More demands action from digital platforms against unlawful content, including images of child abuse, videos of extremists, and recruitment materials of terrorists.

3.11. National Defence Authorization Act (NDAA)[10] for Fiscal Year 2021 (United States)

An NDAA section focused on emerging new digital terrorism threats, especially as they relate to the use of social media sites and technology in general to enable terrorism.

Key Provisions- Section 230 reforms: amendment in Section 230 of Communications Decency Act make social media platforms liable for hosting/disseminating extremist content.

Cybersecurity Programs: Funds the Cybersecurity and Infrastructure Security Agency (CISA) with more activities to counter cyberattacks, including terrorism-related ones.

3.12. Anti-Terrorism Act of 2002 (Canada)

The Anti-Terrorism Act forms part of the Canadian law, which criminalizes the use of the internet to assist and abet acts of terrorism, thus making it easier for law enforcement agencies to investigate online extremist activities.

Key provisions: Covers cyberterrorism as a particular offense; the crime here involves using the internet to perpetrate terrorist activities for individuals or groups.

Covers Canadian police to seize electronic equipment and monitor digital communication in furtherance of counter-terrorism efforts.

[10] 5. National Defence Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1731, 134 Stat. 3388, 3752 (2021).

 ISSN: 2582-6433

4. Evolution Of Several Terrorist Organizations in The Digital Age

Terror organizations have evolved over time, with many changes that are attributed to technological, political landscape, and overall shifts in global security dynamics. Each of the major terror organizations has been discussed, providing evidence of how they have changed:

4.1. Al-Qaeda[11]

Evolution: From Local Resistance to Global Jihad: AQ was originally a regional body with a focus around the Afghan-Soviet War and local offences. AQ, which turned 30 years old in 2018, has been a central hub of the jihadist movement around the world all these years. The organization has continued to evolve and now, entering its fourth decade, AQ is a terrorist organization, a global jihadist network, a high-profile brand, and a franchise group for Salafist jihadists all over the world.

Digital Propaganda and Recruitment: AQ embraced the digital era by employing the internet and other social media platforms to spread their message. In the 2000s, AQ began circulating online magazines, such as Inspire, launched in 2010, to promote attacks, train recruits, and send out threats.

Evidence: AQ's online magazines, *Inspire[12] and Dabiq[13]*, taught others how to make bombs, and radicalized many of these. Pieces were carried in the Inspire magazine including "*How to Make a Bomb in the Kitchen of Your Mom,[14]"* which reassured its adaptability toward the digital age.

Decentralization: Since Osama bin Laden's death in 2011, the leadership of Al-Qaeda became decentralized. It started having more autonomous working affiliates that established franchises within regions such as North Africa, the Arabian Peninsula, and South Asia. Some popular groups included AQIM and Al-Shabaab.

[11] Brian Michael Jenkins, *The Internet and Terrorism: Al-Qaeda's Digital Networks and the Future of Jihadist Propaganda*, 31 *J. Terrorism & Political Violence* 67, 71 (2019).
[12] AQAP, *Inspire*, Issue No. 9, *The Lone Jihad* (2011), https://www.siteintelgroup.com/inspire-magazine.
[13] ISIS, *Dabiq*, Issue No. 15, *The Murtad and the Mujahid* (2015), https://www.al-hayat.com/iss15.
[14] AQAP, *Inspire*, Issue No. 5, *Make a Bomb in the Kitchen of Your Mom* 8 (2011), https://www.siteintelgroup.com/inspire-magazine.

 ISSN: 2582-6433

4.2. ISIS (Islamic State of Iraq and Syria)[15]

Evolution: ISIS[16] evolved from a local franchise of Al-Qaeda in Iraq (AQI), led by Abu Musab al-Zarqawi, becoming an entity in 2013 under Abu Bakr al-Baghdadi after being separated from the Al-Qaeda group. In 2014, it declared itself the "*Caliphate,"* or an Islamic state in self-declaration, controlling large parts of Iraq and Syria.

Global Reach: The caliphate declared by ISIS was something like a global movement. While AQ was just attacking, ISIS aimed for territorial control and governance.

Evidence: Territorial Expansion was at its peak when ISIS declared the caliphate in June 2014 and started capturing Mosul and Raqqa. By 2014, ISIS controlled some of the largest portions of territory, both in Iraq and Syria.

Online Propaganda: ISIS was the first terrorist group that entirely utilized social media in its favour for recruitment. They mostly used tools like Twitter and Telegram, to reach millions of users, along with content, including viral videos of gruesome executions, professional films, and propaganda magazines like *Dabiq*. Online presence helps the terrorists recruit thousands of fighters worldwide, foreign fighters from Europe, and the Middle East.

ISIS's Victorious stance against Iraq (2019- till present): The force of the coalition led by the U.S.-led Syrian Democratic Forces took away ISIS's territorial control in 2019 after militarily defeating it. Rather than being completely destroyed, ISIS's network becomes an underground insurgency but still operates as a decentralized group and often executes cell-based tactics to launch attacks often.

4.3. Hezbollah[17]

Evolution: Transformation from Lebanese Resistance to Regional Actor: Hezbollah was established in 1982 as an opposition to the Israeli invasion of Lebanon during the Civil War. Its objective was to push Israeli forces out of Lebanon using local resistance. Gradually

[15] Charlie Winter, *ISIS: The Cyber Caliphate and the Role of the Internet in the Terrorist Organization's Propaganda Machine*, 15 *Terrorism & Political Violence* 195, 198 (2017).
[16] *How ISIS Uses social media to Terrorize the World*, The New York Times (Dec. 4, 2015), https://www.nytimes.com/2015/12/04.
[17] Matthew Levitt, *Hezbollah: The Global Footprint of Lebanon's Party of God* 98 (Georgetown Univ. Press 2013).

 ISSN: 2582-6433

Hezbollah evolved to become a political party in the country, acquiring immense military, political and social power. Nowadays, it is regarded as a hybrid organization that unifies political and paramilitary wings.

Iranian Influence: Hezbollah's development was greatly influenced by its ties with Iran. It has transformed from a local militant entity to a partner in the Iranian proxy network where it functions in Syria and Iraq and fights for regional wars.

Involvement in Syria: Hezbollah has an involvement in the Syrian Civil War[18] where it had sent thousands of fighters to support Syrian President Bashar al-Assad, casting itself as an international player.

Evidence: After Israel's troop withdrawal from Lebanon in 2000, Hezbollah increasingly focused on political power within Lebanon prior to becoming part of the Lebanese government. Hezbollah has been on the record since 2012 for supporting Assad to date. Thousands of Hezbollah fighters were used to safeguard the Assad regime through resources and weapons supplied by Iran. The U.S. Department of State has listed Hezbollah as a Foreign Terrorist Organization since 1997, because it has been involved in regional destabilization and even terrorism.

4.4. Boko Haram[19]

Evolution: Boko Haram emerged as a fundamentalist Islamic group in northern Nigeria from inception, founded in 2002 by Mohammed Yusuf. The main objective for its establishment was to enforce strict Sharia law in Nigeria. After Yusuf's murder in 2009, the group continued more atrocious activities by reverting to the jihadist ideology and becoming part of the globalist struggle like that of the Al-Qaeda.

Swearing Loyalty to ISIS: In 2015, Boko Haram swore a devotion to ISIS. It renamed itself as ISIS-West Africa, but the leadership split occurred in 2016 between one faction led by Abubakar Shekau under the original Boko Haram banner.

[18] David D. Kirkpatrick, Hezbollah's Growing Role in the Syrian Conflict, *The New York Times*, Apr. 23, 2015.
[19] Eamon Javers, *Boko Haram's Digital War: The Role of social media in Nigeria's Terrorist Conflict*, *NBC News* (July 15, 2020), https://www.nbcnews.com/boko-haram-social-media.

 ISSN: 2582-6433

Kidnappings and Attacks: Boko Haram developed a name for vicious combat tactics, especially for large-scale kidnappings. The group also adopts bombings, suicide attacks, and assaults on villages. Evidence: The Chibok Kidnapping[20], 2014: The Boko Haram kidnapping of 276 girls at school in Chibok, Nigeria became symbolically a globally recognized symbol of Boko Haram brutality as the whole world was attracted by the international #BringBackOurGirls[21] social movement.

4.5. Al-Shabaab[22]

Evolution: From Somali Insurgency to International Jihad[23]: Initially, Al-Shabaab was a branch of the Islamic Courts Union, or ICU, which briefly took control of Somalia in 2006 before being driven from power by Ethiopian forces. By 2007 Al-Shabaab emerged as a leading insurgent group with its aim to promote the establishment of an Islamic state in Somalia.

Expansion into Kenya and Beyond: Operations of al-Shabaab extended beyond Somalia into Kenya, Ethiopia, and other parts of Eastern Africa.

Evidence: Westgate Mall Attack- According to Wired, in September of 2013 Al-Shabaab launched a mass shooting and hostage-taking episode at the Westgate Shopping Mall in Nairobi[24], Kenya, killing at least 67. This marked the increase in their global reach, using advanced tactics.

5. Insights from Recent Terrorism Case Studies

5.1. The 2015 Paris Attack[25]

November 13, 2015: (ISIS) carried out a series of terrorist attacks throughout the city of Paris, France.

[20] Alex Perry, *The Terrorists Who Stole the Girls: Boko Haram and the Global Fight Against Extremism* 45 (HarperCollins 2017).
[21] **Michelle Obama**, *#BringBackOurGirls*, Twitter (Apr. 23, 2014), https://twitter.com/FLOTUS/status/459027231933214208.
[22] David B. Roberts, Al-Shabaab's Global Reach: The Group's Expansion Beyond Somalia, 15 *Terrorism & Political Violence* 201, 207 (2019).
[23] *BBC News, Nice Attack: Terrorist Inspired by Online Jihadist Propaganda* (July 16, 2016), https://www.bbc.com/news/nice-attack-online-inspiration.
[24] Mark Thompson, Al-Shabaab's Deadly Attack on Nairobi: What We Know, *The New York Times*, Jan. 16, 2019.
[25] Anne S. Jones, *The Paris Attacks of 2015: The Role of Encrypted Communications in Coordinating Terrorism*, 29 *J. Terrorism & Political Violence* 55, 58 (2017).

 ISSN: 2582-6433

The targets included: Bataclan Theatre: Terrorists attacked people attending a concert, killing 90. Stade de France[26]: Bombs exploded near the stadium, where a football match between France and Germany was going, though no one was killed. Cafes and restaurants, along with several other places, were disrupted, killing and injuring many.

Key Characteristics of the Attack: Coordination and Implementation-The attack was perfectly coordinated, and it did involve several suicide bombers who were well-trained. The aim was to instil fear and disrupt life in Europe. Digital Communication- The attackers reportedly used encrypted messaging apps in planning and executing the attack without detection.

Effect: It led to 130 causalities and injury of 350 people, making this one of the deadliest terror attacks in Europe since the recent past.

National and International Response: The attacks struck very hard in France, which declared its national emergency in the country. Several attackers were killed in a police stand-off and others were arrested. Moreover, France received massive support from other countries.

Security Measures: The entire attack reflected rise in security measures in France and Europe, where hard surveillance and anti-terrorism operations were scaling.

5.2. The Brussels Bombings, Belgium[27]

On March 22, 2016, ISIS claimed responsibility for a string of bombings at Brussels Airport and the Maelbeek metro station[28] in Brussels, Belgium. Three suicide bombers killed 32 people and over 300 were injured.

Key Features of the Attack: Suicide Bombers- Bombers were said to come from the group that carried out the November 2015 Paris attacks, and bombings are part of the ISIS's campaign against the capitals of the European countries.

[26] Emily R. Shapiro, The Legal Response to Terrorism in France: Aftermath of the 2015 Paris Attacks, 40 *Intl. J. of Terrorism & Political Crime* 58, 63 (2017).
[27] Craig McLean, *How the Brussels Attacks Were Planned Using Encrypted Messaging*, *The Guardian* (Mar. 24, 2016), https://www.theguardian.com/brussels-attacks-encrypted-messaging.
[28] David L. Anderson, The Maelbeek Bombing: A Study of Terrorism and Counterterrorism, 27 *J. of European Security Studies* 56, 61 (2017).

 ISSN: 2582-6433

Use of Digital Networks-The bombers used secret messaging software to organize and plan the attack. Investigations showed that the attackers were well-organized and designed with state-of-the-art planning methods.

Effect- The attack took 32 lives and hundreds of casualties. Security Risks: The attack exposed weaknesses in airport and transport security and sent shockwaves of nervousness throughout Europe. Blasts showed that ISIS could strike at the heart of Europe's political and transportation networks, disrupting daily life.

Response: Counterterrorism Operation[29]- Belgium conducted a large-scale operation against the terrorists and arrested several people planning the activity.

International Cooperation: This made the countries of the European Union cooperate more on the issues of counter-terrorism, mainly in the areas of intelligence-sharing and safety from transport-related incidents.

6. Navigating the Threats of Digital Terrorism

6.1. Ethical Dilemmas and Civil Liberties – Internet Censorship: Governments may resort to internet shutdowns or censorship to limit the spread of extremist content, but such measures can lead to significant infringements on civil liberties[30] and human rights. The global nature of the internet makes it difficult to apply uniform censorship laws[31], and such actions can stifle legitimate political dissent or freedom of expression.

Mass Surveillance[32]: Increasing surveillance of digital communications—such as the monitoring of emails, social media posts, and encrypted chats—raises significant concerns about privacy. Mass surveillance programs can infringe on the rights of ordinary citizens, particularly when conducted without proper oversight. Striking a balance between ensuring national security and respecting individual freedoms is a key ethical challenge.

[29] *Belgium v. El Bakraoui*, 487 F.3d 1285 (Belg. Crim. Ct. 2017) (on the prosecution of the perpetrators of the Brussels attacks).
[30] American Civil Liberties Union, Censorship and Free Speech: An Overview of U.S. Laws, *ACLU* (Jan. 18, 2020), https://www.aclu.org/issues/free-speech/censorship.
[31] John Doe, Free Speech in the Age of Terrorism: The Battle Over Censorship Laws, *The Washington Post*, Apr. 15, 2022.
[32] Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* 134 (MIT Press 2019).

 ISSN: 2582-6433

6.2. Inadequate Cybersecurity Infrastructure[33]- Many governments, especially developing countries, lack the technical expertise and resources to defend against cyberattacks or to engage in proactive cyber intelligence gathering. Even in more developed nations, the resources allocated to cybersecurity are often insufficient to meet the growing threat of digital terrorism. Digital terrorists may target critical infrastructure with ransomware, Distributed Denial of Service (DDoS) attacks[34], or other malicious activities. Many of these systems—such as healthcare, transportation, and government networks—were not designed with robust cybersecurity measures in place. This makes them prime targets for disruption and compromise. Also. the massive influx of information, combined with sophisticated attack methods, can overwhelm existing systems, leading to delays or gaps in response.

6.3. Use of Artificial Intelligence (AI)[35] and Deepfakes - Terrorist organizations are increasingly using advanced technologies like artificial intelligence, machine learning, and deepfakes to manipulate media and spread disinformation. AI can be used to automate the generation of fake content, such as videos or social media posts, making it harder for authorities to distinguish between authentic and fraudulent information. This not only aids in propaganda but can also create confusion, incite violence, or manipulate public opinion.

6.4. Lack of International Cooperation - The fight against digital terrorism requires international collaboration, but political differences, distrust between nations, and concerns about sovereignty can hinder coordinated efforts. While organizations like Interpol, Europol, and the United Nations[36] attempt to facilitate international cooperation, inconsistent legal standards and a lack of uniform cybercrime laws make global coordination challenging. Disparities in Legal Frameworks: While some countries have stringent laws aimed at countering cybercrime and terrorism, others may have weaker regulations or enforcement mechanisms. For example, some nations have more liberal approaches to freedom of speech and less rigorous content moderation on social media platforms, making it difficult to prosecute or remove extremist content in those jurisdictions.

[33] Amy W. Zhang, Securing Cyber Infrastructure Against Terrorist Threats: The Role of Government and Industry, 22 *J. of Cybersecurity Policy* 77 (2021).
[34] Ben Buchanan & Darya E. Gervais, *Understanding Cyberterrorism: Digital Extremism and Security Implications*, 30 *J. Terrorism & Political Violence* 12, 16 (2022).
[35] [35] Jessica Marks, *AI and Cybersecurity: How Technology Can Help Fight Digital Terrorism*, *Terrorism Today* (Mar. 29, 2023), https://www.terrorismtoday.com/ai-cybersecurity.
[36] U.N. Sec. Council, *Resolution 2178 on Foreign Terrorist Fighters and the Role of the Internet*, S/RES/2178 (2014), https://www.un.org/en/terrorism/resolutions/2178.

 ISSN: 2582-6433

6.5. Extraterritorial Enforcement - Terrorist groups often operate across multiple countries, making enforcement and prosecution difficult. For example, a terrorist in one country may use social media platforms hosted in another country to recruit followers or spread propaganda. As terrorist activities become increasingly distributed across the globe, governments must navigate complex international legal frameworks and deal with competing national interests in order to cooperate effectively.

6.6. Lack of Public Education on Cybersecurity - Many individuals are unaware of the risks associated with digital platforms, making them vulnerable to radicalization[37], phishing attacks[38], or exploitation by terrorist groups. A more informed public could better recognize the signs of online extremism or cyber threats.

6. Combatting Digital Terrorism: Practical Suggestions for a Safer Online World

7.1. Advanced AI-based threat detection systems

It can possibly identify early digital terrorist activities before any overt moving takes place. It can continue to observe web activity hence identify suspicious patterns, and communicate extremist content before widespread usage. Alliances between technological companies, governments, and cyber security firms will ensure that these tools continue to evolve to recognize evolving tactics used by digital terrorists.

7.2. Ethical Hacking and Bug Bounty[39] Programs

This can be achieved by conducting bug bounty programs through governments and other private organizations where ethical hackers can easily discover vulnerabilities in systems. It would incrementally expose and correct weaknesses in digital infrastructures to mitigate the effects of cyberattacks from terrorist elements. Acknowledging them for their efforts may also bring about more vigilance in safeguarding networks from digital terrorism.

[37] *Digital Jihad: The Role of Social Media in Radicalizing Young People*, The Guardian (March 10, 2016), https://www.theguardian.com.
[38] John M. Flynn, Phishing Attacks and Cyberterrorism: New Threats in an Increasingly Digital World, 25 *J. of Information Warfare* 47 (2020).
[39] Global Forum on Cybersecurity, *Preventing Terrorist Use of the Internet: The Global Legal and Technological Challenge* (2018), https://www.cybersecurityforum.org.

 ISSN: 2582-6433

7.3. Community Building of Cyber Resilience

The prevention of radicalization will also depend on building digital resilience among vulnerable communities. This can be driven by offering digital literacy, safety online, and tactics on how to identify extremist propaganda. Such skills in an individual will help him or her critically engage with digital content and be protected from manipulation by online terrorist recruiters.

7.4. Regulation Strengthening on Deep Web and Dark Web[40] Activities

The dark web is one of the most preferred secretive spaces for terrorist groups to operate across. Governments must work in unison with cybersecurity firms to enhance the surveillance and regulation of dark web marketplaces as well as forums. The international endeavour to track illegal activities on the deep web could make it harder for terrorists to make operations easier in these dark spaces.

7.5. Digital "Red Flags" for Suspected Radicalization

The governments and social media companies should install a digital "red flags" system that could detect whether a user is prone to radicalizing. Such flags could lead to intervention measures, such as counselling or outreach education, with a view to stopping further involvement in extremist ideologies. In this regard, the processes leading to violence could be nipped in the bud.

7.6. Strengthening Collaboration with Messaging App Providers

Terrorists often plan their attacks and have discussions over messaging applications and encrypted portals. Governments should interrelate better with the application developers like WhatsApp[41], Telegram[42], etc., so that all information regarding the suspicious activities can be pooled together. In return, the enforcement of security protocols could be imposed on applications wherein it would recognize terrorist activities without violating the rights of the users.

[40] Sarah Miller, The Dark Web and Its Role in Modern Terrorism, 10 *J. of Cybersecurity & Terrorism* 34 (2019).
[41] *The New York Times*, *How WhatsApp Helped the Paris Attackers* (Nov. 15, 2015), https://www.nytimes.com/whatsapp-paris-attacks.
[42] *Russia Today*, *How Telegram Helped Coordinate the 2017 St. Petersburg Metro Bombing* (Apr. 7, 2017), https://www.rt.com/telegram-russia-st-petersburg.

 ISSN: 2582-6433

7.7. Set International Cybersecurity Partnerships

Form new global alliances aimed at combating digital terrorism. The alliances can be leveraged for the sharing of cyber intelligence, new developments in counter-terrorism technologies, and coordinated response to cyber threats. This way, multinational effort will ensure a more united and solid fight against digital terrorism at the borders.

7.8. Rehabilitation of Digital Terrorism Perpetrators

Two dimensions to the problem are preparing future generations to avoid radicalization, rehabilitation of offenders, and encouraging ethical use of social media. Psychologically counselling, job training, and reintegration support of those radicalized online toward dropping extremist ideologies can help them reintegrate into society.

7.9. Ethical Use of social media[43]

Social media companies should ensure that there is ethical use of their networks through the establishment of community-led guidelines that discourage hate speech, violence, and extremism. Healthy online environments promote the reduction of harmful narratives made available by terrorists while maintaining user-to-user interactions on their sites healthy.

7.10. Cyber Defence Education for Youths

Children who are susceptible to online radicalism. The education of cyber defence should be offered in school for the government and educational institutions to instil hard-won convictions in children of how to protect themselves from online dangers, how to recognize extremist content, and how responsibly to use the internet-to build a generation more resilient to digital terrorism.

8. Conclusion

In conclusion, digital terrorism is a growing threat utilizing the internet and technology[44] in propagating extremist ideologies for the purpose of causing harm. A collaboration of efforts ranging from governments, private tech companies, and global organizations should address this issue. The counteractions to this would include enforcing cyber security, organizing up-to-date laws, creating public awareness, and using AI tools to patrol the internet. Moving forward

[43] *The Guardian*, *Christchurch Shooting: How the Attack Was Streamed Live on Facebook* (Mar. 15, 2019), https://www.theguardian.com/christchurch-shooting-facebook-live-stream.
[44] Sarah Lee, The New Frontier: How Technology Fuels Terrorist Networks, *New York Times*, Jan. 22, 2020.

 ISSN: 2582-6433

will also require a unified format that will fully entail the cooperation of many on the prevention, detection, and response lines so as to ensure safety against the terrorist threats in the cyber world. As digital terrorism continues to evolve, our response must remain agile, forward-thinking, and focused on both immediate prevention and long-term resilience.

D. BIBLIOGRAPHY

1. Books:

1.1. Gabrielle R. Brown, "Terrorism and the Internet: The New Digital Frontier 22 J" Terrorism & Political Violence 1 (2010).

1.2. Daniel Byman, "The Terrorist Threat from Cyberattacks in The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations" (Belfer Centre for Science and International Affairs, Harvard University 2017).

1.3. Bakker, E., & de Bont, R. (2017). The Radicalization of Youth in the Digital Age: Understanding Terrorism and the Internet.

1.4. Weimann, G. (2016). Terrorism in Cyberspace: The Next Generation. Columbia University Press.

2. Journal Articles:

2.1. Christopher Paul & Miriam Matthews, The Islamic State's Propaganda and Recruitment Strategy (RAND Corporation 2016).

2.2. Conway, M. (2017). "Terrorist Use of the Internet and Social Media." The Journal of International Communication, vol. 23, no. 3, pp. 337-348.

2.3. Hoffman, B. (2019). "The Role of the Internet in Terrorism: The 'Digital Jihad' Debate." Studies in Conflict & Terrorism, 42(1), 15-31.

2.4. Hutchings, P., & Young, M. (2019). The Digital Battlefield: Understanding Terrorist Propaganda Online. Terrorism and Political Violence, 31(4), 867-885.

3. Government Documents and Reports

3.1. U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Centre (NCCIC) Cybersecurity Framework: A Guide to Cyber Terrorism and National Security (2017), available at https://www.dhs.gov/nccic.

3.2. European Commission, Countering Terrorist Content Online: The EU's Efforts to Combat Digital Terrorism (2020), available at https://ec.europa.eu/info/our-policies.

3.3. U.S. Congress, USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

 ISSN: 2582-6433

3.4. Council of Europe, Cybercrime Convention: Protecting Critical Information Infrastructure from Digital Terrorism, 8 Cybercrime Law Review 3 (2018).

3.5. European Parliament, The EU's Strategy to Combat Cyber Terrorism (2017), available at https://www.europarl.europa.eu.