

## Cyberterrorism: Incubator for Ideological Dissemination and Recruitment of Terrorist Networks

Sapto Priyanto<sup>1\*</sup>, Syafira Tasya Azzahra<sup>2</sup>

<sup>1</sup>Universitas Indonesia

<sup>2</sup>Sekolah Kajian Strategik dan Global Universitas Indonesia

**Corresponding Author:** Sapto Priyanto [sapto.priyanto09@ui.ac.id](mailto:sapto.priyanto09@ui.ac.id)

---

### ARTICLE INFO

Keywords: Cyberterrorism, Social Media, Spread of Ideology, Recruitment

*Received : 16, January*

*Revised : 30, January*

*Accepted: 25, February*

©2025 Priyanto, Azzahra: This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



### ABSTRACT

The rapid development of information technology has significantly influenced various aspects of human life, including communication and information dissemination. However, these advancements have also been exploited by terrorist groups to spread radical ideologies and recruit new members through digital platforms, particularly social media. This study examines the use of social media as an effective tool for terrorist organizations, with a specific focus on the recruitment and propaganda strategies of ISIS. Utilizing various online platforms such as websites, Facebook, Twitter, and Telegram, ISIS has successfully expanded its influence globally. According to internal data from BNPT, nearly 50% of ISIS's budget is allocated to media-related activities, highlighting the crucial role of cyberspace in their operations. This research aims to analyze the patterns of radical content dissemination, the effectiveness of social media in recruitment, and the countermeasures that can be implemented to mitigate the threat of online radicalization. The findings of this study are expected to contribute to the development of strategic policies to combat terrorism in the digital era.

---

## INTRODUCTION

To understand the phenomenon of cyber terrorism, it is first important to understand the relationship between cybercrime and terrorism in general. There are various definitions and substantive debates regarding the nature of cybercrime and terrorism, making it difficult to immediately distinguish between these acts. Terrorism continues to evolve, and one example of its development is the emergence of Cyber Terrorism. Cyber terrorism is a sophisticated form of traditional terrorism in which terrorists use information, networks, and computer technology (the Internet) to carry out their actions. Cyber terrorism can include hacking, the distribution of software or malware, threats to computer systems, and chain attacks (Mahardhika et al., 2023). Experts initially debated whether cybercrime should be understood as a traditional offense enabled by new tools and devices or as a completely new form of offense that had never been compared before (Holt, 2012).

In modern terrorism, almost all terrorist organizations utilize the Internet to carry out their activities such as delivering messages/information to the masses for propaganda purposes, facilitating communication, raising funds, recruiting new members into their organization or to train newly recruited members. Concerns due to Internet exploitation have spread not only in the domestic sphere, but also in the transnational and international spheres (Ogun, 2012). With the development of globalization that brings innovations such as technological advances, easier cross-border connectivity, and increasingly complex networks in various regions, terrorism has undergone a transformation from merely a national level threat to a threat that reaches a regional and even global scale (Alexander, 2008; Suhito, 2017).

The era of social media began almost three decades ago, when Bruce and Susan Abelson created a social networking site called Open Diary with the intention of connecting online diary writers in one community. Along with the increase in high-speed Internet access, this concept became more popular, which then led to the emergence of social networking sites such as My Space (in 2003) and Facebook (in 2004). With this development, the term social media or social media emerged. One of the early forms of social media is Blog (Kaplan & Haenlein, 2010), which is a website with a personal page and has a variety of variations (Shodiq, 2021).

Cyber terrorism incidents where a terrorist organization uses social media as a means to spread radicalism and extremism are not something new in the 21st century. Terrorist organizations have used or utilized the internet before the terrorist attacks that occurred in the United States on September 11, 2001 or also known as the 9/11 incident. Before 1999, almost 30 terrorist groups were found on the Internet by the United States Government Department. At that time, terrorist organizations considered the internet media as a very powerful communication tool to be used in spreading propaganda (Banez, 2010; Sarinastiti & Vardhani, 2018). However, the role of the Internet became more significant for them after 9/11. Al-Qaeda leader Osama Bin Laden tried to disseminate videos from their hideout in Pakistan through the Al-Jazeera television channel, but they were frustrated because their segments or duration were very limited, which

might cause their message to be misconstrued. Therefore, they turned to the Internet to upload the videos in clearer and more detailed form without any editing (Gardner, 2013; Sarinastiti & Vardhani, 2018)

Al-Qaeda decided to utilize the Internet because they felt that conventional media such as television and magazines had become a threat to the security of the organization and its members. They saw television as a limited means of conveying a deep message in accordance with their ideology because it was limited by broadcast time. In addition, mass media was considered unsafe by them, because it could potentially allow parties with other interests to take their messages and manipulate facts that could influence the public's view of their actions (Soriano, 2008). For Al-Qaeda, the Internet is not only a method to achieve faster and safer media, but also a turning point in the rise of a more effective communication strategy compared to conventional media. For the first time, cyberspace is able to allow direct communication between terrorists and their public. The Internet not only fills the limitations of mass media, but the Internet also allows them to avoid a number of moral rules contained in mass media and limit their actions, and this is beneficial for their terrorist action strategy. As a group of jihadists did along with the invasion of Iraq in 2003, the Internet not only allows them to avoid operational risks, but allows them to gain access by infiltrating traditional media systems such as Al-Jazeera (Soriano, 2008).

The expansion of online social networks by the terrorist organization Islamic State of Iraq and Syria or known as ISIS began around 2015, when their sympathizers began using social media, such as Facebook, Twitter, Telegram, and several other social media to spread their propaganda, online and independently from the social media accounts of each terrorist (Susanti et al., 2023). In addition, ISIS also changed mobility patterns by utilizing technological advances in the recruitment process for network members. Various videos showing acts of violence carried out by ISIS against its enemies were posted on social media, one example of which is in YouTube and Twitter has proven to be an effective propaganda in attracting new followers from all over the world (Sukoco et al., 2021; Putri, 2019).



Source: (*jambi.tribunnews.com*, 2020)

Figure 1 One Example of a Video Clip of an Execution (Beheading) carried out by ISIS Militants against their Enemies/Opponents

The cases above show that the Internet has opened up quite large opportunities and chances for terrorist groups to carry out their actions. These opportunities are in the form of (Behr et al., 2013; Sari, 2017) The internet creates opportunities for individuals to be exposed to radical ideologies. In this case, the internet indirectly facilitates the process of radicalization through the emergence of radical sites. As a result, with its wide reach, the internet opens the door for terrorist groups to introduce and inspire their ideologies to internet users. In addition, the internet increases the probability of self-radicalization or self-radicalization to someone. An internet user no longer needs to interact directly with other terrorist members to understand deeper patterns of terrorist activity. This is due to the availability of abundant information on the internet that allows users to gain an understanding and learn patterns of terrorist activity.

The purpose of this paper is to identify the extent to which terrorist organizations exploit the internet in their activities. In addition, this paper aims to provide a theoretical framework on the use of social media by terrorists as an efficient tool or container in terrorist activities.

## LITERATURE REVIEW

### *Cyber Terrorism*

*Cyber Terrorism* or cyber terrorism, in its general concept, can be interpreted as a form of terrorism that attempts to attack and damage computers, along with the networks and information stored in them (Blane, 2003; Breen, 2008; Matusitz, 2005). Cyber terrorism was created and made an official reference in the 1980s (Alexander & Swetnam, 2001; Colarik, 2006). Cyber terrorism acts share significant similarities with conventional terrorism in many aspects. For example, cyber terror attacks tend to be planned, influenced by political issues, carried out by a small group of individuals (rather than by a government entity), and aimed at drawing attention (Matusitz, 2005; Radin, 2002). In addition, by analyzing the possibility of the emergence of cyber terrorism, Denning (2001) argues that in order for terrorists to view an attack on a computer network as a sufficient weapon, the attack must be sufficiently destructive or chaotic to produce public fear equivalent to a physical attack. terrorism that causes injury. Denning (2001) further stated that cyber terrorist attacks that cause many casualties or physical injuries may become the main aspiration of cyber terrorists in the future (Holbrook, 2015).

Terrorists have strengthened their networks with the increasing use of the Internet. Although many of their members have been captured or killed, their propaganda continues to be disseminated and spread widely through the Internet, even without leaving a trace. For example, after the US Air Force airstrike in Damadola, Pakistan, Al-Qaeda members in Pakistan attempted to infiltrate their propaganda messages into US websites as a warning that they would continue to carry out terrorist acts (Soriano, 2008). The Internet provides message boards and chat rooms for terrorists to recruit, buy bombs, purchase plane tickets, coordinate attacks and gather in one place without being physically present (Lumbaka & Gray, 2011; Sarinastiti & Vardhani, 2018). The existence of the internet they tried to hack several sites owned by the United States government and several Western countries allies. Therefore, they tried to

eliminate their weaknesses by placing the organization on the use of new technology. Osama Bin Laden's organization in this way chose to spread their news developments mostly on the internet.

The emergence of the term cyberterrorism is relevant, where terrorist groups utilize cyberspace (various internet applications) to launch their terrorist actions. The internet can facilitate the rapid dissemination of information, with relatively low risk and affordable costs to various groups, including in terms of recruiting potential members and seeking potential partners for their organizations (Seib & Janbek, 2011). Many of them use cyberspace, for example the group found by Abu Musab Al-Zarqawi from the Al-Qaeda faction in Saudi almost never had direct contact with the mass media, they focused their communication activities in cyberspace. This method prevented them from receiving widespread media attention.

Paradoxically, the mass media itself uses the web to search for traces and messages about the latest terrorism they are carrying out which will encourage the emergence of public opinion internationally (Soriano, 2008). The same applies to security issues that have undergone developments with the addition of meanings that are not only limited to military or physical aspects alone, but the concept of security has developed to include various aspects that are non-military or known as non-traditional security. Non-traditional security issues cover a variety of different but often interrelated and sometimes overlapping fields, such as threats to the environment, food security, economic security, energy security, human security, maritime security, and so on. All of these aspects are believed to have serious impacts at various levels, including human security, national security, regional security, and international security (Sagena, 2019).

### ***Terrorism Propaganda***

According to the 1997 Encyclopedia Britanica and The Oxford Companion to the English Language by Tom McArthur (1992: 333-334) explains that the term propaganda comes from the Neo Latin "propagandus" or "propagare," which means to spread. This term was first used by Pope Gregory XV in Italy in 1622 to refer to the institution responsible for the missionary activities of the Roman Catholic Church, known as the Congregatio de Propaganda Fide, which was a standing committee of cardinals. Since then, the term "propaganda" has been widely used to refer to systematic efforts and organized movements to spread certain beliefs, doctrines, dogmas, or systems of principles.

According to Thackrah (2004) in his journal (Bambang & Fitriana, 2017):

".. Propaganda can be defined as any information, ideas doctrines or special appeals disseminated to influence the opinions, emotions, attitudes or behavior of any specified group in order to benefit the sponsor either directly or indirectly..".

So, it can be interpreted that propaganda is a concept or idea of information intended to influence the views, actions, or behavior of individuals or certain groups of people. The delivery of propaganda can be direct or indirect. Terrorists use propaganda with the intent and purpose of communicating messages to

seduce, persuade or instill fear. The targets of this message can be other terrorist members, potential recruits or members, and supporters.

Terrorist propaganda is widespread in various media, including the internet which is a platform. Giving individuals or terrorist groups the opportunity to spread messages or information to them. The internet opens up various opportunities, one of which is allowing audiences or internet users to accept radical ideologies. The great advantage provided by the internet is its broad reach, which is beneficial for perpetrators or terrorist organizations. Terrorist propaganda often uses various techniques, including propaganda by deed or which is interpreted as propaganda carried out through acts of violence, dehumanization, even manipulation techniques to influence an individual's beliefs (Bambang & Fitriana, 2017).

### *Social Network Theory (SNT)*

Social networks are networks that have a special type where there is an interaction that connects a bond from one point to another in the network and forms a social relationship. Based on this type of bond, then directly or indirectly the members of a social network are humans. Social relations can be said to be a path that connects one person to another where through this path something can be flowed, such as goods, services, and information. Social relations consisting of two people reflect the existence of role expectations from each of their interaction partners. The behavior manifested in social interactions is systematic, although the perpetrators are not necessarily aware of it. Achieving good social relations will facilitate the development of social networks. Social networks are very important in society because in this world it can be said that there is no one who is not in someone else's social network. However, society does not always use all existing social relations to achieve its goals, but must adjust them according to space, time, or social context (Agusyanto, 2007). Social networks refer to interactions that occur between many members of a group or between different groups. Network theory emphasizes the importance of understanding structures on both a large and small scale, indicating that the role of actors is not limited to individuals, but can also include groups, organizations, and even broader scopes. These relationships can form in various social contexts, ranging from large-scale to more limited (Ritzer & Douglas, 2004).

Barnes (1969) in the book *Social Networks in Organizations* (Agusyanto, 2007) distinguish networks for the purpose of his research. According to him, networks are divided into total networks and partial networks. Total networks are used to refer to complex social networks, and partial networks to refer to networks that only contain one type of social relationship. Another thing is if social networks are reviewed from the purpose of social relationships that form networks. Several sociologists and anthropologists from several literatures say, from this side social networks can be divided into three types, namely (Agusyanto, 2007):

1. Network of interest, where the network is formed from social relationships that are based on interests.
2. Network of power, where the social relationships that form the network are charged with power. Power here is the ability of a person or social

unit to influence the behavior of a person and decision maker or other social unit through control.

3. Emotional network (network of sentiment), where the network is formed on the basis of social relationships that are emotionally charged. The social relationship itself is actually the goal of social action such as romance, friendship or kinship, and the like. Social structures formed from emotional relationships are generally more stable or permanent.

These three types of social networks in real life often intersect. These encounters create tension for stakeholders because the situational logic or social structure of each type of network is different or incompatible. Therefore, there is often a contradiction between the actions and attitudes that the actors manifest. (Hidayaturrehman & et al., 2020).

### ***Social Construction of Technology (SCOT)***

According to Wiebe E. Bijker and Trevor J. Pinch, technology does not shape human action patterns, but technology is born from the culture of society as an answer to human needs (Bijker et al., 1989). Bijker states that Social Construction of Technology in his book entitled *The Social Construction of Technological System* makes the claim that:

“.. In the social constructivist approach, the key point is not that the social is given any special status behind the natural; Rather, it is claimed that there is nothing but the social: socially constructed natural phenomena, socially constructed social interests, socially constructed artifacts, and so on (Bijker et al., 1989)”

Based on the explanation given above, it can be concluded that in the social construction approach, the main key is not a phenomenon that is natural or inherent. On the contrary, this phenomenon is claimed to be nothing other than a social construct by humans through social, cultural and linguistic interactions.

So, science and technology are basically cultural reconstructions through social processes. Thus, basically humans are the creators of technology itself so that their role is not as slaves to technology, but as controllers. Because as controllers, humans can use the technology for good and vice versa it can also be used for bad or evil.

### **METHODOLOGY**

This study explains the relevance of the threat of cyber terrorism and social media utilized by terrorist groups. *Media Literacy in Countering Radicalism and Terrorism Propaganda Through Internet Media* which explains that media literacy is the ability of society to use mass media, especially the internet, intelligently, critically, and wisely. In an effort to overcome radicalism and terrorism propaganda through internet media, it is necessary to continue to improve media literacy skills so that the Indonesian nation has a strong defense in its society against radicalism and terrorism propaganda (Sari, 2017).

*The Doctrine of Radicalism Terrorism Through Social Media in Indonesia* examines the negative impacts of using social media, including loss of privacy, decreased quality of information, widespread dissemination of untruths, and the emergence of radical groups in the online environment. Followers of radical or

extremist ideologies use freedom of speech on social media to spread information that can influence society, even recruiting to support their views (Shodiq, 2021).

Strengthening Global Cyber-Terrorism Actions Through New Media which explains the phenomenon of global cyber-terrorism actions, the variants of new media used and the current situation *cyber terrorism* in Indonesia. The results of his research show that the use of the internet by terrorist groups is triggered by the weaknesses of traditional mass media, such as television and print media, which are considered no longer safe and vulnerable to content manipulation related to terrorist group activities. One of the most sophisticated terrorist groups in utilizing online media for terrorist purposes is the Al-Qaeda group.

Based on research and reports that have been studied, online media that are open to the public and often used by terrorist groups include platforms such as YouTube, *online game*, websites, social media, such as Twitter, Facebook and a kind of online magazine. Since the Bali bombing in 2002, Indonesia has become one of the countries that has felt the strong impact of the threat of cyberterrorism. The level of availability and strength of cyberterrorism, as well as regulations related to the use of online media in a government, will play a key role in determining the level of public security against the threat of terrorist action groups via the internet (Sarinastiti & Vardhani, 2018).

Writing explaining the threat of terrorism by utilizing social media/internet. An approach that applies the theory of social networks and Social Construction of Technology in analyzing how terrorist groups utilizing internet networks/media to launch cyber attacks, spread propaganda such as spreading radical ideology or planning other terrorist activities, one of which is the process of recruiting new members.

The research method used in this study is descriptive qualitative where the data is taken from literature studies (*library research*) to several previous literature or research works and the thoughts of previous researchers and practitioners related to the discussion topics that are evaluated, identified and synthesized (Agus, 2005). Literature research can examine various reference books and previous similar research findings, which are useful in order to obtain fundamental theory for research questions (Anshori & Iswati, 2019).

In addition, researchers have also interviewed terrorist prisoners recruited through social media at the Salemba Class II Correctional Institution, Central Jakarta in 2017. Researchers have also conducted interviews with several former terrorist prisoners affiliated with the IS/ISIS terrorist group in Bekasi in 2021. This study aims to describe the results of the analysis and synthesis related to how social media becomes a means of cyberterrorism in spreading radical ideology and recruiting terrorist members.

## RESEARCH RESULT AND DISCUSSION

In 2017, the author interviewed a terrorist prisoner who said that he was influenced by the radical understanding of terrorism from social media. While seeking knowledge about religious understanding on social media, he entered a study that eventually had someone communicate with him personally. Furthermore, the person indoctrinated the radical understanding of terror,

taught him to make bombs and ordered a suicide bombing in a church. During the process, the terrorist prisoner had never met his mentor until he served his sentence. When he was practicing making bombs behind the house, there was a big explosion so that his older sister asked what the explosion was. However, after it was explained that it was just a firecracker explosion, his sister immediately became silent.

According to several former terrorist prisoners, most of the Indonesian female workers working in Hong Kong were also influenced and recruited by terrorist groups affiliated with the IS/ISIS group through social media. In addition to those who went to Syria, some of them were recruited by being courted or even made wives, while the terrorists were still prisoners. Some even had their property drained by the terrorist prisoners.

The Mujahirin At Tauhid Terrorist Group affiliated with ISIS recruits through social media. The mode of the MAT group is to enter social media groups, then in addition to interacting with other members, they will invite members of the social media group who are considered to have the same understanding as ISIS supporters to join a special social media group for MAT members. After that, the MAT group planned terrorist actions in Indonesia through the social media groups they had created (Putra & Priyanto, 2021).

Social media differs from conventional media in many aspects. These include the level of interactivity, reach, frequency, usability, responsiveness, and continuity. Unlike traditional media, where only a few capable institutions can disseminate information to a wide and unlimited audience, social media gives every individual the ability and convenience to publish or access information. New communication technologies, such as mobile networks and the easily accessible and affordable web, create highly interactive platforms, allowing individuals and communities to share, discuss, and edit content. Through social media, consumers of information also act as producers or communicators. This two-way communication encourages the formation of a large and dispersed group of communicators. Virtual communities using social media are increasingly popular globally, especially among the younger generation (Sulfikar, 2018).

The millennial generation is the main target for the spread of extreme terrorist ideology because they are considered to have high motivation to learn and develop. Terrorist groups are interested in recruiting these young people because they are considered to have great potential. This is exacerbated by the fact that the younger generation is more skilled in using and applying digital technology. The National Counterterrorism Agency (BNPT) has noted that since 2014, the spread of terrorism-related content has increased significantly in the digital realm. Terrorists are now taking advantage of this technological advancement to facilitate the process of recruiting new members. According to the Director of Law Enforcement of BNPT and Spokesperson of BNPT, Brigadier General Eddy Hartono, terrorist groups have dominated and taken control of the digital space. Many of them do not even need to meet face to face or know each other directly to feel that they have the same views (Susanti et al., 2023).

Terrorist acts that often involve young people mostly occur because they take advantage of unstable psychological conditions. In addition, this group of young people also tend to have a high spirit of idealism. However, unfortunately, individuals who are influenced by this radical ideology are often not fully able to understand information related to propaganda and indoctrination carried out by terrorist groups. Propaganda spread by terrorist organizations often contains speeches or lectures that condemn injustice in various countries, emphasize the need to act to uphold justice, and claim that violence is a way to overcome or solve the problem. The content of the speeches or lectures also includes a religious context as propaganda that violent acts are justified under the pretext of religion. They interpret it exclusively to achieve their goals.

With the evolution of the digital realm, the internet is often considered an efficient means of communication for terrorist groups, providing them with a relatively high degree of anonymity. In addition, the internet provides access to a large amount of information at a very low cost compared to other conventional means of communication (Hilkevics & Hilkevics, 2017; Limba et al., 2017). The potential benefits they gain include the availability of important information on the internet, such as guides to making explosives, instructions on how to acquire weapons of mass destruction, or tactical strategies for terrorism. Benson(2014)highlighting that this kind of information can give perpetrators the full ability to plan terrorist attacks and act independently (Benson, 2014; Shodiq, 2021).

In the framework of social network theory (SNT) according to Barnes (1969), the phenomenon of cyber terrorism is closely related to where *cyber terrorism* often operate through networks consisting of individuals, groups, or entities that work together. They use these networks to launch cyber attacks, spread propaganda or plan other terrorist activities, one of which is the spread of ideology and the recruitment process. The internet enables the process of online radicalization, where individuals can be exposed to radical ideology and terrorist propaganda through various social media platforms. This can also be categorized as a power network, where terrorists from a group can control digital media by using the internet as a tool for spreading ideology to recruit and seek support or sympathy among the public. Influencing the intensity of site visitors and online information that is targeted by terrorists and this is played through interactions with prospective members via chat, email, and so on. The recruitment method carried out by terrorists by utilizing the internet through social media such as Facebook is used to recruit people. One case that occurred in 2014, where a witness was questioned after previously being recruited and sent to Syria. This witness admitted to making friends through the Facebook platform and Facebook chat and was promised facilities to go to Syria (Golose, 2015).

This recruitment is an important agenda for terrorists in rallying support from the community that will be their target. Like any form of propaganda, recruitment is intended to attract sympathizers to join a terrorist network or organization. Then it is also hoped that terrorist cadres can conduct training and preparation with materials that are disseminated through social media platforms such as Facebook, Twitter, Telegram, and now Instagram has become a place

used by several terrorists to conduct propaganda and recruitment. Knowing that the social media platform has many users from various circles, including millennials and gen z.

The legal system is expected to play a role in anticipating developments and changes that occur in society, by ensuring that the implementation can run regularly, orderly, and smoothly. In general, what is regulated through legal procedures, such as in the form of legislation or judicial decisions, is considered better and more beneficial than unplanned changes. In its development, Indonesia has currently formed legislation that specifically regulates technology and information-based cybercrime, namely Law Number 11 of 2008 concerning ITE (Adam, 2014). Almost all articles can be applied to protect against cyber terrorism, especially internet users. However, the author concludes that this Law is not yet effective enough in overcoming cyber terrorism.

Law enforcement in handling cybercrime in Indonesia is still not optimal and effective. Several factors influence the efficiency of law enforcement against *cybercrime*, including legal aspects, availability of law enforcement and law enforcement infrastructure. Of the three factors, the factor that has the most significant impact on the weakness of law enforcement in combating cybercrime in the context of transnational crime is the lack of legal substance and the lack of adequate law enforcement.

The government, through the Ministry of Information and Communication, has a communication strategy that has been used by Kominfo to prevent radicalization on social media, namely by means of counter narratives, blocking, providing informative, persuasive and educational messages and content to improve public literacy. However, the fact is that even though social media used by terrorist groups in propaganda and recruitment has been blocked, they will reappear in greater numbers and better quality. Of course, this is a challenge for Kominfo in maintaining national security from the threat of cyber terrorism (Utomo, et al, 2022).

## CONCLUSIONS AND RECOMMENDATIONS

The development of internet technology, especially in the context of social media, has influenced the way radical and extreme propaganda is spread. The emergence of social media platforms has made it easier for users to share violent terrorist content, which has dramatically provided powerful means and tools for terrorist networks to support activities, legitimacy, and effectiveness in the process of propaganda and recruiting new members. Similar to the role of the internet in the involvement of terrorists in information technology. In this way, the influence and spread of radicalization ideology can occur. The internet plays a very important role in the radicalization process, even more significant than religious institutions. Terrorist networks use violent campaigns as a propaganda tool or as a way to advance operational tactics at the global and local levels. The government through the Ministry of Communication and Information and other institutions has also tried to prevent propaganda and recruitment by terrorist groups. The role of the entire community is the key to success in suppressing propaganda and recruitment by terrorist groups.

## ADVANCED RESEARCH

The proliferation of internet technology, particularly through social media, has fundamentally transformed the dissemination of radical and extremist propaganda, enabling terrorist organizations to leverage digital platforms for recruitment, ideological indoctrination, and operational coordination. Unlike traditional methods of radicalization, which were often confined to religious or ideological institutions, online spaces facilitate the rapid and borderless spread of extremist narratives, amplifying their reach with sophisticated algorithms that inadvertently reinforce echo chambers and ideological silos. Terrorist groups exploit encrypted communication channels, multimedia content, and persuasive narratives to attract vulnerable individuals, fostering a sense of belonging and ideological justification for violent actions. Moreover, the strategic use of cyber tools, including AI-driven propaganda, deepfake technology, and the dark web, has further complicated counterterrorism efforts. While government agencies, such as the Ministry of Communication and Information, have implemented measures to curb the digital proliferation of extremist content through content moderation and cybersecurity initiatives, the effectiveness of these efforts relies heavily on proactive community engagement, digital literacy, and international cooperation in dismantling online radicalization networks.

## REFERENCES

- Aa Bambang A.S. Fitriana, I. (2017). Cyberterrorism: Suatu Tantangan Komunikasi Asimetris Bagi Ketahanan Nasional, *INTER KOMUNIKA Jurnal Komunikasi* Vol 2, No.1, Th, 2017. <http://dx.doi.org/10.33376/ik.v2i1.12>
- Banez, J. D. (2010). *The Internet and The Homegrown Jihadist Terrorism: Assessing U.S. Detection Techniques* [Thesis]. Naval Postgraduate School. [https://voxpath.eu/wp-content/uploads/filebase/ma\\_thesis/The-Internet-and-Homegrown-Jihadist-Terrorism-Assessing-U.S.-Detection-Techniques.pdf](https://voxpath.eu/wp-content/uploads/filebase/ma_thesis/The-Internet-and-Homegrown-Jihadist-Terrorism-Assessing-U.S.-Detection-Techniques.pdf)
- Blane, J. V. (Ed.). (2003). *Cybercrime and Cyberterrorism: Current Issue* (UK edition). Nova Science Pub Inc. <https://www.amazon.com/Cybercrime-Cyberterrorism-John-V-Blane/dp/1590337115>
- Breen, G.-M. (2008). Examining Existing Counter-Terrorism Tactics and Applying Social Network Theory to Fight Cyberterrorism: An Interpersonal Communication Perspective. *Journal of Applied Security Research*, 3(2), 191–204. <https://doi.org/10.1080/19361610802135888>
- Colarik, A. (2006). *Cyber Terrorism: Political and Economic Implications*. IGI Global. <https://doi.org/10.4018/978-1-59904-021-9>
- Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The future of Terror, Crime, and Militancy* (pp. 239–288). RAND. <https://faculty.nps.edu/dedennin/publications/ActivismHacktivismCyberterrorism-NetworksAndNetwars.pdf>

- Gardner, F. (2013, November 2). *How do terrorists communicate?* BBC News. <https://www.bbc.com/news/world-24784756>
- Golose, P. (2015). *Invasi Terorisme Ke Cyberspace*. Yayasan Pengembangan Kajian Ilmu Kepolisian. <https://lib.ui.ac.id/detail?id=20420244>
- Hilkevics, S., & Hilkevics, A. (2017). The comparative analysis of technology transfer models. *Entrepreneurship and Sustainability Issues*, 4(4), 540–558. [https://doi.org/10.9770/jesi.2017.4.4\(11\)](https://doi.org/10.9770/jesi.2017.4.4(11))
- Holbrook, D. (2015). A critical analysis of the role of the internet in the preparation and planning of acts of terrorism. *Dynamics of Asymmetric Conflict*, 8(2), 121–133. <https://doi.org/10.1080/17467586.2015.1065102>
- Holt, T. J. (2012). Exploring the Intersections of Technology, Crime, and Terror. *Terrorism and Political Violence*, 24(2), 337–354. <https://doi.org/10.1080/09546553.2011.648350>
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), 59–68. <https://doi.org/10.1016/j.bushor.2009.09.003>
- Limba, T., Plêta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, 4(4), 559–573. [https://doi.org/10.9770/jesi.2017.4.4\(12\)](https://doi.org/10.9770/jesi.2017.4.4(12))
- Lumbaca, S., & Gray, D. H. (2011). The Media As An Enabler For Acts Of Terrorism. *Global Security Studie, Volume 2*(Issue 1). <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7d220174259ce80d885a029fdce9e18dd333ba40>
- Mahardhika, D., Cheryanti, G., Salim, K., & Natania, M. (2023). Terorisme Siber Dilingkungan Generasi Millennial Saat Pandemi. *INNOVATIVE: Journal Of Social Science Research*, Vol. 3(No. 5), 749–757. <https://j-innovative.org/index.php/Innovative/article/view/4919/3453>
- Matusitz, J. (2005). Cyberterrorism: How can American foreign policy be strengthened in the Information Age? *American Foreign Policy Interests*, 27(2), 137–147. <https://doi.org/10.1080/10803920590935376>
- Ogun, M. N. (2012). Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes. *Journal of Applied Security Research*, 7(2), 203–217. <https://doi.org/10.1080/19361610.2012.656252>
- Putra, Y.G & Priyanto, S. (2021). Mengungkap Perekrutan Jaringan Kelompok Teror Muhajirin At-Tauhid (Mat) di Media Sosial, *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, Vol 8 No 7 Tahun 2021, 2247–2262 <http://dx.doi.org/10.31604/jips.v8i7.2021.2247-2262>
- Putri, D.S. (2019). Cyber Terrorism: Strategi Propaganda dan Rekrutmen ISIS di Internet Dan Dampaknya Bagi Indonesia Tahun 2014-2019, *Journal of International Relations*, Volume 5, Nomor 4, 827–833. <https://doi.org/10.14710/jirud.v5i4.25094>
- Radin, P. (2002). Book Review: *Networks and Netwars: The Future of Terror, Crime, and Militancy*. *New Media & Society*, 4(2), 300–304. <https://doi.org/10.1177/146144480200400211>
- Sagena, U. W. (2019). Memahami Keamanan Tradisional dan Non-Tradisional Di Selat Malaka: Isu-Isu Dan Interaksi Antar Aktor. *Jurnal Hubungan*

- Internasional Interdependence*, Vol. 1, 72–90.  
<https://ocs.unmul.ac.id/index.php/JHII/article/view/1891/1435>
- Sari, B. D. A. C. (2017). Media Literasi Dalam Kontra Propaganda Radikalisme Dan Terorisme Melalui Media Internet. *Jurnal Prodi Perang Asimetris*, Vol. 3(No. 1), 15–31. <https://doi.org/10.33172/pa.v3i1.91>
- Sarinastiti, E. N., & Vardhani, N. K. (2018). Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism Melalui New Media. *Jurnal Gama Societa*, Vol. 1(No. 1). <https://doi.org/10.22146/jgs.34048>
- Seib, P., & Janbek, D. M. (2011). *Global Terrorism and New Media The Post-Al Qaeda Generation*. Routledge. [https://www.routledge.com/Global-Terrorism-and-New-Media-The-Post-Al-Qaeda-Generation/Seib-Janbek/p/book/9780415779623?srsId=AfmBOoq8klFu-aykJ1ozQcODLLu349KMPuU32m\\_FzZeXset9VP9gdhO9](https://www.routledge.com/Global-Terrorism-and-New-Media-The-Post-Al-Qaeda-Generation/Seib-Janbek/p/book/9780415779623?srsId=AfmBOoq8klFu-aykJ1ozQcODLLu349KMPuU32m_FzZeXset9VP9gdhO9)
- Shodiq, Moh. D. (2021). Doktrin Radikalisme Terorisme Melalui Media Sosial Di Indonesia. *Jurnal Penelitian Hukum Legalitas*, Vol. 15(No. 1). DOI: [10.31479/jphl.v15i2.221](https://doi.org/10.31479/jphl.v15i2.221)
- Soriano, M. R. T. (2008). Terrorism and the Mass Media after Al Qaeda: A Change of Course? *Athena Intelligence Journal*, Vol. 3(No. 1), 1–20. <https://ciaotest.cc.columbia.edu/journals/aij/v3i2/0001004.pdf>
- Suhito, Y. P. (2017). *Transformasi Natur Terorisme Kontemporer: Studi Kasus Praktik Cyberterrorism oleh Islamic State of Iraq and Syria (ISIS)*. [https://www.academia.edu/39293035/Transformasi\\_Natur\\_Terrorisme\\_Kontemporer\\_Studi\\_Kasus\\_Praktik\\_Cyberterrorism\\_oleh\\_Islamic\\_State\\_of\\_Iraq\\_and\\_Syria\\_ISIS](https://www.academia.edu/39293035/Transformasi_Natur_Terrorisme_Kontemporer_Studi_Kasus_Praktik_Cyberterrorism_oleh_Islamic_State_of_Iraq_and_Syria_ISIS)
- Sukoco, A., Syauqillah, M., & Ismail, A. U. (2021). Media, Globalisasi Dan Ancaman Terorisme. *Journal of Terrorism Studies*, 3(2). <https://doi.org/10.7454/jts.v3i2.1039>
- Sulfikar, A. (2018). Swa-radikalisasi Melalui Media Sosial di Indonesia. *Jurnalisa*, Vol. 4(No. 1), 76–90. <file:///C:/Users/Asus/Downloads/5622-Article%20Text-13283-1-10-20180809.pdf>
- Susanti, E., Ismira, A., & Sadriani. (2023). Analisis Propaganda Islamic State of Iraq and Syria ( ISIS ) di Indonesia Melalui Jalur Media Sosial. *Hasanuddin Journal of International Affairs*, Vol. 3(No. 2). <https://doi.org/10.31947/hjirs.v3i2.27663>
- Utomo, ES., Sukabdi, ZA., Priyanto, S. (2022) Strategi Pencegahan Radikalisasi Melalui Media Sosial Selama Pandemi Covid-19 oleh Kementerian Komunikasi dan Informatika (Kominfo), Nusantara: *Jurnal Ilmu Pengetahuan Sosial* 9 (8), 3037-3046. <http://dx.doi.org/10.31604/jips.v9i8.2022.3037-3046>