SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 01 No. 02 (2024), pp. 128-137
Research Article
doi: https://doi.org/10.70710/sitj.v1i2.17

Counter Radicalization in Cyberspace by the Police

Abim Aji Akbari[1,a,*], Basir Sagena[1], Muhamad Syauqillah[1]

[1]School of Strategic and Global Studies, University of Indonesia, Jakarta, Indonesia
[a]abimakbari@gmail.com; [b]basirsagena@gmail.com; [c]muhamadsyauqillah@ui.ac.id
*Corresponding author

Article Info
Received: 13-Nov-2024
Revised: 20-Nov-2024
Accepted: 01-Dec-2024

Keywords
Cyber; Police; Radicalization; Religion; Terrorism

Abstract
This article examines further how the Indonesian police carry out counter-radicalization enforcement in cyberspace. This is important because radicalism triggers a person to be violent towards different views, and this does not follow the nature of the diversity of the Indonesian nation. Radicalism is the embryo of terrorism. This situation becomes more dangerous when radicalization efforts are carried out through cyberspace, which can be accessed by the entire community, including impressionable teenagers. In this regard, the Indonesian National Police, which maintains security and order and protects the community, also takes part in counter-radicalization in cyberspace to ward off negative influences that underlie intolerant and radical actions. This particular observation of the role of the police against radicalism through online media is what then differentiates it from similar research. The discussion uses a qualitative research approach and literature study method, incorporating counter-radicalization theory through the Internet. This paper finds that counter-radicalization in cyberspace by the police is cyber patrols and content takedown, establishing a social media task force, increasing the role of moderate religious mass organizations, strengthening religious literacy, and collaborating with national and international institutions and digital platforms. In addition, law enforcement is following the ITE Law and the Terrorism Law.

1. Introduction

The use of the internet in the digital era and the rapid advancement of technology is now the most loved means of finding information. In addition to being fast and easy, cyberspace provides vast and almost unlimited information content. The Indonesian Internet Service Providers Association (APJII) published data that the number of Indonesians using the internet in 2024 reached 221,563,479 people, or 79.5% of the total 278,696,200 Indonesian population recorded in 2023. Then, based on a survey from We Are Social, around 139 million people, or as much as 49.9% of the Indonesian population, actively use social media as of January 2024. On average, they spend up to 7 hours 38 minutes per day browsing cyberspace, with reasons for spending leisure time (58.9%), interacting with friends and family (57.1%), and viewing and reading trending content on the internet (48.8%).

Unfortunately, the ease of finding information in cyberspace is also followed by the ease of placing narratives. This ease, which is pretty without rules, makes internet facilities have a positive impact and a negative impact because some narratives cannot be fully accounted for. At its momentum, it can pose a threat to public security and order and even national resilience when the internet is used to spread radicalized content in the name of religion. Radicalism is an attitude that wants to bring rapid and revolutionary changes to existing values through violence and extreme actions. Thus, radicalism is the embryo of terrorism. People who have been exposed to radicalism will easily reject different views and be violent towards people who differ from them. This is not by the nature of diversity owned by the Indonesian nation. In this case, exclusivity is related to religion and threatens the peace and freedom of adherents of other religions to worship. It is expected to endanger the safety and lives of those with different views or

beliefs. Sadly, cases of intolerance or conditions of worship limitations for religious minorities are arguably a reasonably common sight in Indonesia.

A recent case that caught the public's attention was when a middle-aged woman, known to work as a State Civil Apparatus (ASN) in Bekasi City, scolded and tried to disperse a Christian congregation that was worshiping in a location adjacent to her house. This incident occurred in September 2024. In addition to this case, there was also an incident of intimidation and violence using sharp weapons when several residents, one of whom was the Head of the Neighborhood Association (RT), wanted to disperse 15 Catholic Pamulang University (Unpam) students who were holding a Rosary prayer event in one of the boarding houses on Jalan Ampera, Babakan Setu Village, South Tangerang City, on May 5, 2024.

Moderation and tolerance in religious life are the main foundations for maintaining social harmony in a diverse society, especially in Indonesia, which has religious and cultural diversity. However, the case above illustrates that the practice of intolerance is still often found, especially in interfaith interactions. Moderation in religion is an attitude that avoids extremism and emphasizes balance in religious practice. According to the Islamic perspective, moderation (wasathiyah) is a concept that teaches people to be in the middle, not excessive in worship, and not extreme in treating others, especially those with different beliefs. In plural Indonesia, moderation is essential to maintain religious harmony. Ustad Muhammad Nasir Abbas, a former prisoner of terrorism, explained that the stages of exposure start from the failure to address differences to the potential for radicalism and ultimately lead to acts of terrorism. Therefore, negative influences underlie intolerant and radical actions must be immediately counteracted.

Based on data from the Indonesian Ministry of Religious Affairs, the Religious Harmony Index in 2023 they were increased from 73.09 points in 2022 to 76.02 points despite a significant decline in 2020, from 73.83 points to 67.46 points. The Ministry of Religious Affairs also stated that it will continue to improve community harmony and expects the KUB Index to increase in the coming years with two primary efforts: strengthening moderation and conflict prevention. In line with this, cleaning up radical exposure on social media is also essential. In addition, the three groups most vulnerable to radicalism, according to the latest Radicalism Potential Index from the National Counterterrorism Agency (BNPT), are women, the younger generation, especially Gen Z, and those who are active on the internet. Furthermore, throughout 2023, 2,670 contents containing intolerance, radicalism, and terrorism were found on social media.

The Indonesian government, through the Ministry of Communications and Digital RI, continues to make efforts to deal with the spread of radical content through the Internet media. One of these efforts is by blocking sites that are considered violating. Another effort is to cooperate with various parties in the context of counter-narratives. In its implementation, the Ministry of Communication and Digital RI has provided access to several other state institutions to help counteract the spread of radical content on social media, including the Indonesian National Police (Polri) through the Directorate of Cyber Crime of the Criminal Investigation Agency (Dittipidsiber Bareskrim), Special Detachment 88 Anti-Terror (Densus 88), and also special units for handling cybercrime in the Regional Police (Polda).

Densus 88 Spokesperson Kombes Pol Aswin Siregar revealed that social media is a significant factor in teenagers' radicalization process and is used by extreme groups to strengthen terror ideology. He says reading and watching radical content individually can lead to radicalization. Self-radicalization (considering all things different from themselves as threats and enemies that must be eliminated) is very dangerous. Individuals can be influenced without direct guidance from mentors.

Setia's research (2021) shows that the future of Indonesia is very worrying because the radicalism movement is increasing. This can be seen from the changes in the radical group movement in Indonesia, which now uses social media as a new platform to spread public beliefs wrapped in post-truth political practices. Radical groups use various approaches to support their cause, and one of them is to boldly incorporate elements of information manipulation into proselytizing statements made to the general public. This represents a potential threat to the future of Indonesian democracy, especially in terms of the struggle to maintain religious moderation in Indonesia. Therefore, major religious organizations in Indonesia, such as Nahdhatul Ulama and Muhammadiyah for Muslims, as well as other components of society, have a significant role in providing counter-narratives through social media.

According to research by Sanjaya and Putranto (2022), online and social media can encourage radicalization. Most terrorist groups focus on publicity, propaganda dissemination, recruitment, network

building, and mobilization. As a result, social media is used to radicalize individuals and groups for political and social change, especially among teenagers and the younger generation. Effective social media can make people feel directly involved in an event and connect them with various sources of information. In addition, social media can increase people's emotional reactions so that they engage with and support radical movements.

Bureni, Ismail, and Iryani (2022) conducted research showing that terrorism has entered people's lives like a virus, and terrorism has spread to many people in the country for decades. If previously the radicalism virus spread through educational institutions and places of worship, now social media makes it easier to spread the virus. Terrorist groups spread the understanding of radicalism through propaganda activities that are carried out secretly and systematically. This makes it difficult for the government to identify and prevent its spread. The current focus is on repressive law enforcement because the Counterterrorism Law does not cover the criminal threat of spreading radical propaganda through social media. Densus 88 Anti-Terror cannot effectively enforce the law against those who spread radical propaganda but have not yet committed the crime of terrorism. In contrast, counterterrorism through non-criminal means begins with cyber patrols and the takedown of radical content, which BNPT and Polri carry out in collaboration with the Ministry of Communication and Digital RI.

Wibowo and Hadingrat (2022) studied social media, which currently plays a vital role in spreading radicalism in Indonesia and is supported by increased internet usage. Indonesia's positive law has yet to entirely regulate radicalism's spread through social media. Currently, the focus of efforts to counter radicalism through social media in Indonesia is on repressive law enforcement. The concept of criminal policy to counter the spread of radicalism through social media is formulated in three points: surveillance, enforcement, and platform and community cooperation. Enforcement will include the removal of content on social media and evaluation to measure the level of radicalization of the perpetrator.

In addition, Utami and Yumitro's (2023) research mentioned that radical groups use social media as a tactical tool to spread their ideology worldwide. The government implements three main strategies to tackle radical ideology on social media. First, a cybersecurity strategy that is used as a policy maker, as an instrument, as shock therapy, and as a dispute resolver. Second, an educational strategy that uses positive content to educate the public about the dangers of radicalism and spread peaceful messages through social media. In addition, the third approach is law enforcement, which is made possible through the ITE Law Number 19 of 2016 on the Crime of Cyber Radicalism.

2. Method

2.1. Methodology Approach

This research uses descriptive qualitative methods, meaning qualitative data describes events, phenomena, or social circumstances. This approach aims to explore or portray the social situation to be studied in depth and thoroughly. Furthermore, data collection techniques are carried out by literature study, which involves reviewing previously published written sources. After collecting the required data, descriptive analysis is carried out, describing the data so the reader can understand it. In this case, the researcher analyzes the police's efforts and constraints on counter-radicalization in cyberspace.

2.2. Theoretical Foundation

Counter Radicalization through the Internet

According to Karen J. Greenberg (2016), the authorities can take three actions to deal with the spread of radical group propaganda through the internet media: providing disruption, diversion, and counter-messaging.

a. Disruption

One of the actions that can be taken to counter propaganda through the internet is to interfere in the form of technical intervention to radical sites provided by internet companies. Through cooperation with these internet companies, accounts on social media that spread propaganda and even recruitment can be stopped. Although considered adequate, Greenberg stated that there are several obstacles in the effort to

close radical accounts, including determining content that falls into the radical category because social media is related to a global community with different norms. Then, accusations, stings, and censorship on social media can reduce the platform's credibility. For this reason, the government must have precise regulations in determining the indicators of content classified as radical. According to Greenberg, the next obstacle is the difficulty of approaching internet and technology companies to provide information on their users to the government. In addition, easy access to the internet and social media platforms is another obstacle. Account closures are vulnerable to being responded to by the individuals behind them by creating new accounts or changing platforms. Closing radical accounts can also trigger groups to go to the dark web, the part of the internet that is not accessible from common browsers like Google Chrome, making it harder to track.

b. Diversion

Diversion and alternative approaches are carried out by encouraging the community to use social media to engage in counter-radicalization efforts and create harmony. The government also needs to build relationships with communities and non-governmental organizations. Activities that the government can carry out in this action are encouraging community involvement and peace campaigns on social media. Greenberg gives an example of a diversionary action that Google has taken. The company redirects specific keywords or topics users search to sites that contain counter-radicalization messages and peace narratives.

c. Counter-Messaging

This is done by spreading peaceful and tolerant messages contradicting the radical narrative. Counter-messaging efforts fall into two categories. The first category includes discussions on religious teachings by holy books and proper teachings. Internet users can be taught by religious leaders and teachers about religious knowledge that coexists in humanity. The second category is the idealization of life in radical groups. These groups often spread the narrative that implementing a government based on religion is the solution to every problem. Therefore, it is necessary to spread narratives about the incompatibility or the many new problems caused if Indonesia becomes a religious state, as well as narratives about the beauty of living amid diversity in Indonesia.

3. Result and Discussion

3.1. Modus Operandi of Radicalization through Internet Media

Radical content is information or ideas posted in the media, both online and in print, that contain radical elements, such as encouraging and condoning the use of violence against people who disagree with the group, showing intolerance, and promoting propaganda that encourages people to oppose the system they consider reasonable. The National Counter Terrorism Agency (BNPT) interprets the characteristics of radical content as (1) Having principles of interpretation of group teachings that are different or contrary to existing group practices or movements. (2) Using violence that is considered suitable by the group, which includes fighting the government or apparatus, even allowing the killing of someone who is considered deviant. (3) Blaming other people or groups for differing opinions and suspecting the other party of having bad intentions towards one's group. (4) Provoking people to join and participate against other opposing groups.

Also, according to BNPT, radical content is harmful to individuals because:

- Triggering intolerant attitudes, i.e., unwilling to respect the opinions or beliefs of other groups or people considered different from their views.
- Fanatic, i.e., feeling that their group or belief is entirely correct and blaming other groups or beliefs that differ from theirs.
- Exclusive, i.e., considering themselves or their group as different and not on the same level as other groups or beliefs.
- Revolutionary, which does not hesitate to use violence to achieve the group's goals.

Radical groups often use social media to spread extremism. They may use Facebook, YouTube, Twitter, blogs, and free messaging apps like WhatsApp to propagandize, gain influence, and recruit members. Many accounts on social media managed by radical groups spread propaganda about their political views. They also dismiss democracy as a national system of government and reject Western concepts, products, and ideas such as liberalism, secularism, human rights, gender equality, and pluralism. Its propaganda is carried out through videos of activities, periodic posts, and even the organization's internal decision-making process. They are systematically and widely spread, even in schools and universities.

Setia (2021) outlines two motives for mobilizing public opinion, which in turn become the leading spirit of radical groups, which in this case is exemplified by the case of the Hizbut Tahrir (HT) organization, to carry out their agenda on social media. First, political reasons. This motivation is related to the political year or capitalizing on the heated political situation, with HT claiming that it is engaged in political struggle (although it refuses to participate in parliamentary politics). In addition, the current political momentum is used to raise awareness of the refusal to participate in elections; in other words, they promote abstention. The propaganda aims to tell people that elections will not solve the national problems. As a result, people should join HT, and there is no need to participate in the election—second, philosophical motivation. Over the years, Islamic ideology in the form of the Khilafah Islamiyyah has been a milestone in HT's struggle. The condition of Indonesia, which adheres to secular-capitalist democracy, also encourages the spirit of this ideology. HT argues that Indonesia should adopt Islam because it is the truest ideology and can solve many of the problems facing the country today. The mobilization of public opinion on both motives shows that the group's activities occur frequently, especially when the political situation is of concern.

Despite being disbanded by the government, HT in Indonesia continues to struggle to ground the Khilafah. In the end, social media became the central place for them to spread their ideology and achieve broader goals. Radical groups remain present on social media with claims of fighting for the truth and against evil. Moreover, they can attract public sympathy through content that is interesting and easily understood by many people.

Some of the activities of radical groups launched through social networks include:

- Twisting or frying issues. The act of raising a hot issue on social media with an attempt to link it to religious teachings.
- Dissemination of graphic and video content. This addresses the tendency of people today to pay more attention to graphic or video content than just a series of narratives.
- Creation of groups/fan pages. On Facebook, users can create a group or fan page specifically formed as a forum for exchanging information about understanding extremism.

If we look closely, a critical aspect of radical group movements on social media is that they take advantage of actual public concerns or events. Unsurprisingly, they can control public opinion on social media, as netizens' heated discussions will center on the current event, especially if the content is created repeatedly by each member in an organized, systematic, and massive way. Thus, there is a high probability that the content will go viral or dominate public opinion. In addition, adherents of ideologies different from Pancasila use various state problems and sources of public dissatisfaction with government actions as tools to influence the public. Dissatisfaction will make people credulous, panicky, emotional, and manipulated.

3.2. Police Counter-Radicalization Efforts in Cyberspace

Various radical groups in Indonesia use social media to promote their propaganda and recruit new members, which is a significant threat to the future of the country. As mentioned, their primary target audience is young people, who comprise more than half of Indonesia's population. The younger generation will be easily influenced by religiously-based values of violence, hatred, and hostility, especially as they are in the age of identity search. National theories such as democracy, nationalism, patriotism, and love of country are not accepted by radical activists. Thus, the beliefs of these fundamentalist groups can not only disturb the peace of religious communities but can also endanger civilization, defense and security, political-economic stability, and state civilization.

In carrying out police duties to prevent criminal acts, preventive and repressive actions are interconnected and a combination of related activities in decision-making. However, preventive action is

more emphasized at the implementation level so that exposure to radicalism does not lead to acts of terrorism. The purpose of repressive action is to deter the perpetrators.

There are three strategies used by the police cyber unit to counteract radical information on the internet: socialization strategy, cooperation strategy, and monitoring strategy. The socialization strategy emphasizes repressive efforts through notifications and warnings. The cyber unit must carry out its duties and responsibilities to handle criminal acts in cyberspace, even if there is no complaint from the reporter. Cooperation is needed since countering radical or terror information cannot be done independently and requires collaboration. The police cooperate with related parties, such as the Ministry of Communication and Digital, as well as social media activists or influencers. It is hoped that the public will receive education about the ITE Law. Surveillance strategies, on the other hand, are pre-emptive and preventive measures aimed at tracking, educating, warning, and preventing the public from cyber crimes that may occur.

In more detail, several steps taken to counter radicalization through cyberspace by the police are described as follows:

a. Cyber Patrol

Prevention of radicalization crimes in social media can be started with cyber patrols by Polri in collaboration with the Ministry of Communication and Digital to take down content that is considered violating because it is radical or threatens the position of the Pancasila ideology. To specifically deal with radicalization crimes that occur in cyberspace, Polri has Dittipidsiber Bareskrim, Densus 88 AT, and special units in the Polda. The virtual police or cyber troops are tasked with reconnaissance or cyber patrols. There are undercover efforts where members of a particular unit appear to be part of a radical group by using social media accounts to engage in chat and enter the community.

Cyber Patrol finds a violation, which is then analyzed and profiled word by word, including who the author is, the IP addresses, and the location of the perpetrator's coordinates. In addition to profiling, it is also necessary to do mapping related to when and where content is usually uploaded, what the conversation is, what the purpose is, etc., so that the Police can read the patterns and potential that can occur.

b. Establish a Social Media Task Force

Social media provides more diverse information and uses alternative viewpoints, which is different from information in the mainstream media. This now causes social media users to be greater than mainstream media viewers in Indonesia. Implementing non-criminal crime prevention strategies is carried out by forming a Social Media Task Force. This task force emerged because of the high number of crimes that occurred on social media. Davis et al. (2014) state that the potential of social media is not used to change or add to the work of the police so far but instead encourages good relations between the police and the community. Social media is essential for police institutions to pay attention to because what is channeled through it comes from the community itself.

The relevance of social media as a tool that helps police performance lies in the easy access to information that is always new from time to time, improving two-way communication between the police and the community, as well as asking for clues from the community to help the process of investigating a crime. In addition to informing the public, Polri can use social media to solve and mitigate crime in four critical areas. These areas are as a source of intelligence information, up-to-date information related to security issues, a place to exchange ideas between police institutions, and implementing online crime prevention.

c. Increasing the Role of Moderate Religious Organizations in Indonesia

Radical groups use various tactics to support their cause. One of them is that they do not hesitate to incorporate elements of information manipulation into their campaigns by claiming religious proselytization to the general public. This shows a threat to the future of Indonesian democracy, especially in the struggle to maintain religious moderation. Therefore, significant religious organizations in Indonesia, such as Nahdhatul Ulama (NU) and Muhammadiyah for

Muslims, are crucial for conveying a counter-narrative. That is why the police often embrace religious leaders from prominent organizations in conveying messages of peace and rejection of radical concepts.

d. Strengthening Religious Literacy to the Community

Since social, religious, and psychological factors that weaken the mindset about the importance of unity in diversity cause radicalization in the name of religion, a literacy or education strategy is needed. Efforts to address radicalization and intolerance cannot ignore the role of the broader community in strengthening educational strategies. This includes spreading positive content and peaceful narratives through social media and educating the public on the dangers of radicalization. The police often conduct socialization through digital platforms such as Instagram, Facebook, Twitter, or official online channels, as well as direct meetings at events, either organized by themselves or as resource persons.

The public is urged to be careful when surfing the internet, as radical groups can quickly provide and manipulate information for their political interests. People must be more observant in choosing which religious content to believe in and which contains radical elements harmful to the harmony of the community. Furthermore, religious moderation in Indonesia must be increased by instilling a sense of nationalism and tolerance, preventing provocation and incitement, building positive social media situations, and conducting religious activities that are full of peaceful values.

e. Inter-Agency and International Cooperation

Polri cooperates with national, such as BNPT (National Counterterrorism Agency) and international agencies to strengthen counter-radicalization efforts in cyberspace. This collaboration is essential, given that cyberspace is global, and the spread of radical content can cross national borders. With this collaboration, Polri can be more effective in dealing with the threat of transnational radicalism.

f. Collaboration with Digital Platforms

The police collaborate with social media platforms and digital service providers to identify and take action against accounts that spread radical content. This cooperation allows the police to access the data needed to reveal the identity of the perpetrators and stop the spread of radical content that could trigger conflict or division in society.

g. Law Enforcement

Perpetrators spreading radicalism in cyberspace can be charged with the Electronic Information and Transaction Law (UU ITE) and Law No. 5/2018 on the Criminal Acts of Terrorism. These two laws allow the National Police to impose legal sanctions in the form of severe imprisonment and significant fines, which aim to provide a deterrent effect and reduce the risk of repeating radical actions.

From the description above, strategies or efforts based on indicators of disruption, diversion, and counter-messaging from the theory of counter-radicalization through the internet are fulfilled. Disruption efforts are carried out through cyber patrols, followed up with take-down steps and the formation of a Task Force. This step will be more biting when there is prosecution or law enforcement discipline through the ITE Law and Terrorism Law. Then, diversion efforts are carried out by strengthening religious literacy in the community, especially among internet users. Finally, counter-messaging efforts are carried out by increasing and utilizing the role of moderate religious mass organizations in Indonesia. Religious organizations such as NU and Muhammadiyah provide reliable enlightenment to counter the narrative games of radical groups. These efforts can then become a strategy in the sense of a plan, tactic, method, or tactical management to achieve a goal, in this case, counteracting radical exposure through cyberspace.

3.3. Obstacles for Police in Countering Radicalization in Cyberspace

The main obstacle in countering radicalization in cyberspace is regulation. Radicalism is not regulated in Law 5/2018 on the Eradication of the Crime of Terrorism. Meanwhile, Law No. 19/2016 on Electronic Information and Transactions (ITE) in Article 27 paragraph (3) only regulates defamation and insults, and Article 28 paragraph (2) only on ethnicity, religion, race, and intergroup (SARA).

For this reason, there is no precise regulation on radicalism on the internet. At the same time, in a state of law, the principle of legality is an essential basis to ensure that all people, or residents, are subject to the applicable law and that the means of the state can be used. The only reliable way to combat radicalism in cyberspace is through takedowns. However, this will not permanently impact as perpetrators can easily create accounts or channels and spread other content.

One problem in countering radicalization in cyberspace is determining the perpetrator's identity. Moreover, the rise of anonymous accounts on social media has made this even more challenging. Without a clear system for identifying and scrambling radical content, the police face significant challenges in recognizing and addressing sources of radicalism.

The availability of human resources (HR) is a common problem. The human resources owned are still very limited in quantity and quality. Even with a relatively high level of education, police officers have been unable to meet the specific HR needs for cyber technology empowerment. In addition, the motivation and concern of police members for conduciveness in cyberspace is also not optimal. It is assessed that cyber police members still lack awareness and understanding of their essential role in maintaining public security and order through detection, prevention, repression, and rehabilitation in cyberspace.

Then, the police have a problem because there is no comprehensive cyberspace management system. Each member responsible for managing cyberspace has a different assessment due to the absence of standard guidelines. This causes the process of monitoring and responding to radical content to be inconsistent and ineffective. In addition, the benchmarks for radicalism used by the police often differ from those used by the public. This can lead to different interpretations of content, so the police must have clear standards for classifying radical content. Especially in social media, which has unique characteristics where users can be more critical and opinionated, the police must be careful in their actions.

Furthermore, the police institution's position, which seems non-neutral and only protects the interests of the authorities, can reduce public trust. Often, the public perceives that the police respond differently to specific political issues, which can be interpreted as active participation in politics. This can compromise the integrity of the police institution and make the public doubt the legitimacy of police responses.

The resistance of radical groups is often an obstacle to counter-radicalization efforts implemented by the police, especially in the digital era. Radical groups are highly adaptable and quick to react to changes in counter-radicalization strategies. They can change and evolve their ideology according to the evolving political and technological situation. This makes it difficult for the police to establish a permanent and effective strategy in dealing with the threat of radicalism.

4. Conclusion

The National Police uses various strategies to counteract radicalization in cyberspace. These strategies involve preventive and repressive measures to prevent the spread of radical ideologies through the Internet. Some necessary steps include cyber patrols and content takedowns, the establishment of a social media task force, increasing the role of moderate religious organizations, strengthening religious literacy, and cooperation with national and international institutions and digital platforms. In addition, legal action by the ITE Law and Terrorism Law is implemented to provide a deterrent effect. The strategy encompasses three main approaches: disruption, diversion, and counter-messaging.

On the other hand, there are several significant obstacles faced by the police in implementing counter-radicalization efforts in cyberspace. One of the main obstacles is the lack of specific regulations governing radicalism in cyberspace in the Law. In addition, identifying radical actors in cyberspace is difficult due to the limitations of effective technology to identify sources of radicalism. The limited number and competence of human resources is another problem in handling cyber radicalism. The existing human resources are not fully prepared regarding technical skills and motivation to carry out tasks in cyberspace

optimally. The police also face challenges in unsystematic cyber management, including the lack of clear guidelines and assessment standards for identifying radical content. This has led to inconsistencies in actions and responses to radical content. Public trust in the police is also affected by the perception that the institution is not neutral, especially on specific political issues. In addition, resistance from radical groups that are adaptive and quick to innovate with technology hinders the effectiveness of counter-radicalization strategies. Other constraints include easy access to the internet for radical groups, low compliance of foreign technology companies with local regulations, and inefficient coordination between government agencies in dealing with cyber radicalism. These constraints indicate the need for improvements in regulations, data collection of real identities for social media account owners, improving the quality of human resources, neutral positioning, and strengthening governance and coordination across institutions so that counter-radicalization efforts in cyberspace can run more effectively.

References

Argastya, Alfendo Yefta. (2024). Penanggulangan Terhadap Kejahatan Cyber-Terrorism Melalui Politik Hukum Pidana. Jurist-Diction Vol. 7 (2): 243-260

Bureni, Adi Iksan., Ismail., & Iryani, Dewi. (2022). Penanggulangan Penyebaran Propaganda Paham Radikal Tindak Pidana Terorisme di Indonesia. Jurnal Ilmu Hukum SETARA Vol. 3, No. 1

Greenberg, Karen J. (2016). Counter-Radicalization via the Internet. The Annals of the American Academy of Political and Social Science 668(1):165-179

Haryanto, Agus Tri. (2024). APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang.

Heryanto, Gun Gun. (2018). Media Komunikasi Politik: Relasi Kuasa Media di Panggung Politik. Yogyakarta: IRCiSoD

Jamillah & Raffi, Muhammad. (2022). Kampanye Ide Khilafah: Studi Manajemen Dakwah Akun Facebook Buletin Dakwah Kaffah. TAZKIR: Jurnal Penelitian Ilmu-ilmu Sosial dan Keislaman Vol. 08 No. 1

Januri. (2022). Upaya Kepolisian Dalam Penanggulangan Kejahatan Cyber Terorganisir. Audi Et AP : Jurnal Penelitian Hukum, 01 (02): 94-100

Lintang, Indira. (2024). 10 Media Sosial dengan Pengguna Terbanyak di Indonesia 2024. https://www.inilah.com/data-pengguna-media-sosial-indonesia.

Lubis, Rizky Reza. (2017). Potensi Pengguna Internet Indonesia dalam Counter-Cyber Radicalization. Jurnal Pertahanan & Bela Negara Vol. 7, No. 2: Hal. 19-34

M, Andy Sanjaya & Putranto, Rahmat Dwi. (2022). Upaya Pencegahan Radikalisme Melalui Media Sosial di Kalangan Remaja. J-CEKI: Jurnal Cendekia Ilmiah Vol. 2, No. 1

Maulana, Wakit. (2023). Peranan Kepolisian Dalam Kontra Cyber Terorism. Tesis: Universitas Islam Sultan Agung Semarang

Maulidya, Erine Nur., dkk. (2023). Strategi Penanggulangan Informasi Hoax dan Terorisme di Media Sosial Oleh Unit Polisi Virtual Provinsi Lampung. Jurnal Dakwah dan Komunikasi, Vol.8 No.1

Mubin, Nuril., & Setyaningsih. (2020). Pengaruh Konten Radikal Terhadap Sikap Radikalisme (Analisis Berdasarkan Theory of Planned Behavior dari Ajzen dan Fishbein). Personifikasi Vol.11 No.2

Muthohirin, Nafi. (2015). Radikalisme Islam Dan Pergerakannya di Media Sosial. Jurnal Afkaruna, Vol. 11, No. 2, pp. 240-259

Nurrosikin, Adi Muhammad (2021). Infiltrasi Ideologi Khilafah melalui Media Sosial di Era Pandemi Covid-19 (Tinjauan Teori Media Massa McLuhan). Skripsi: Universitas Islam Negeri Sunan Ampel Surabaya

Pasaribu, Roberto G.M. (2020). Implementasi Strategi Pencegahan Kejahatan Ujaran Kebencian Melalui Media Daring (Analisis Pencegahan Penyebaran Konten Provokatif Oleh Direktorat Tindak Pidana Siber Bareskrim Polri). Tesis: Universitas Indonesia

Prakosa, Pribadyo. (2022). Moderasi Beragama: Praksis Kerukunan Antar Umat Beragama. Jurnal Ilmiah Religiosity Entity Humanity (JIREH) 4.1: 48

Riyadi, Dedi Slamet. (2008). Analisis terhadap Konsep Khilafah menurut Hizbut Tahrir. Skrispi: Institut Agama Islam Negeri Semarang

Setia, Paelani. (2021). Membumikan Khilafah di Indonesia: Strategi Mobilisasi Opini Publik oleh Hizbut Tahrir Indonesia (HTI) di Media Sosial. Journal of Society and Development 1, 2: 33-45

Sunarto. (2018). Pencegahan Persebaran Propaganda ISIS melalui Media Internet di Indonesia. Tesis: Universitas Indonesia

Tawaang, Felix & Mudjiyanto, Bambang. (2021). Mencegah Radikalisme melalui Media Sosial. Majalah Ilmiah Semi Populer Komunikasi Massa Vol. 2 No. 2 Desember 2021 Hal: 131 – 144

Utami, Ihsanul Religy & Yumitro, Gundo. (2023). Strategi Pemerintah Indonesia Dalam Mengatasi Pengaruh Ideologi Transnasional Radikal di Media Sosial. Jurnal Sosial Politik Vol.6 No.1

Wibowo, Kurniawan Tri & Hadingrat, Wahyu. (2022). Penanggulangan Penyebaran Radikalisme melalui Media Sosial dalam Hukum Pidana Indonesia. IBLAM Law Review Vol. 02 No. 03, Hal 56-81

Zakiyudin, Ahmad. (2018). Teknik-Teknik Propaganda Politik Jalaludin Rakhmat (Studi kasus pada Kampanye Pemilu 2014 di Kabupaten Bandung dan Kabupaten Bandung Barat). Jurnal Academia Praja, Vol.1, No.1, h. 3

Zein, Meizar Rudi. (2024). Polri Sebut Radikalisme Mulai Menyebar Menggunakan Media Sosial. https://www.rri.co.id/nasional/887067/polri-sebut-radikalisme-mulai-menyebar-menggunakan-media-sosial.