Social Media as a Tool for Cyber Terrorism (ISIS as a Case Study)

Sara Haiman Ali Briah

[1]Department of International relations and Diplomacy, political Sciences College, Salahaddin University
Erbil, Kurdistan Region - Iraq

Abstract:

The use of social media, particularly by terrorist organizations, has become one of the world's top concerns. Terrorists and terrorist organizations use social media and other online platforms to conduct operational communication, acquire intelligence, share technical information, recruit, and train new members.

ISIS is one of many terrorist organizations that have exploited social media to their advantage. Utilized a variety of social media channels, including Facebook, Twitter, Instagram, YouTube, and Viber. As a result, ISIS benefited greatly from using social media because it is a less expensive, more straightforward, quicker, and more effective means of communication. Additionally, via social media platforms, members of terrorist organizations are promoting their ideologies, propaganda, and activities throughout the world. The study's finding is that Islamic State would not have been able to grow so swiftly or assemble such a sizable force without its control over the internet.

This study aims to identify the threat of cyberterrorism in the twenty-first Century and investigate how social media may be contributing to the rise in terrorist attacks around the world, particularly among ISIS adherents.

***Keywords*— Social Media, cyber terrorism, ISIS, Communication networking, security.**

I. Research Aims and Questions:

This study examines the ways in which terrorist groups, particularly the terrorist organization ISIS, have used social media platforms for a number of reasons. The purpose of this study is to address following questions:

1. ISIS uses social media to spread its propaganda, but how does it achieve this?
2. What strategies does ISIS employ on social media to draw in new members?
3. Do terrorists use social media as a tool, as a go-to material and/or as a weapon?

II. Research Hypothesis:

With the rise in terrorist actions, social media has a big impact on the dissemination of terrorism. The terrorist organizations, especially ISIS, communicate with their supporters and donors through various social media platforms, recruit new members from around the world, and disseminate training materials because this is frequently the best, fastest, easiest, and most affordable form of communication given the state of technology.

III. Research Methodology:

As we describe cyberterrorism and the Islamic State of Iraq and Sham (ISIS) in this study, we will use a historical perspective. From there, we will do academic analyses to demonstrate how ISIS is related to social media. Since primary sources like newspaper articles, books, and websites tend to be the focus of primary sources, we will employ case studies in this research.

IV. Introduction

Today, the media serves as the principal arena for setting power since it has the broad reach necessary to influence public opinion. Communication networks are convenient means of power consolidation because they may be used to exert influence over people's ideas. Social media tools in particular, including Twitter, YouTube, Facebook, and many more, powerfully mediate this creation process and enable people to speak without relying on conventional organizational structures (Gökce and Şengönül, p 27, 2017). As a result, terrorists and terrorist organizations use social media and other online platforms in various ways,

including for operational communication, intelligence collection, technical information sharing, recruiting, and training.

To promote their ideologies worldwide, terrorist groups are constructing virtual battlefields within cyberspace instead of actual ones. The use of social media platforms by terrorist organizations has grown substantially, becoming one of the most crucial means of connecting, recruiting, and conducting business with the members and supporters of such terror organizations around the world. This has led to phobia organizations becoming more organized and violent, endangering the peace and security of the entire planet. A warning sign of the longer-term threats posed by terrorism may be the large number of terrorist occurrences in recent years. Many terrorist organizations, including ISIS, have benefited from social media. The most active political movement on social media is ISIS, which uses Facebook, Twitter, Instagram, YouTube, and Viber among other platforms. According to research by the Brooking Center for Middle East Policy, between September and December of 2014, between 46,000 and 70,000 Twitter accounts that supported IS were active, with a mean of 1,000 followers per account (Hossain, p.6, 2018). The purpose of this study is to identify the threat of cyberterrorism in the twenty-first Century and investigate the contribution of social media to the rising number of terrorist occurrences around the world, particularly among ISIS adherents. This study will also discuss the idea of cyberterrorism in the context of scholarly theories and legal regulations. In this study, the media methods of ISIS will be analyzed. The research's final step is to evaluate the media methods used by ISIS.

1-The Concept of Cyberterrorism:

The discussion over the new "information society" and the expanding Internet use in the first 1990s spurred various studies on the possible threats posed by the highly networked, high-tech-dependent population, which can be used to date the origins of cyberterrorism. The words "We are at risk, Increasingly, America depends on computers, Tomorrow's terrorist may be able to wreak more damage with a keyboard than with a bomb" were used by the National Academy of Sciences to start a study on computer security in 1990 (Janczewski and Andrew, p.xiii,2008). The United Kingdom's national security strategy cites cyber-attacks by terrorists as one of the four highest priority hazards, illustrating how vital cyberterrorism is for national security in all countries worldwide (Ibid). On the other hand, Chen and Macdonald (p.27, 2014) stated that although the term "cyberterrorism" was first used in the 1980s, it did not fully gain popularity until a decade later. It could also be attributed to two crucial dynamics at this specific time. The first, it should be noted, was the transition to a post-Cold War world in which notions and presumptions of security that had previously been relatively secure were being dramatically tested and rapidly, drastically altered. As a result, there was more room to consider cybersecurity risks like cyberterrorism, cyberespionage, cybercrime, and cyberwarfare. Second, and perhaps even more significantly, this era saw the growth of the internet and the consequent interconnection it enabled—nationally and internationally, publicly and privately. Elites in politics and security have developed new worries due to this rising interconnectedness.

As a result, there have been varying viewpoints on essential concepts related to cyberterrorism, including the meaning of the term itself. Additionally, various purposes could have significant practical implications. Dissident voices can be heard and a range of other crucial research questions can be opened up by deconstructing various understandings of cyberterrorism.

Even though the term "cyberterrorism" has many definitions, Dorothy Denning defined it as "illegal attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government its people in furtherance of political or social objectives." (Tehrani, p.38,2017). Additionally, for an attack to be cyberterrorism, it must result in violence against people or property, or at the very least, it must do enough damage to inspire fear. Explosions, airline disasters, water poisoning, and attacks that result in death or serious bodily harm are a few instances. Severe strikes against essential facilities qualify as cyberterrorism, considering their potential consequences.

But according to the US Department of State, cyberterrorism is defined as “The deliberate, politically motivated attack against information, computer systems, computer programs, and data that results in violence against non-combatants is known as cyberterrorism.” (Centre of Excellence Defence against Terrorism (CSIS), p.118, 2008). According to CSIS, cyberterrorism is using electronic network technologies to shut down crucial national infrastructures (such as transportation, energy, and government activities), coerce or frighten a government, or both (ibid, p.119). Although the emphasis is different, these definitions have a lot in common. The ability of the terrorist "to alter physically" something significant to the victims could likewise be used to quantify the effects of cyberterrorism. Assaults don't appear to be effective in the end. Still, the perpetrator may succeed in making many people afraid of attacks, which frequently has adverse economic effects on enterprises. Even while a "hybrid attack" is possibly the most plausible way to exploit the internet for what would undoubtedly be a terrorist crime (ibid).

Additionally, it's critical to distinguish between cyberterrorism and hacktivism, a term used by academics to describe the union of hacking with political action. Here, "hacking" refers to operations carried out

secretly and online that aim to find, manipulate, or otherwise take advantage of weaknesses in computer operating systems and other software. Therefore, hackers frequently lack political motivations (Matusitz, p.179, 2008).
Sirohi noted that cyberterrorism has significant psychological, political, and economic effects on society. The word "cyberterrorism" combines contemporary anxieties from a psychological standpoint, fear of unprovoked, violent victimization connects. An unknown threat is viewed as more dangerous than one that is identified. Although there is no immediate threat of violence involved with cyberterrorism, its psychological effects on fearful society could be just as potent as those of terrorist bombings. Furthermore, a lack of data or, even worse, an abundance of false information are the main destructive elements that prevent an understanding of the specific threat posed by cyberterrorism. (Sirohi, 2015)

Weimann (2004) thinks that there has been significant concern over the possible threat posed by cyberterrorism, as Sirohi (2015) previously highlighted. Numerous security professionals and politicians have raised awareness of the danger posed by cyberterrorists breaking into personal and government computer systems and causing havoc in the military, financial, and repair sectors of advanced countries. The media, the security community, and the information technology (IT) industry, have all focused on the threat posed by cyberterrorism. Journalists, politicians, and experts in various fields have widely publicized a scenario in which highly skilled cyberterrorists electronically broke into computers that control dams or traffic control systems. This scenario would cause havoc and put many lives and the nation's security at risk. Nevertheless, despite all the doomsday scenarios that have been predicted, there hasn't been a single case of actual cyberterrorism documented.

According to Fay (p. 96, 2016). a new type of vulnerability has also evolved due to our societies' growing reliance on IT, allowing terrorists to attack targets that would otherwise be impenetrable, such as traffic control and national defense systems. A region becomes more vulnerable to cyberattacks on its infrastructure the more technologically advanced it is. The potential threat posed by cyberterrorism should give rise to anxiety. That does not imply, however, that all of the worries raised in the media, during congressional debates, or in other public forums are legitimate and pertinent. Thoughts about certain things are simply unfounded, while others are excessively inflated. Additionally, the difference between the potential and subsequently the actual harm produced by cyber-terrorists has been far too frequently neglected, and the relatively benign activities of the majority of hackers are mistaken with the Spector of pure cyberterrorism.

Because most of the critical infrastructure in Western countries is networked by computers, the potential danger from cyberterrorism is undoubtedly quite worrisome. The Sum-Up is the most significant impacts of cyberterrorism on society. Despite not being driven by the same objectives as terrorists, hackers have shown that people can access sensitive information and the functioning of essential services. Thus, terrorists may theoretically follow hackers' lead and, after infiltrating government and personal computer systems, cripple or paralyze modern economies' defense, finance, and repair sectors. Our society's increasing reliance on IT has led to a new type of vulnerability, offering terrorists the chance to approach targets that will likely be all but impossible to attack, such as traffic control and national defense systems. The more technologically advanced a country is, its infrastructure is susceptible to cyberattacks.

Thus, there is a legitimate cause for concern over the threat that cyberterrorism may offer. That does not imply that all of the anxieties expressed in the press, Congress, or other public forums are valid and justified. Some worries are merely unfounded, while others are greatly exaggerated. The distinction between the potential and actual damage caused by cyberterrorists has also far too frequently been overlooked. As a result, the primarily benign activities of most hackers are mistaken for the threat of pure cyberterrorism.

In conclusion, cyberterrorism's appeal to terrorists for several reasons, modern terrorists often engage in cyberterrorism because it is firstly less expensive than conventional terrorist techniques, and a laptop and an internet connection can be all that the terrorist needs. Instead of purchasing weapons like guns and bombs, terrorists will construct and distribute computer viruses using a phone line, cable, or wireless link. Second, compared to more conventional terrorist tactics, cyberterrorism is more anonymous. Terrorists, like Internet users, frequently use "screen names" or visit websites as anonymous "guest users," making it difficult for security organizations and law enforcement to determine the terrorists' true identities.
Furthermore, there are no physical obstacles in online, such as checkpoints, borders, or customs officers that must be avoided. The third point is that there are a vast variety of targets. Governments, individuals, public utilities, and private planes are just a few marks that a cyberterrorist could choose. Terrorists will therefore be able to locate holes and openings to exploit due to the sheer volume and complexity of prospective targets. According to studies, critical infrastructures like electricity grids and emergency services are vulnerable to cyberterrorist attacks because of how sophisticated the infrastructures and the computer systems that run them are, making it practically hard to find and fix all flaws (Matusitz, p.197, 2008). Fourth, cyberterrorism is frequently carried out remotely, a trait that terrorists find very alluring. Compared to traditional forms of terrorism,

cyberterrorism needs less physical training, psychological commitment, risk of death, and travel, making it more straightforward for terrorist groups to enlist and keep supporters. Fifth, compared to traditional terrorist tactics, cyberterrorism can directly influence a higher number of people, resulting in more media coverage, which is ultimately what terrorists seek. (ibid). On the other hand, Bogdanoski and Petreski (2003) suggested that cyberattacks are growing more tempting since they require less manpower and resources to conduct, which is crucial given that terrorists have limited financial resources. Because they are far from the terrorist act's site, cyberattacks also give terrorists the chance to maintain their anonymity. Unlike traditional terrorists who establish their bases in countries with weak governments, cyber terrorists can store anywhere while maintaining anonymity. It is believed that combining cyberterrorism with physical terrorism is its most effective use.

Islamic State of Iraq and Sham (ISIS): Historical Background

The so-called an Islamic caliphate was founded by the Sunni jihadist organization known as the Islamic State of Iraq and al-Sham (ISIS), also known as the Islamic State of Iraq and Levant. (Johnston and Wallace, p.45, 2016). On July 1, 2014, a 20-minute audio file featuring the head of the Islamic State, Abu Bakr al-Baghdadi, was published on extremist websites and social media. He established a new caliphate and crowned himself its caliph (Atwan, p, 20,2015). Five months after the occupation of Iraq in 2003, all of the Islamist organizations—aside from Zarqawi's al-Tahwid wal Jihad—merged under a new name, Jaish Ansar al-Sunna (Army of the Followers of the Teachings - JAS). JAS shared Zarqawi's group's objectives, which were more in line with the philosophy and global outlook of al-Qa'ida. When the invaders were driven out of Iraq, one of these groups—from which ISIS would eventually emerge—expressed the desire to establish an Islamic state there. When Zarqawi formally joined forces with al-Qa'ida in December 2004, he launched a campaign with various goals, some of which still guide IS's tactics today. First of all, there has been a decade-long campaign of infiltration and attacks on recruitment centers for the military and police to prevent Iraqis from cooperating and to destabilize the national security forces. Iraq was therefore quickly becoming as the ideal Islamist training camp. The recruitment of foreign militants into the insurgency in Iraq grew, and a slow flow of them started to enter the nation, mainly across the Syrian border. Iraq was in some ways a better, more enticing environment for its members to traverse since it was Arab-speaking and culturally familiar; the Arab mujahideen had last gathered in substantial numbers in 1980s Afghanistan. The ruthless military strategy advocated by Zarqawi represents a turning point in the development of global jihad. The seeds of Islamic State were initially sown at this period, even though they failed to consolidate and thrive during Zarqawi's lifetime (ibid).

On the other hand, according to Chandra (2018), American forces entered Iraq in 2003 with the relatively straightforward mission of ridding the country of Saddam Hussein and the Baath Party and establishing a new democracy. While the United States did manage to arrest Saddam Hussein and remove his Baathist allies from the most crucial government positions, the new democracy established in Iraq turned out to be highly shaky. After American soldiers were wholly withdrawn from Iraq at the beginning of 2011, most of the country's leaders were expelled, leaving a power vacuum. The lack of effective leadership in Iraq provided ISIS, a youthful Islamist organization that broke away from al-Qaeda, with the ideal chance to pursue the establishment of their Caliphate. The main factor in the rise of ISIS was the unrest in Iraq. The Syrian war is the second, arguably most important, element that contributed to the recent rise of ISIS. The so-called "Arab Spring" movement increased activity across numerous countries in 2011 and was observed in many regions. The Arab Spring Movement opposed oppressive governments throughout the Arab world and assisted in overthrowing a dictatorship in Egypt. When the Arab Spring finally reached Syria, despot Bashar Al-Assad greeted it with a military force. Although Assad did not fire the initial shots, his actions plunged his nation into war. Then a group known as the Free Syrian Army (FSA) started using weapons to overthrow the Assad government. Another fantastic chance for ISIS emerged from the Syrian conflict. Even if ISIS may have found enough strength in the absence of genuine leadership in Syria, the conflict there provided them with another benefit (ibid).

The unsuccessful Islamic State of Iraq (ISI) was founded between 2006 and 2013, and both Western and local media referred to it as al-Qaeda in Iraq (Bunzel, p.15, 2015). Al Qaeda and Al Zarqawi's strategic goals were to undermine US soldiers, undermine the government's ability to form alliances, and stir sectarian strife between Sunnis and Shiites to put US security at danger. Osama Usama bin Laden and his successor Ayman al Zawahiri even chastised Zarqawi for his tactics, which led to the mass massacre of Shiites. Al Qaeda and al Zarqawi became rivals due to this philosophical and tactical divergence. He created Majlis Shura al Mujahideen, an umbrella grouping of six distinct organizations, without seeking permission from al Qaeda leadership. Al Zarqawi proceeded to assault Shiite strongholds and symbolic locations to strengthen his organization among Sunni tribes despite the ongoing hostilities. The regular army killed al Zarqawi in an offensive in 2006, and Abu Hamza al Muhajir, also known as Abu Ayyub al Masri, assumed control of AQI.

The second phase of ISIS was hinted to by the forced shift of leadership (Harvey and Pregent, p. 196, 2015).

The Alliance of the Scented Ones was subsequently formed by several different jihadi groups and Sunni tribal leaders, as stated by the Mujahidin Shura Council. Three days later it declared the creation of "the Islamic State of Iraq." "Baghdad, Anbar, Diyala, Kirkuk, Salah al-Din, Nineveh, and portions of Babil and Wasit" were included in the emirate's sphere of influence. An Iraqi named Muharib al-Juburi, the Islamic State's recently appointed communications spokesman, released the audio message introducing the organization. Abu 'Umar al-Baghdadi, also known as the "Commander of the Faithful," was named Juburi as the state's commander.

Baghdadi, a former police officer whose actual name was Hamid Dawud Khalil al-Zawi, rose to prominence as the head of the jihadi movement in Iraq and chose Abu Hamza to serve as his deputy and the Islamic State's minister of defense. Both routinely handled the world through the Islamic State's official Furqan Media Agency, yet neither would reveal their faces to the media (Bunzel, p. 19,2015). Mosul, the second-largest city in Iraq, was reportedly taken over by the Islamic State in about four hours in 2014. There was a flurry of activity and hand-wringing in the ranks of officials in many capitals and the media. No significant observer of the region, inside or outside government, had anticipated its ascent. U.S. officials, starting with the ident, had openly dissed ISIS while praising what they saw as their much more significant victory against al Qaeda. However, ISIS was doing something that al Qaeda had never even attempted to do during its existence: seizing territory from two governments that had previously held it via the use of force. ISIS declared the creation of its so-called caliphate overnight, removed the internationally recognized boundary between Iraq and Syria, and appointed an Iraqi as its *amir almuminin* (commander of the faithful). Abu Bakr al-Baghdadi (Al- Istrabadi and Ganguly, p. 5, 2018).

ISIS rapidly seized territory in Iraq and Syria between 2014 and 2016, establishing a *wilayat* (governorate) and enforcing regulations according to the organization's interpretation of Islam. The US formed a coalition against IS in September 2014. They launched airstrikes to stop its advance, assisting the Syrian Kurdish YPG force in driving the terrorists away from Kobani near the Turkish border. IS captures Ramadi in Iraq and Palmyra, a historic desert town, in Syria in May, but by the end of the year it is on the backfoot in both nations.

Iraq retakes Fallujah in June 2016, the main town that ISIS had taken during its early burst of success. Manbij in Syria is captured by the Kurdish YPG-led Syrian Democratic Forces (SDF) in August 2017 is a year of devastating losses for Islamic State. After months of conflict, it loses Mosul to Iraqi forces in June, and Baghdad proclaims the caliphate's end. In an effort to relieve Deir al-Zor and restore state control at the river, the Syrian army is moving east in September with the support of Russia and Iran. The SDF expels IS from Raqqa in October 2018 saw the recapture of IS strongholds by the Syrian government at Yarmouk, south of Damascus, and along the border with the Israeli-occupied territory. Iraqi soldiers gain control of the remainder of the border zone while the SDF moves further downstream on the Euphrates. US military withdrawal is promised. The SDF reports that in 2019, IS forces are routed at Baghouz, their final stronghold along the Euphrates. The SDF proclaims the "caliphate" to have fallen (Ingram and Winter, p.35, 2020)

The US declared the creation of a large international coalition to battle ISIS on September 10, 2014. Before the Iraqi military formally said the final liberation of all Iraqi areas from ISIS on December 9, 2017, the fight against ISIS in that country continued for over three years. The Kurdish combatants known as Peshmerga were instrumental in the war against ISIS. With the use of air power, Kurdish forces in Iraq were able to retake essential cities like Kirkuk26 and save many Yazidi refugees by giving them a safe passage to retreat via Syria to Kurdistan (MATAR, p.4, 2019)

2- Cyberterrorism and Social Media:

In the past, foreign terrorist organizations or their affiliates were in charge of plotting them, and recruiting and planning usually involved some direct, face-to-face contact with terrorist agents. Similar social networks, motivation, and inspiration may be found online today, all nicely wrapped with information on how to make bombs. Adherents can self-radicalize without having to interact directly with a political movement or cell that has existed for a while. It will also be more difficult for law enforcement to uncover schemes in their earliest phases due to the rise in online self-radicalization among individual extremists who have no direct physical contact with established terrorist organisations or cells (Chandra, p.12, 2018).

In addition, since swords and guns were the only decisive weapons in the past and were crucial in conflicts, the media (such as mobile phones, cameras, the internet, computers, and TV) emerged as the popular tools and a game-changer in warfare and the development of strategies. The media has a significant impact on the general public today, may disseminate messages and propaganda, and can install certain notions in its audience's brains. It comes as no surprise that terrorist networks are fully aware of the power and influence of media technology and use it to achieve their objectives as well as reach their intended audiences (Hossain, p.4,2018).

Consequently, as stated by Ozeren and Canbegi (2016), among many other media tools, online communication technologies and the public cyberspace are the primary agents of construction for people's, groups', movements', and institutions' meaning and identity. Social media sites like Twitter, YouTube, Facebook, and many more,

significantly mediate this creation process and allow people to talk without relying on conventional organizational structures. Online social networks now play a significant role in daily communication and have an impact on practically all facets of life. Online propaganda may be a popular tactic used by terrorist organizations like ISIS to entice and recruit recruits as terrorist organisations like ISIS are successful public agents in the cyberspace. It allows militants to take use of the convenience and convenience brought on by advancements in communication technologies, allowing them to connect with and inspire their supporters.

The efforts of terrorist organizations to exploit modern technologies to create more accessible and practical materials that justify and legitimize violence are growing as social media usage and Internet literacy become more and more widespread. They disseminate their messages through Facebook, Twitter, YouTube, and other cutting-edge channels (Chandra, p. 12, 2018).

Today, social media is essential to both the daily lives of individuals and the operation of governments. According to statistics, there will be 7.8 billion people on the planet as of February 2020, there seem to be only so many billions of internet users. The ease of social networking is such that it is expected that by 2021, there will be 3.02 billion monthly active social media users worldwide. It is easier to predict how the 21st Century will develop with considering social media. It isn't an exaggeration to say that social media is present in all aspects of life, including business, health care, politics, emergency management, the tourism industry, and education. The use of social media for sharing and entertaining media also doesn't need to be mentioned. However, social media does have a darker side to it, in addition to all the conveniences it offers. The flip side of the coin, social media misuse, must also be taken into consideration. On the one hand, this would seem to close the information gap and speed up the dissemination of news among people; on the other hand, many individuals are abusing it severely, abusing it to the point of genocide, murders, bombs, and conspiracies (Jain and Vaidya, p.11,2020).

Bogdanoski and Petreski (2013) suggested that terrorist organizations use the Internet and modern IT more frequently to carry out their plans to raise money, disseminate propaganda, and safeguard communications. Cyberspace is a tool that terrorists utilize to spread uncertainty. There are several different types of cyberattacks, one of which targets control systems and targets data. As the most prevalent type of Internet and computer attacks, data theft and destruction leads to in-service sabotage. The second attack will target control systems that are used to change or disable the physical infrastructure. For instance, they operate distant railways, water supplies, and electricity supply networks to create a wrong impression of more significant geographic areas. This can be done via hacking security systems or transferring data over the internet. On the other side, Medina (2014) shown that terrorists and terrorist organizations are interested in using social media platforms to communicate globally because it is quicker, less expensive, and more straightforward than traditional methods. In addition, the social media platforms make it easier for extremists and terrorists to share knowledge and other resources. They may offer counsel, training manuals, films, and operational security information even from foreign battle zones.

Then, the terrorist groups employed social media in a variety of ways, the first of which was for notoriety and propaganda. The media no longer needs to dilute and censor the messages of terrorists. This is typically accomplished by publishing a variety of articles along with image galleries. However, it is also possible to add audio and video recordings in which the terrorists defend their conduct. A gallery of alleged atrocities committed against innocent citizens in Iraq by foreign forces to win local and global sympathy for the terrorists illustrates this. Though it's uncommon, there are instances where terrorists like to disseminate material that shows their violent crimes or other related behaviours. Again, these can be through written accounts of the violence, but more frequently they are through films and images. Examples of this would include the pre-mission pictures of the Air Tiger squadron, which a few days prior had carried out its successful maiden raid against Sri Lankan government forces, published on the Liberation Tigers of Tamil Eelam website. One particularly extreme instance was the terrorist group ‘The National Movement for the Restoration of Pakistani Sovereignty's’ distribution of the journalist Daniel Pearl's beheading (Banyasz,p. 55, 2018).

The second is that for data mining, terrorists are aware that the internet is a tremendous information base that anyone can access. According to an al Qaeda training manual found in Afghanistan, which Secretary of Defense Donald Rumsfeld quoted on January 15, 2003, "Using public sources openly and without resorting to illegal means, it's possible to assemble a minimum of 80% of all information required about the enemy," access to highly detailed maps, schematics, and other sources of information online may make it possible for terrorists to gather information for planning purposes. More significantly, after this information has been produced, it is disseminated across terrorist organizations in volumes or "How to" manuals (ibid).

The third one is for raising money. Whether legally or illegally, terrorist organizations have made full advantage of the Internet's capacity to generate revenue. The most common ways that terrorists do this are: Selling goods: products with a direct connection to the terrorist group, like LTT-published CDs, DVDs, and books. Website- and email-based appeals: publishing messages on

newsgroups, forums, and their websites with information on how and where donations can be made. They are emailing sympathizers who expressed interest on a group's website. Terrorist organizations are funded through deception by exploiting what appear to be reputable charities or businesses. Criminal activity: Mastercard fraud, online trading, and gambling are just a few of the unethical methods that terrorist organizations are known to exploit to raise money (Bogdanoski and Petreski, p. 69,2013).

Another is for recruitment. This area has a solid connection to propaganda. Terrorist organizations are prepared to keep an eye on people who visit their websites, collect their information and profiles, and contact them if they seem to be potentially helpful to their cause. This grooming process begins as soon as the user starts consuming the propaganda on the website, such as the much mentioned "charismatic" method of delivery used by Osama terrorist in his video messages. Perhaps spurred on by this video, the user visits online chat rooms and discussion forums to look for answers. Skulking recruiters identify potential recruits who progressively encourage discussion of spiritual concerns while incorporating more political topics. As a result of this grooming, recruits are drawn farther and deeper into talks about terrorism and guided through a maze of private chat rooms until they are personally indoctrinated, which typically takes place through the use of the secure software such as Paltalk (ibid).

Finally, there will be a time for networking and communication. Terrorist organizations have recently moved from having a definite hierarchy within the organizations with designated leaders to having several, semi-independent cells with no apparent unique leader to allow them to remain covert. Web-based communication between cells makes it possible to exchange data and guides. The web also facilitates internal cell communication, particularly when discussing attack strategy. Conspirators frequently send messages using emails, which are commonly transmitted using open email services like Hotmail and Yahoo. They will even send emails from public libraries and internet cafes to avoid being discovered and targeted by security agents. You might also do this via chat rooms.

Moreover, websites' graphic files frequently contain information that is hidden using steganography. Graphic files can also be used to convey very subtle messages. For example, flipping a gun's position may signal that an idea is moving to the next step. Other ways to hide orders and messages include the use of coded language, as shown in Mohamed Atta's final email to the other terrorists responsible for the 9/11 attacks, which is said to have read: Three more weeks till the start of the semester. 19 confirmations have been received for the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering. The four targets—"architecture" being the World Trade Center, "arts" being the Pentagon, "law" being the Capitol, and "politics" being the White House—are thought to match the four categories mentioned. Using one-time anonymous public email accounts is a far safer alternative to traditional methods of communication. Two terrorists who want to communicate open 30 of these accounts, each with a username and password that is known to both parties. To put it another way, a terrorist creates an online email and keeps it as a draft online rather than sending it. Once logged in, the "receiver" reads and deletes the message. the next day, a brand-new account is used, exacerbating the user traceability issue (Banyasz, p. 70, 2018).
Stopped here

3- ISIS and Social Media: Interconnections

ISIS's intelligent and skilled media department adopts a well-thought-out strategy to focus on local and global audiences because media campaigns have long been a crucial component of the group's international propaganda efforts. The group has acquired the capacity to produce its periodicals, newspapers, booklets, and to extensively use the internet (particularly social networking websites) to spread its beliefs and objectives. As part of its skilful use of media, ISIS also threatens its opponents and effectively communicates with the general public while legitimizing its power inside the territories it controls. As a result, the media allows ISIS to terrify its adversaries and draw in supporters of its ideology worldwide.

ISIS used social media for several purposes, including to advertise its campaign of killing hostages and to maintain fear among their enemies and rivals. Second, to indoctrinate their ideals into young people's minds (especially those of Muslims), continue to find new militants, and expand their reach and influence. Thirdly, to promote the "benefits" of living in the Islamic State to legitimize their power inside the areas they have taken control over. Fourthly, to establish contacts with other militants, followers, or allies to persuade them to carry out ISIS-inspired actions abroad. ISIS used these platforms as a propaganda tool because they are open and public by nature, such as Twitter, Facebook, YouTube, and other related websites. ISIS members frequently utilize social networking sites to broadcast messages, photographs, and videos. At the same time, the warriors on the battlefield often stand next to dismembered victims to be seen by anybody watching the combat. ISIS's media wing makes good use of social media to advertise its gruesome killings campaign and intimidate its adversaries. It was also noted that the group's media wing actively promoted its cruelty in order to strengthen its military and demoralize its adversaries and their resistance. ISIS successfully used this tactic because many soldiers battling the organization fled the battlefield out of fear for their lives. Additionally, ISIS made requests on its Facebook and Twitter profiles to raise money online, enlist new fans, and collect donations. According to intelligence sources, ISIS also

got financial support online, which enabled the group to bolster its military capabilities and solidify its regional control (Hossain, 2018).

ISIS also have aggressively pursued numerous sophisticated internet recruiting and propaganda activities since 2014. In part, Twitter became ISIS's preferred platform because it can hide user identities more than other forums and social networking sites. The global and multilingual web presence of ISIS is available. The fear group publishes online periodicals in Arabic, English, Turkish, and French. It has also produced statements and films in Hebrew, Spanish, Russian, Kurdish, and German (ibid). Their recent success can be partially due to its global recruitment success. ISIS has developed for the 21st Century to ensure that it is not easily defeated, making it a distinct Islamist organization. They have various recruiting resources available, but they naturally favour the internet. Social media's advent has provided ISIS with a recruiting tool that other terrorist organizations haven't had. ISIS has an innovative, alarming way to recruit resolute potential new members thanks to social media. Through social media, ISIS may identify those susceptible to joining a revolutionary organisation. ISIS frequently targets people in danger emotionally or physically, and their social media profiles might draw attention to these problems for it to exploit. Members of ISIS have also had little trouble obtaining followers on social media. Many ISIS members may attempt to conceal their genuine motivations by appearing as religious mentors, providing people with a way of "family," or promoting ISIS territory as a fake utopia on social media. ISIS can broadcast propaganda on social media for free and easily, from military triumphs to beheadings of its adversaries. Much evidence shows how effectively ISIS recruits new members via social media sites like Facebook, Twitter, and YouTube. ISIS's use of social media is risky and gives the organization a unique chance to radicalize others. For ISIS recruitment to be successful, social media is essential (Chandra, p, 15, 2018).

Hossain (p.14, 2018) noted that as a result, social media platforms might quickly develop into vehicles for terrorist organizations to spread their ideology, foster a sense of belonging to the group, legitimate their actions through false information, and propagandize for recruitment. Unlike other traditional terrorist organizations, ISIS has a clear and highly professional communication strategy. It intentionally sows fear, just like other terrorist organizations do, but it does so in a more radicalized and strategic manner. Every element, especially in their video materials, is shown in full, strengthening the impression of horror that other terror organizations, in contrast, only allude to. ISIS utilizes the media to spread anxiety and dread. It does not simply seek to be a symbol of fear; instead, it also purports to offer "illusions of hope and justice" to anyone interested in joining their ranks.

ISIS uses a variety of media platforms to communicate with the public, from professionally produced journals and periodicals to media outlets airing Hollywood-style propaganda videos. Through these media platforms, ISIS functions as a propaganda machine online and promotes the idea that those under its rule uphold justice and harmony. The message, however, is at odds with the depressing facts of the areas where ISIS has taken over. ISIS use Twitter for a variety of functions, including communication. According to ISIS's 'Hijrah' magazine, necessary communication occurs via militants' Twitter accounts when transporting recruits.

Accordingly, as Atwan (p. 183, 2015) observed, ISIS members' or recruiters' social media posts have also been valuable for gaining insight into how ISIS uses social media. These posts are direct from the group and give us the most accurate representations of the propaganda and other messaging that ISIS disseminates worldwide. ISIS postings and pages will be accessible through an online archive tool, despite the fact that many social media platforms like Facebook and Twitter actively work to remove them.

Twitter has emerged as the most effective and valuable social media platform for ISIS. ISIS has a colossal online presence on Twitter. ISIS uses its official Twitter account to post any Caliphate-related official news. There are a lot of Twitter accounts with strong ISIS support, and the Cyber Caliphate is a well-known example. Black-hat ISIS hackers known as The Cyber Caliphate once had 110,000 Twitter followers. ISIS is now able to convey its message easily via a variety of channels thanks to Twitter. One way to promote ISIS propaganda on Twitter is by using well-known hashtags. In the Digital Caliphate, Atwan (p. 183, 2015) describes how this operates: Utilizing popular hashtags in one's tweet to link to Islamic State content housed on an unregulated, anonymous platform like Just Paste is one particularly efficient tactic used by activists.

ISIS is aware that by using Twitter, their propaganda will always be freely accessible to the general population. This propaganda is used to entice potential recruits and gives them a chance to persuade them to cooperate with ISIS fighters. A constant stream of battle reports and news about life in Islamic State is provided by thousands of Twitter accounts.

Large ISIS Twitter accounts are used often by regular ISIS members to maintain engagement with potential recruitment and sympathizers. Recruits can use Twitter to declare their decision to join the Islamic State, like American Douglas McArthur McCain did in 2014. His social media profiles stopped being active in 2013, they resumed activity in May 2014. McCain changed the subject of his tweets from basketball to jihad. Even though his anti-Islamic tweets have been removed for a

while, they can still be found on the web archive. As soon as McCain's Twitter account started to function once more, he wrote on May 14th, 2014, "Ya Allah when it's my time to travel have mercy on my soul have mercy on my bros." In August 2014, McCain lost his life while battling for ISIS in Syria. McCain is one illustration of the fact that any and every ISIS member is free to use Twitter to spread their radical ideology. ISIS's primary recruiting platform is Twitter (ibid).

Members know that those who could be recruited, mostly young Millennials, frequently use Twitter. Indeed, Twitter has taken on the role of the Islamic State's de facto spokesperson. ISIS engages in a virtual hashtag jihad geared primarily at these continually connected, tech-obsessed Millennials. There is no denying that Twitter can help ISIS recruit members. ISIS now has a chance that other Islamist organizations in the past have not had thanks to Twitter; they will simply erase the geographic barriers separating them from potential recruits all around the world. Anyone looking to move to Iraq or Syria can acquire advice on how to do so from someone who is already there from Dawla (short for Dawlatul Islamiyyah, the Islamic State), who is easily reachable via Twitter.

Another platform is Facebook. According to Stakelbeck (p. 114, 2015), while being the most popular social media site overall, Facebook has been less helpful to ISIS than Twitter. Despite this, ISIS still frequently uses Facebook as a medium for message dissemination. Like Twitter, Facebook has a sizable following for ISIS. ISIS recruiters have established a devoted following on Facebook and communicated with potential recruits through this platform. Anwar al-Awlaki, an American-Yemeni ISIS member who invented social media to find recruits, is one recruiter. His Facebook profile has thousands of likes. Al-Awlaki is not the only well-known ISIS member to garner a following on Facebook. Sheikh Ahmad Musa Jibril's usage of Facebook by ISIS is an intriguing example. Jabril, an imam from Michigan, makes encouraging remarks about ISIS and its activities rather than inciting murder. Jabril's Facebook profile has at least 245,000 likes by the end of 2015. Facebook has given ISIS members an easy way to find potential spouses or, for the feminine members of ISIS, to look for a husband. It also provides a platform for notable members of ISIS and its followers to gain a following. Potential jihadist couples may easily converse in front of the camera using Facebook's chat feature. Many women joining ISIS to wed jihadists are trying to flee something, such as overbearing parents or other planned marriages. The women already living in the Islamic State looking for a husband will become overly enthusiastic on Facebook. Some young jihadists have reprimanded their "sisters" for acting in a way that is haram since some ladies are so forthright in their overtures to potential Facebook friends. Even American women have looked for potential jihadist husbands on Facebook. A Colorado woman named Shannon Conley used Facebook to share her faith and locate a husband. Twitter and Facebook serve ISIS similarly, but each has its perks. Important ISIS supporters and members with Facebook accounts attract a sizable following, and those who have joined the Islamic State utilize it to find companions. Facebook may not allow ISIS' message to move as quickly as a tweet, but it is still crucial to the organization's overall social media presence. Stakelbeck (p. 116, 2015)

In addition to Facebook and Twitter, ISIS used many other social media platforms to recruit and disseminate propaganda. Instagram and YouTube were both crucial for spreading ISIS propaganda. Videos showing beheadings, military victories, and more recently, videos that resembled advertisements for the Islamic State, were routinely posted by ISIS accounts on both platforms. The production quality of ISIS's videos may have something to do with the group's effectiveness in exploiting online video to recruit. Its propaganda movies, which have high production elements that pay homage to a Hollywood action movie, are the jewels of its multimedia assault. ISIS was also not ashamed to post any videos of its successes right away on social media. Stickleback points out that ISIS frequently posts films and images of the carnage with excitement for their ardent fans to enjoy on platforms like YouTube, Facebook, Twitter, and Instagram. ISIS also used YouTube to highlight individuals who had joined the caliphate after emigrating from Western nations. Both social media sites enable ISIS to instantly disseminate propaganda and share it with recruits, from the organization's official YouTube accounts to the Instagram accounts of regular ISIS members. (Ibd, p117)

ISIS uses a variety of additional social media sites in addition to YouTube and Instagram. The Islamic State has all used Snapchat, Kik, and What's App. ISIS's ability to expand outside of Syria was made possible by the use of both Snapchat and WhatsApp, when the issue of banning some social media platforms was brought up in a House of Lords session in 2015. ISIS has benefited from Kik and WhatsApp as an anonymous recruiting tool. A recruiter will communicate with a potential new hire after making the first contact on Kik or WhatsApp. Even the most powerful figures inside ISIS are aware of the significance of social media for recruiting. YouTube, launched in 2005, provided the correct forum for these videos and for the recorded posthumous 'wills and testaments' of suicide bombers, which can be uploaded anonymously. This is discussed how ISIS' early leader Abu Musab al-Zarqawi used YouTube for his propaganda. ISIS leaders other than Zarqawi were aware of the value of social media. The current head of ISIS, Abu Bakr al-Baghdadi, started a campaign in 2014 to improve the group's online reputation by uploading pictures of its militants having fun in an effort to attract more ladies to the cause. ISIS has an advantage over the other Islamist group in recruitment and message dissemination thanks to their command of social media.

ISIS has extensively embraced social media, from the leadership to the inexpensive members (Atwan, p.34, 2015).

Internet subcultures give users the power to set agendas, control the flow of news, and spread misinformation while fostering a favourable atmosphere for media manipulation. The Islamic State's web approach was first designed to entice foreign soldiers to join IS assaults in Syria and Iraq. Additionally, it swiftly emerged as the most straightforward method for social media users to contribute to expanding IS-related content on websites like Twitter and YouTube. Online, right-wing extremist groups used a similar tactic. Ideologically-driven websites like Infowars and Roosh V's blog Return of Kings are significant online knowledge sources for the far-right due to their focus on far-right movements and men's rights activists. Online social communities of like-minded individuals who engage in and spread extremist messaging and material are facilitated by forums and message boards like 4chan and 8chan. As a result, far-right extremists use social media sites like Twitter, Facebook, and YouTube to disseminate radical messages to huge audiences. These sites also serve as major distribution hubs for memes and other visual forms of misinformation. As a result, there is a thriving online community where right-wing and terrorist organization like IS use small groups of social media users to smother potential recruits with attention and shift the conversation to safer online platforms. As a result, while recruitment may not end on Twitter, mounting evidence points to Twitter as the place where identifiable patterns of recruitment begin. While terrorism experts comparatively understudy the far-right movement's use of social media networks, Jihadist terrorist groups' use of social media as a platform for speaking and committing terrorism can be compared to identify patterns. Terrorist organizations have used social media's ability to permit a borderless flow of information as a tool to broadcast their messages around the globe, support online social communities, and sow discord and fear. Terrorists may quickly adapt to changes in how the world receives their communications. States and social media platforms must modify their counterterrorism tactics to meet these inescapable problems to keep up with the development of terrorist strategy (Jain and Vaidya, 2020).

Modern and intricate, IS's propaganda campaign makes considerable use of internet social networking and high-end video production and publications. A professionally produced video of American journalist James Foley's beheading in August 2014 received much attention. A gruesome image was posted on the front page of The Big Apple Post, and screenshots from the video quickly went viral on Twitter. Most media organizations and journalists rejected posting the horrific video or photographs, but IS knew that social media was an easy way to get over the controls put in place by media organizations to stop the dissemination of propaganda.

ISIS releases yearly progress reports that include high-quality infographics and drawings. Attack metrics are jammed into accounts, mimicking today's metrics-driven businesses. According to a paper by the Institute for the Study of War (2017), the result is to demonstrate organizational effectiveness to outside parties like sponsors, al Qaeda groups, and competitors.

The sophisticated propaganda effort of ISIS heavily relies on social media. A specially created app called Dawn of Glad Tidings was installed by thousands of IS's Twitter users, allowing IS to send centrally produced tweets through their accounts. Released simultaneously, the messages flood social media and significantly increase IS's online visibility. province Twitter accounts publish live information concerning regional IS operations in addition to centralized accounts. Thousands of IS sympathizers who support the group online also retweet its hashtags and translate its statements from Arabic to Western languages.

The entirety of IS's worn-out propaganda approach has a synergistic impact to build the brand. In addition to having more resources, weapons, and combat experience than al-Qaeda, IS also benefits from the assistance of an increasing number of Western recruits who bring English and technology expertise. Additionally, it utilizes English on purpose in several posts and films, such as James Foley's execution in the video mentioned above.
While the fourth estate frequently criticizes IS's barbarism, its propaganda strategy has been described as the broadest, encompassing five other narratives:

- Mercy as opposition brutality.
- Victimhood, where a casualty is blamed on the enemy.
- War or military gains.
- Belonging (which especially appeals to foreign recruits with friendship, security, and a sense of belonging).
- Utopianism, where the caliphate is not just discussed but also implemented.

In other words, IS propaganda aims to appeal to a wide range of people rather than only ruthless combatants, which helps to explain its recruitment success.

One of the most advanced social media efforts was allegedly run by IS. It is heavily funded and widely known. It is reportedly another beneficiary of its tremendous wealth, raking in £3 million every day through theft, extortion, and people trafficking. In terms of content and intended audience, it is purposefully biased in favour of foreigners. For instance, near the end of Ramadan in August 2014, IS released a 20-minute film that featured footage of the Mujahideen reciting the

same message in British, Finnish, Indonesian, Moroccan, Belgian, American, and South African accents. Important IS communications are frequently released in English, French, and German simultaneously, followed by translations into additional languages including Russian, Indonesian and Urdu. IS appears to have learned from previous ruthless terrorist organizations that lost their backing. IS has created a distinctive media strategy that blends a story of heinous murder with romantic ideals. The recruitment method of IS has also been different from that of al-Qaeda, which attracted fighters initially before radicalizing them. ISIS is looking for new members who are further along the path of intellectual radicalization or have a stronger inclination toward violence. These pre-radicalized fighters and their families are thrust into a violent and deadly environment when they arrive in Iraq and Syria (Macdonald and Jarvis, 2016)

Conclusion:

With the rise in terrorist actions, social media has a big impact on the dissemination of terrorism. The terrorist organizations, especially ISIS, communicate with their supporters and donors through various social media platforms, recruit new members from around the world, and disseminate training materials because this is frequently the best, fastest, easiest, and most affordable form of communication given the state of technology.

There are many opportunities for cyberterrorism to be carried out online using cutting-edge technology. Government computer networks, financial networks, and power plants are frequently thought of as potential targets of cyber terrorism. This is because terrorists often choose all of those mentioned above as the best targets to harm or take out of service to create havoc. Terrorists can penetrate a secured system by manipulating it using hidden entrance software, stealing sensitive data, erasing data, damaging websites, and injecting viruses, to name a few examples. The technology-enabled terrorist attacks will also be carried out through the traffic system or remotely damaging the facility supply networks.

Social media and ISIS have a lot in common. Despite being relatively young, both have significantly impacted the 21st Century. The relatively young ISIS militants have grown up utilizing social media widely. But once they became jihadists, they benefited the caliphate by using their familiarity with social media. Even the leaders of ISIS know how to utilize social media to propagate misinformation and garner support across the globe. Facebook and Twitter have proven to be quite helpful for ISIS. They have helped the Islamic State recruit new members, propagate its message, and serve as many young jihadists' online diaries. Even if the significance of Twitter and Facebook cannot be disputed, ISIS has used numerous other social media sites, including YouTube, Instagram, and Snapchat, as recruitment tools. Social media is the ideal weapon for ISIS to efficiently recruit new members worldwide because of the combination of instant connection and members' computer expertise. Even though ISIS uses social media to disseminate horrific depictions of war and violence, they have also tried to portray the Islamic State as a lovely haven from the challenges of both Western and local life. ISIS's use of social media is frequently used to explain some aspect of the phenomena and how it became so widespread. Without social media, it's unlikely that the group's message would spread as quickly or that recruiters could build the kind of close bonds with new members essential to their radicalization. The Islamic State has found that social media is a valuable tool.

ISIS is particularly active in several sectors, including the cybersphere. A highly effective media communication strategy aims to create belongingness to the group and fortify ties among its sympathizers—particularly in Western nations—in addition to spreading propaganda and enlisting new members. Its social media infrastructure fosters unity and a sense of belonging among its members while providing ways for ISIS supporters to stay in touch regardless of location. ISIS therefore places a high priority on propaganda efforts and manages its social media with impressive expertise.

The comprehension of the ISIS media strategy may continue after this study but may serve as a starting point. The evidence presented above contributes to the conclusion that ISIS is defined by its extensive use of highly dynamic social media platforms, global audience targeting, online supporter mobilization, and reliance on a non-secular narrative for legitimacy. ISIS and other Islamic extremist organizations will probably use these. Without its command of the internet, Islamic State could never have realized its geographical goals or amassed a sizable army in such a short period.

It is exceedingly doubtful that Islamic State would have existed in the first place, let alone been prepared to endure and grow, without digital technology. IS has effectively fended off challenges from military adversaries and foreign intelligence agencies by using the online communications for everything from recruitment and propaganda to coordinating simultaneous military operations across enormous distances.

References:

Books:

Atwan, a. b. (2015). *Islamic State: The Digital Caliphate.* londan : saqi books .

fay, j. j. (2016). *Cyberterrorism: Key Terms and Concepts for Investigation: A Reference for Criminal, Private ...* new yourk: routledge.

feisal al-istrababi, sumit ganguly. (2018). *The Future of ISIS: Regional and International Implications.*washington: broolongs institution press.

haroro j. ingram, craig whiteside, charlie winter. (2020). *The ISIS Reader: Milestone Texts of the Islamic State Movement.* oxford: oxford university press.

janczewski, lech, colarik, andrew. (n.d.). *Cyber Warfare and Cyber Terrorism.* new yourk: information seience refrence.

patrick b. johnston, jacob n. shapiro, howard j. shatz, benjamin bahney, danielle f. jung, patrik k. rayan, jonathan wallace. (2016). *Foundations of the Islamic State: Management, Money, and Terror in Iraq, 2005-2010.* santa monica: rand corporation.

sirohi, m. n. (2015). *Cyber Terrorism and Information Warfare.* delhi: vij books india pvt ltd .

tehrani, p. M. (2017). *Cyberterrorism: The Legal And Enforcement Issues.* singapore: world scientific.

terrorism, c. o. (2008). *(terrorism, 2008)Responses to Cyber Terrorism.* amsterdam: IOS Press.

terrorism, c. o. (2008). *Responses to Cyber Terrorism.* Amsterdam: IOS Press.

thomas m.chen, lee jarivs, stuart macdonald. (2014). *Cyberterrorism: Understanding, Assessment, and Response.* new yourk, 1, 2, 3: springer.

Bunzel, C. (2015) From Paper State to Caliphate: The Ideology of the Islamic State. The Brookings

Harvey, D. ,Pregent, M. (2014). The Lesson of the Surge: Defeating ISIS Requires a New Sunni Awak-ening. New America Foundation. P. 196.

Erick Stakelbeck, ISIS Exposed : Beheadings, Slavery, and the Hellish Reality of Radical Islam (Washington, DC: Regnery Publishing, 2015) 114.

Articles:

Matusitz, J. (2008). Cyberterrorism: Postmodern State of Chaos. Information Security Journal: A Global Perspective, 17(4), 179-187.

banysz, p. (2018). social media and terrorism. AARMS – Academic and Applied Research in Military and Public Management Science, 17(3), 47-62.

chandra, r. (2018). CYBER TERRORISM/HATE SPEECH ON SOCIAL MEDIA: A REVIEW OF INDIAN LEGAL FRAMEWORK. commonwealth law review journal, 4, 1-23.

hossain, s. (2018). Social Media and Terrorism: Threats and Challenges to the Modern Era. south asian survey, 2(22), 1-20.

Aly, A., Macdonald, S., Jarvis, L. & Chen, T. (2016). Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization. Studies in Conflict & Terrorism, 40(1), 1-9. Cronfa - Swansea University

medina, r. m. (2014). Social Network Analysis: A case study of the Islamist terrorist network. security journal, 27(1), 97-121.

mitko bogdanoski, drage petreski. (2013). cyber terrorism global security threat. TERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL, 13(24), 59-73.

orhan gokce, gulise gokce, abdullah sengonul. (2017, october). Media and Terrorism: Is Media the Tool for Terrorism?*. internatuion journal of advance research in computer science and management studies, 5(10), 1-29.

pooja n jain, archana s vaidya. (2020). Analysis of Social Media Based on Terrorism | A Review. vietnam journal of comuter science, 8(1), 1-11.

Electronic sources:

matar, j. (2019). IRAQ: ANY HOPE FOR CHANGE? [online] available from https://www.geneva-academy.ch/joomlatools-files/docman-files/Iraq%20Any%20Hope%20for%20Change.pdf

Suleyman Ozeren, Ph.D. Hakan Hekim, Ph.D. M. Salih Elmas, Ph.D. Halil Ibrahim Canbegi. (2016). isis in cyberspace: findings from social media research. [online] available fromhttps://www.academia.edu/24311407/ISIS_in_Cyberspace_Findings_From_Social_Media_Research

weiman, c. (2004). Cyberterrorism How Real Is the Threat? [online] available from

https://www.usip.org/sites/default/files/sr119.pdf

الخلاصة:

أصبح استخدام وسائل التواصل الاجتماعي، وخاصة من قبل المنظمات الإرهابية، أحد أهم اهتمامات العالم في الوقت الحاضر. يستخدم الإرهابيون والمنظمات الإرهابية وسائل التواصل الاجتماعي وغيرها من المنصات عبر الإنترنت لإجراء الاتصالات والحصول على معلومات استخباراتية وتبادل المعلومات التقنية وتجنيد وتدريب أعضاء جدد.

تعتبرالدولة الاسلامية من المنظمات الإرهابية التي استغلت وسائل التواصل الاجتماعي لصالحها. حيث استخدمت مجموعة متنوعة من قنوات التواصل الاجتماعي ، بما في ذلك Facebook و Twitter و Instagram و YouTube و Viber. ونتيجة لذلك، استفاد تنظيم «الدولة الإسلامية» بشكل كبير من استخدام وسائل التواصل الاجتماعي لأنها وسيلة اتصال أقل تكلفة وأكثر وضوحا وأسرع وأكثر فعالية. بالإضافة إلى ذلك و عبر استخدام منصات التواصل الاجتماعي ، يروج أعضاء هذه المنظمات لأيديولوجياتهم ودعايتهم وأنشطتهم في جميع أنحاء العالم. وتوصلت هذه الدراسة إلى أن تنظيم الدولة الإسلامية لم يكن ليتمكن من النمو بهذه السرعة أو تجميع مثل هذه القوة الكبيرة دون سيطرته على الإنترنت.

تهدف هذه الدراسة إلى تحديد تهديد الإرهاب السيبراني في القرن الحادي والعشرين والتحقيق في كيفية مساهمة وسائل التواصل الاجتماعي في زيادة الهجمات الإرهابية في جميع أنحاء العالم، وخاصة بين أتباع الدولة الاسلامية.