# Study of Non-State Actors and Digitalized Methods of Terrorism

Syed Haris Shah[*] & Maryam Baloch[**]

**Abstract**

*Terrorism has long been a problem for the world community, and it also impedes the progress of many developing nations. Since the rise of digitalized and cyber capacities in terrorist networks, the task has increased in difficulty and reached an advanced level for the non-traditional security arena. Although there are numerous advantages of the internet, it may also be used to spread information within terrorist organisations. Using digital information to radicalise target audiences for recruitment into terror networks or prepare illegal intimidation actions. These digital spaces promote their objectives. Although advancements are made to improve our lives, radicals, criminals, and even non-state organisations frequently abuse them. A number of terrorists today use big data, sophisticated networking systems, and cryptography in addition to other digitalized components. Therefore, it is crucial that non-state entities are restricted from doing such activities.*

**Keywords**: Terrorism, Cyber-Security, Non-State Organizations.

[*]Syed Haris Shah is serving as Research Assistant with Research Center for international Maritime Law and Practice. His areas of interest are Afghanistan, Post-Conflict Peacebuilding, Terrorism. Terror Financing, Maritime Security and Human Rights. He can be reached at sharishah99@gmail.com.

[**]Maryam Baloch retains her interests in areas of Pakistan-India Relations, Hindutva Extremism, Counterterrorism, Big Data Politics and cybersecurity. She can be reached at maryambaloch1281@gmail.com.

## 1. Introduction

Technological advancements have not only created new opportunities for society, but they have also given terrorists, criminals, and other anti-social forces new ways to influence societies. Social media sites like Facebook, Instagram, and Twitter have altered how people communicate, giving radicals new ways to spread their ideas and incite violence. Criminals have also been communicating with one another on any illegal or terrorist acts through these social media platforms. These technological advances are being used by extremists for communication, to incite hatred and terrorism, to raise money, to further their objectives, to publicize crimes, to gain sympathy and supporters, and even to teach their team members. Social media platforms can be thought as facilitating elements for such terrorists because they are quick, cheap, and accessible.

Islamic State of Iraq and Syria (ISIS), Al-Qaeda, Al-Shabab, Boko Haram, and the Revolutionary Armed Forces of Colombia (FARC) are just a few of the terrorist groups that use this medium of high-tech tools, and quick-moving information. According to a source, terrorist groups may potentially use PlayStation games for communication because it is difficult to decrypt information sent over the console.[1] This is in addition to social media. In terms of politics or religion, the complex phenomenon known as extremism can be characterized as defiance of conventional wisdom and rigidity in particular actions or ideals. Extremism nowadays can take many forms,

[1] Luke Graham, "Terrorists Are Using PlayStation 4 to Communicate: Lawmaker," *CNBC*, November 16, 2015. https://www.cnbc.com/2015/11/16/terrorists-using-playstation-4-to-communicate.html

including religious, right-wing, left-wing, political, etc. This can then result in severe acts of violence.

**2. Cyberspace Conflict**

The increasing importance of computational techniques has changed the terrain of conflict from conventional physical combat to cyberspace in both national and international contexts. Armed or military engagements that previously occurred on land, in the water, the air, or in space are now carried out via a variety of channels of artificial information technology. The use of technology to interfere with networks is referred to as cyber conflict, also known as cyberwar, cyberwarfare, and information war. The significance of this type of warfare has increased to the point where even states now engage in conflict using a virtual environment. Every day, violent cyber confrontations occur, and various cyber weapons are employed. The nature of cyberwarfare differs significantly from traditional warfare in that it is less expensive, requires no physical presence, is less likely to be detected, is challenging to identify the oppressor, and is accessible to all parties to a dispute. Since the scope of these severe fights is threatening national security and sovereignty, nearly every state has developed an effective cybersecurity framework to fend off cyberattacks. Cyberattacks, which can be carried out by people or organizations anywhere in the world, have the potential to harm a state's infrastructure. It is obvious that machine learning is currently a battleground in many technical fields.

### 3. Cyber Terrorism

The combination of cyber activities and terrorism refers to "the activities of violent extremism carried out via virtual platforms".[2] The violent actions can be directly carried out through cyberspace or this platform can be used indirectly as a facilitating actor for their motives. Cyber terrorism also called Techno Terrorism refers to the violence that can be directly conducted through the internet from an internal or external matrix. Tracing back the roots of cyber terrorism, the USA declared 15 organizations as international terrorist organizations in 1998 and all of them subsequently showed their virtual presence.[3] Terrorists had already concentrated on cyberspace because there are no boundaries or cross-checks on virtual platforms thus it is not easy for state officials to identify or hit the target. Different acts of cyber terrorists vary from privacy violations to propaganda and promoting hate material and financing. Types of cyber-terrorist attacks include hacking, denial of service, mutilation of websites, and simple or advanced unstructured and complex coordination.[4] During an interview with Al Emarah, Taliban leader Abdul Sattar while mentioning the importance of cyberspace maintained that, "Wars today cannot be won without media".[5]

[2] Conway and Maura, "Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 77-98.
[3] Cronin and Audrey Kurth, "How al-Qaida ends: The decline and demise of terrorist groups," *International Security* 31, No. 1 (2006): 7-48.
[4]Albahar and Marwan, "Cyber-attacks and terrorism: a twenty-first century conundrum," *Science and engineering ethics* 25, no. 4 (2019): 993-1006.
[5] Bashir Ahmad Gwakh, "The Taliban's Internet Strategy," September 09, 2011. https://www.rferl.org/a/the_talibans_internet_strategy/24323901.html

## 4. Research Method

By examining the contents of several websites, this study uses the content analysis method. Random social media channels that are used by terrorist organizations to spread their beliefs are investigated for the content analysis method. To assess the content; themes and categories are developed. An observation technique was also utilized to determine the techniques employed by such organizations for their online content.

## 5. Discussions and Findings

The latest and the most influential tool of cyberspace in the present age is social media, being the cheapest and the most easily accessible. Social media is used by 4.48 billion people as reported in 2022.[6] From Islamist groups like Tehreek-e-Taliban Pakistan (TTP), Moro Islamic Liberation Front (MILF), Ansar-al-Islam, Hizbul Mujahideen, Al Qaeda[7] as well as groups with other motives like the defunct Liberation Tigers of Tamil Eelam (LTTE)[8], the Kurdistan Workers Party (PKK)[9] and the Baloch Liberation Army (BLA), almost all the non-state actors and extremist organizations now own accounts or pages on social media including Twitter, Facebook, WhatsApp, Instagram, Telegram and other platforms. Through such digital and computational venues, these organizations improved their strategies and expanded their influence. Even though some terrorist groups, such as Al Shabab and

[6] Brian Dean, "Social Network Usage & Growth Statistics: How Many People Use Social Media in 2022?" *Backlinko*, October 10, 2021, https://backlinko.com/social-media-users

[7] Dave and Aaditya, "Transnational Lessons from Terrorist Use of Social Media in South Asia," *Royal United Services Institute for Defence and Security Studies*, 2019.

[8] Ariyapperuma, A., "Use of Visual Media by LTTE Front Organisations to Influence Post-war Sri Lanka," *KDU Library,* 2021.

[9] Seda Sevencan, "Sweden Takes Measures against PKK-Related Social Media Posts in Stockholm," *World Europe*, June 18, 2022, https://www.aa.com.tr/en/europe/sweden-takes-measures-against-pkk-related-social-media-posts-in-stockholm/2616664

the Taliban, have in the past claimed that social media is a tool used by the west to spread its culture and ideas throughout the world and that the west is spying on the population using the information gathered through the use of these platforms. But eventually, after realizing the usefulness of the online community, all of these organizations changed their stances.[10]

The fact can be demonstrated by numerous instances of terrorist groups appearing online, including the TTP Mohmand chapter on Facebook and Twitter, the Al Qassam Brigades, the Tamil tigers Twitter account, Jihad-o-Scope, the Al Qaeda Twitter account, the Khilafat Movement and the Mosul film by ISIS, the "Alemarah web" by the Taliban, and many more. There is no question that the public is greatly impacted by these terrorists' online messaging. These groups are not only limited to their websites. They also spread information in various ways. They have journalists who promote their ideology against opposition parties in an underhanded manner.

### 5.1. Data Buying

The data generated through techno-related products and applications are owned by different companies and are not the property of any specific department or country. This data can be sold to different companies or non-state actors for business or security purposes. There is room for terrorists to get that data from any specific company under any business name. There is no evidence that such an incident occurred up till now but there was accusation on the CEO of Facebook, Mark Zuckerberg[11] in 2018, for selling the individual information collected

[10] Deibert and Ronald J., "The road to digital unfreedom: Three painful truths about social media" *Journal of Democracy* 30, no. 1 (2019): 25-39.
[11] "Facebook's Data-Sharing Deals Exposed," *BBC News*, December 19, 2018.

from one of the leading online platforms (Facebook) for business purposes. He was afterwards called by the state authorities for a trial because this was thought to be an unethical act. The gathering of data and written texts pertaining to any delicate themes is also included in the purchasing of the data. The literature or translation services that are utilized in terrorism and extremist actions may be purchased through lawful means as well.

### 5.2. Online Radicalization

Radicalization is the process of gradually adopting extremism or other abnormal conduct in order to bring about a change in one's political, social, cultural, or religious position and to believe that war or other violent means are the only options. While same process occurring online is known as online radicalization.[12] Extremist ideology becomes a discourse as more individuals communicate online and gradually begin adhering to an extremist group's particular ideology as a result of the general public spending more time online. These radical organizations recruit people, especially teenagers, and build their virtual networks in this way. Traditional communication channels were difficult to access, but modern technology offers radicals more refined means of spreading their message. As a result, the proportion of people changing their minds is higher and happens more quickly in this situation. Religious scholar from the US, Yasir Qadhi argued that, "Radicalization takes place in media, not in mosques".[13]

https://www.bbc.com/news/technology-46618582

[12] Macdonald, Stuart, and Joe Whittaker, "Online radicalization: Contested terms and conceptual clarity," In *Online terrorist propaganda, recruitment, and radicalization*, pp. 33-45. CRC Press, 2019.

[13] Blaker and Lisa, "The Islamic State's use of online social media," *Military Cyber Affairs* 1, no. 1 (2016): 4.

### *5.2.1. Examples*

Zachary Adam Chesser who converted to Islam is one of the great examples of a suspect of online radicalization who later was also accused of aiding Al Shabab. He also promoted radical views through his online content.[14] Brevik a far-right extremist in Norway who plotted two severe attacks also wrote articles aiming to unify the far-right political groups.[15] Al-Qaeda, a leading terrorist organization also opted for this strategy and mainly targeted youth. It promoted their radical views through high-quality content and familiarized youth with their ideologies. Ayman Al-Zawahiri, the leader of Al Qaeda himself mentioned that "their half of the struggle to gain supporters is dependent on media".[16]

Al Shabab from different social media platforms, particularly on Twitter, radicalized a number of Somalis to adapt their views. Abu Mansoor Al-Amriki, Al-Shabab leader mainly worked on these online operations. Several HD videos were released. One of them was particularly significant since Al-Shabab pledged their assistance to Osama Bin Laden in the video, which served as an excellent case study of internet radicalization.[17] The substantial use of social media by ISIS to get more followers is also witnessed internationally. Quoting an example, a girl named Aqsa Mahmood who was labeled as a converted

[14] Michael W.S. Rayyan, "Defeating ISIS and Al-Qaeda on the Ideological Battlefield: The Case for the Corporation Against Ideological Violence," *U.S Naval War College Digital Commons*, 2018. https://digital-commons.usnwc.edu/ciwag-case-studies/16/

[15] Ibid.

[16] Ibid.

[17] Menkhaus and Ken, "Al-Shabaab and social media: A double-edged sword," *Brown J. World Aff.* 20 (2013): 309.

radical through Tumblr, left her home in the name of Jihad following the ISIS online radicalization programs.[18]

### *5.3. Publicizing Act of Terrorism*

Extremists pose a serious threat to national security by instilling fear, and this threat is now being spread via internet channels. Spreading panic or ascribing someone with the title of martyr or hero are two ways terrorists use to publicize their crimes. Terrorists use cyberspace in a variety of ways, but one of the biggest risks to public safety is the strategy of making crime visible. Social media is frequently used by armed non-state actors or extremist groups to demonstrate their extremism and the brutality with which they will go to achieve their objectives. The cases that were used in the pertinent aspect are as follows:

Al-Nusra Front leader, Abu Mohammad Al-Jolani in an interview mentioned how they were planning attacks against the west and was in contact with Al-Qaeda leader Zawahiri who told them, "Not to use Syria as a sanctuary".[19] Facebook Livestreaming by Brenton Tarrant perpetrator of the Christchurch Mosque shootings in New Zealand, is a crucial example of publicizing crime through the internet. London underground attack was proudly owned by Zawahiri, and Muhamad Siddique Khan was mentioned as a martyr of that suicide attack. A video was broadcast on the internet and later by Al Jazeera magazine. Another terrorist Shehzan Tanveer, a bomber from Al Qaeda

[18] Emn den Aakster, "ISIS, Radicalization and the Gendered Online Jihad," *E-International Relations*, May 22, 2020. https://www.e-ir.info/2020/05/22/isis-radicalization-and-the-gendered-online-jihad/

[19] "Syrian Nusra Front Announces Split from Al-Qaeda," *BBC News*, July 29, 2016, https://www.bbc.com/news/world-middle-east-36916606.

was also celebrated as a hero by the similar terror network.[20] Al Shabab also observed people sharing information about their assaults and promoting them as Mujahideen and heroes. This was initially observed during the Nairobi mall incident, when their tweet served as the official government source of information though they were not even aware of the attack prior to that tweet.[21] Al Qaeda owned two websites, alneda.com and drasat.com in the aftermath of the 9/11 attacks to publicize the attack and to answer various questions asked by Muslims around the globe.[22]

### *5.4. Terror Financing*

According to Fredric and Fernanda, 90% of terrorist organizations are not able to survive for more than a year without a proper financial system. A constant flow of money is required for a long-lasting continuance, and finance is not required only to buy weapons but also for the continuance if recruitment process and further maintenance. Extremists adopt both formal and non-formal methods, such as the Hawala systems, Zakat, Fitrana to international banking system, the Islamic banking system, and money laundering to raise funds for their organization.[23] According to Michael Freeman, there are four basic categories of sources for financing terrorism: popular endorsement, unlawful actions, illegal activity, and occasionally state-sponsored

[20] Victoria Fassrainer, "Tweeting Terror Live," *Military Review* (Mar-Apr 2020). https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MA-20/Fassrainer-Tweeting-Terror.pdf

[21] Ibid.

[22] Thomas and Timothy L., "Al Qaeda and the Internet: The Danger of Cyberplanning*" U.S Foreign Military Studies Office (ARMY) Fort Leavenworth Ks*, 2003. https://apps.dtic.mil/sti/citations/ADA485810

[23] Lemieux, Frédéric, and Fernanda Prates, "Entrepreneurial terrorism: financial strategies, business opportunities, and ethical issues," *Police Practice and Research* 12, no. 5 (2011): 368-382.

initiatives.[24] Nowadays, most of these activities—including the dissemination of financial information, requests for financial assistance on social media platforms, extortion, cryptocurrency, and charitable giving are carried out through cyberspace channels. Taliban were accused of using radio campaigns to gain funds for their financing in the name of donations. They also got international funds worth $200m through online transaction from countries specifically in private trusts located in the Persian Gulf. [25] The 9/11 attack by Al Qaeda cost approximately $500000 which was investigated to be transferred in three stages i.e., money transferring in accounts of hijackers, physical transfer, through debt or credit cards in international accounts.[26] Under the name of Zakat, Al Shabab used to get millions of dollars in their bank accounts. Online transactions are made and campaigns for this zakat are made through different social media platforms.[27]

### *5.5. Hacktivism or Cyber-attacks*

Radicals and non-state actors can use information technology effectively for terrorist aims. Therefore, on both traditional and non-traditional levels, hacking represents one of the major risks to society and the security sectors. Most of the time, hacking just needs technical know-how to pose a virtual threat and leaves no digital traces. The hijacking of computer-related systems, such as phones, social media

[24] Michael Freeman, "Financing terrorism: Case studies," *Routledge*, 2016.
[25] Gilles Dorronsoro, "The Taliban's Winning Strategy in Afghanistan" *Washington, Dc: Carnegie Endowment for International Peace*, 2009.
[26] John Rothe, Douglas Greenburg, and Serena Wille, "Tenth Public Hearing of the National Commission on Terrorist Attacks Upon the United States," *Tenth public hearing of the National Commission on Terrorist Attacks Upon the United States* § (2004), pp. 2-152.
[27] Harun Maruf, "In Somalia, Businesses Face 'Taxation' by Militants", *Voice of America* - English, December 3, 2018, https://www.voanews.com/africa/somalia-businesses-face-taxation-militants

accounts, sim cards, official websites, and enterprises, is referred to as hacking.[28] The perpetrators may be script kids, site defacers, pirates, or phone phreakers, and they may employ viruses, cookies, DoS attacks, bogus emails, and a variety of other techniques. Additionally, this harm to the computer network may help their cause, or they may alter the website using the names of officials. Following the current wave of attacks attributed to Anonymous, intelligence officials increasingly view hacktivism as a significant medium.

Electronic hands of ISIS, United Cyber Caliphate is notorious for hacking several French, Australian, and US military databases, and British and Swedish websites.[29] ISIL associated Junaid Hussain, a British hacker who belonged to the hacking group "Teamp0isoN"[30] is commonly assumed of targeting NATO websites, Twitter accounts of US central command, international business times, French websites, servers of the US Department of Defense and was sent to jail for hacking Tony Blair's official account.[31] Cyber-attack skills by Tamil tigers are also well known, as they hacked Sri Lankan satellites and official websites.[32] Hezbollah affiliated team Lebanese Cedar was involved in year long hacking which hacked 250 websites of telecom and ISPs aiming to get hands-on intelligence sensitive data.[33]

---

[28] Johan Sigholm, "Non-state actors in cyberspace operations," *Journal of Military Studies* 4, no. 1 (2013): 1-37.
[29] Christina Schori Liang, "Unveiling the" United Cyber Caliphate" and the Birth of the E-Terrorist." *Georgetown Journal of International Affairs*, Vol-18, No.3 2017: pp.11-20.
[30] Kovacs, E., "Site of NATO Croatia hacked and defaced by TeaMp0ison. Soft pedia," (2012).
[31] Nafees Hamid, "The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain" *CTC Sentinel* 11, no. 4 (2018): 30-37.
[32] Shyam Tekwani, "Working Paper" *London*, January, 2006: pp. 2-50.
[33] Becky Bracken, "Hezbollah-Linked Lebanese Cedar APT Infiltrates Hundreds of Servers," threatpost.com, February 1, 2021, https://threatpost.com/hezbollah-lebanese-cedar-apt-servers/163555/

### *5.6. Use of Cryptocurrency*

According to experts, after laws and organizations were established to avoid such features, financing for terrorism and radicalization through cyberspace from online, digital, or computational sources is now controlled in the majority of the world. Numerous terrorist and extremist actors had already preferred cryptocurrencies like Bitcoin for financing and facilitating their actions. Both in the Global North and in some regions of the Global South, the flow of several digitalized currencies is currently being watched. Numerous terrorist and extremist non-state groups have increased their reliance on cryptocurrency sources as a result of the prohibitions and stringent monitoring. The fact is that it is now possible to prevent transactions that finance terrorism through the internet and computational means.

Terrorist networks and radicalized non-state actors have already entered the bitcoin market to facilitate their general and digital organized crime operations. It was discovered that terrorist organizations had learned how to use and profit from cryptocurrencies. According to the book "Terrorist Use of Cryptocurrencies",[34] the dark net was employed multiple times to purchase weapons as well as to fund the agents of non-state actors who radicalized people. In places where they had maintained a low profile, the sleeper cells of organizations like the Islamic State of Iraq and the Levant (ISIL) can simply convert cryptocurrencies to fiat currencies. Already, terrorism networks had found cryptocurrency to be a lucrative source of funding for their operations. As per Nikita Malik, the cryptocurrency has the

[34] Cynthia Dion-Schwarz, David Manheim and Patrick B. Johnston, "Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats," *Rand Corporation*, 2019.

potential to bring the funding of terrorism and radicalism from the Hawala System towards such unmonitored digital currencies that can be used through the dark net as well. A number of Kurdish and Islamist groups had opted for the use of cryptocurrencies as an alternative to the Hawala System.[35]

### *5.7. Cyber-Propaganda*

Web forums are significant informational resources, and social media is the best channel for spreading any fake news. A vast amount of information is available on social media and other online platforms. Because there is no adequate procedure for verifying the news, media, or knowledge published on it, anyone may simply find any specific information and upload anything, whether it is fake or legitimate. Although propaganda is nothing new, it is currently relevant when it is disseminated online. Extremists make full use of this chance to spread ideas according to their own agendas, readily shaping or constructing the public discourse in the process. Following the availability of three crucial demands, namely the tools, the motivations, and the social networks to engage more people online, terrorists are able to successfully manipulate the public.

For this, long posts with statements and media (pictures or videos) to logically support them (which may be fake) are submitted, and every attempt is made to increase audience engagement. According to the article "Web 2.0",[36] several terrorist organizations still managed to upload a number of videos about attacks, hostage-taking, and other

[35] Nikita Malik, "Terror in the dark: how terrorists use encryption, the darknet, and cryptocurrencies," *The Henry Jackson Society* (2018).
[36] Fredrick Romanus Ishengoma, "Online Social Networks and Terrorism 2.0 in Developing Countries," *International Journal of Computer Science & Network Solutions* 1, no. 4 (2013): pp. 2-12.

forms of cyber terrorism despite YouTube's restrictive guidelines. By doing this, more people become involved, and radical ideals and animosity toward their rival political parties spread quickly and widely.

Breaking the barriers of literacy and geography, the expansion of sophisticated propaganda by Al Qaeda is one of very important examples. It has seen sharing audio, visual, or text messages, which makes it easy for the audience as it makes it understandable for all. Al Qaeda has often offered a job as "Cyber Mujahideen" or "Electronic Mujahideen". It has also added its propaganda in psychological warfare many times, sympathizers can easily get access to their recorded media i.e., CD, DVDs, photographs etc.[37] Local problems and content emphasizing Al Shabab's potential were delivered through radio Andalus and Khatib in Somalia.[38] Emerged in 2013, ISIL Cyber propaganda came up into the notice of the international community when it started uploading content aiming to be a part of cyberterrorism on anonymous websites open to all, like Sendvid.com, Dump.to, justpast.it. Several Pro-LTTE materials, fake information regarding Sri Lankan history and domestic issues were posted and shared, even though recommendations for amendments in Sri Lankan politics were also made, all from internet technology, and the most influential channel in this regard was the website named "Tamilcanadian.com".[39]

[37] Carol K. Winkler and Cori E. Dauber, "Visual Propaganda and Extremism in the Online Environment," *Carlisle, Pa: Strategic Studies Institute and U.S. Army War College Press*, 2014.
[38] Callie J. Burke, "The Culture of Terrorist Propaganda in Sub-Saharan Africa a Case Study on Al-Shabaab's Use of Communication Technologies in Somalia and Kenya," *Master of Arts in Law and Diplomacy Capstone Project*, 2018.
[39] Iromi Dharmawardhane, "Use of Ideology and Technology in Terrorist Warfare in the Sri Lankan Conflict," *Centre for Political Violence and Terrorism Research (ICPVTR)*, 2014.

### *5.8. Recruitment for terrorism*

Terrorists nowadays are aware of the innovative and sophisticated potential of online recruitment. For the purposes of their extreme and terrorist actions, they very carefully target individuals using identification expertise, and they then follow them through the final stages of rigorous indoctrination. A terrorist organization is more likely to target vulnerable people for recruitment. They simply sharpen their psychic intention and mold it for terrorist aggressive endeavors since it is simple for terrorists to manipulate them. That is the way the young adults volunteer for the blowing up of themselves or to be ready to pick up the AK-47 till their very last breath. Internet usage is an incubator for susceptible individuals that they are just one click away from the recruiting process in terrorist groups.[40] Terrorist groups need to broaden their support base by subtly and non-violently expressing their ideological ideas. Therefore, the best weapon for this is the internet, which enables indirect communication with the intended audience. They mostly target young people because they are active, more susceptible to manipulation, psychologically more open, and well-versed in technological resources. In the last decade, terrorists have increased their recruitment campaigns with the name "jihadi Cool"[41] in which they used pop culture, video games and comics portraying Islamic fundamentalism to attract and manipulate the young generation in a non-violent way.[42]

[40] Andrew Dornbierer, "How al-Qaeda recruits online" *The Diplomat*, September, 13 2011. https://thediplomat.com/2011/09/how-al-qaeda-recruits-online/
[41] Anne Speckhard, "Is internet recruitment enough to seduce a vulnerable individual into terrorism," *Homeland Security Today*. *U.S*, April 15, 2020.
[42] Ibid.

Terrorists always tried to identify like-minded, self-reinforcing individuals. They have so many platforms like Facebook, blogs, Vlogs, social media websites, and the dark web which have been used to identify notorious people toward extremism. When someone expresses an interest in seeing their extreme information, they begin to follow them and control their thoughts with additional fanatical material.[43] They have a discussion team that guides them with more fanatic material. For example, they pointed out many posts to the target person on another web or other social media platform. Tawheed.ws is the online library for extremist literature for the people they point out. An article has been written with the title "Why We Hate Them".[44] This article served as a means of explaining to them why the extremists target the Western states and why they must wage Jihad against Christians and Jews. They can cultivate like-minded, and self-reinforcing individuals through these websites and social media platforms.[45]

The extremist non-state actors have created Jihad inspiring video games which became very popular. The game's name was Night of Bush Capturing. In this game, players embarked on Jihad with a targeted aim to assassinate the former President of the US George W. Bush.[46] Terrorists have introduced a cartoon movie on an online platform entitled "Al-Qaeda in the Arabian Peninsula".[47] That movie

[43]Siqueira, Kevin, and Daniel Arce, "Terrorist training: Onsite or via the Internet?" *European Journal of Political Economy* 63 (2020): 101878.
[44] Martin Rudner, ""Electronic Jihad": The Internet as al-Qaeda's catalyst for global terror" *Violent Extremism Online, Routledge,* pp. 8-24. 2016.
[45] Ibid.
[46] Jenna Ann Altomonte, "Virtual Trauma and Simulation: Cybernetic Performance in Wafaa Bilal's A Night of Bush Capturing: The Virtual Jihadi" *Stories in Post-Human Cultures, Brill,* pp. 207-216, 2013.
[47]Alex P. Schmid, "Perspectives on Terrorism," *Terrorism Research Initiative*, 2014.

created a boost in the recruitment of radicalized individuals. That movie created a much more poisonous effect on children while the other TV Channels have started broadcasting it.[48] Most likely the cyber experts of Al-Qaeda and ISIL have used traditional propaganda through the internet and the use of traditional ways like sending religious messages, videos of terrorist operations, and speeches. The start of the videos contains very motivational speeches and at the end, they add hate comments on the Western media by calling them "Kafirs".[49]

### *5.9. Training for terrorism*

All of these electronic sources have improved the resources available to training facilities around the world. These online training facilities offer the finest options in terms of price and removing practical barriers. Such violent online video consumption seems to be a more recent ambition for people who want to carry out terrorist operations. The initiative of the online library to coach the newly joined sympathizers and extremists is made by Al Qaeda which teaches different terrorist activities like making of biological weapons, bomb-making, etc. via different sources like the magazine "Inspire".[50] There was the publishing of the 2011 summer issue of the Inspire magazine, by Al-Qaeda. The articles contain proper training of jihadists, the best AK-47 firing stances, and instructions on how to manufacture highly explosive material. Some articles contain "Destroying Buildings" and

[48] Ibid., 47:91.
[49] Garth Davies, et al., "Terrorist and extremist organizations' use of the Internet for recruitment" *Social networks, terrorism and counter-terrorism: Radical and connected, Routledge,* pp: 105-127, 2015.
[50] Mehmet Nesip Ogun, "Terrorist use of internet: possible suggestions to prevent the usage for terrorist purposes" *Journal of Applied Security Research* 7, no. 2 (2012): 203-217.

make the bomb in the mom's kitchen. The articles contain "What to expect in Jihad".[51]

### *5.10. Accumulating Information*

The internet was created to disseminate knowledge and serve as the primary source of information for the entire world, without any constraints, much as computational technologies were initially developed to erase physical barriers expressly for communication purposes. Without a question, the unpredictably successful emergence of the Internet has achieved its goal, yet this information source is not only accessible to the general public but also to extremists who are easily misled and mistreated by criminals, culprits, or extremists. These search engines offer essential resources for information gathering and are crucial in the development of the operations or attacks, as well as the inspirations, propaganda, expansion, funding, and recruiting of these extremists. Prior to the 1990s, this process was slower and made it more challenging for offenders to quickly put their motives into practice. However, the introduction of the internet brought with it a wealth of easily accessible intelligence tools and details about likely targets. Use of google earth by Al Qaeda in an attack that was planned for Yemen but failed due to some unknown reasons. Mumbai attacks in 2006 were also successful with the help of user navigation on google earth by terrorists.[52] Several reports highlight the surveys and evaluations made by google search engines, in which the term "How to make a bomb" was in the top 10 most searched keywords. Other than

[51] Ibid., 50:92.

[52] Reich, Pauline C., "Case Study: India-Terrorism and Terrorist Use of the Internet/Technology." In *Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization, IGI Global,* pp. 377-408, 2012.

this, Salafi publications and beheading videos also include in highly searched content.[53]

## 6. Conclusion

The digital signature that extremist organizations leave behind after an incident and in some cases even before their goals have been fully achieved is the fundamental cost that they encounter in the context of the use of digitalized and computational means. There is no question that computational methods were initially developed to eliminate physical barriers to communication, and the internet was created to disseminate knowledge and serve as the primary global source of information without boundaries. However, the reality is that, like other crimes involving hacking and cyber theft, cyberterrorism has emerged as a significant threat to national and individual security on a huge scale. In the same way, improved computational techniques used by intelligence officials can track any propaganda, cyberattacks, internet funding sources, and the way they recruit via technology. All of these social media can be tracked, and artificial intelligence can quickly determine the operator's precise location.

Terrorists are gaining a lot from the use of information technology, especially given the success rate of these computational tactics. The fact is that it is now possible to prevent transactions that finance terrorism through the internet and computational means. Another aspect is that cryptocurrencies operate using an unrestricted system. In order to facilitate the general and digital operations of organized crime, terrorist networks and radicalized non-state actors have already gotten involved in the cryptocurrency industry. It was

[53] Von Behr, Ines., "Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism." *RAND*, 2013.

discovered that terrorist organizations had learned how to use and profit from cryptocurrencies.