SEARCCT'S
SELECTION OF ARTICLES
2024

SEARCCT'S SELECTION OF ARTICLES 2024

PUBLISHER
SOUTHEAST ASIA REGIONAL CENTRE
FOR COUNTER-TERRORISM (SEARCCT)
MINISTRY OF FOREIGN AFFAIRS
NO 516, PERSIARAN TUANKU JA'AFAR, BUKIT PERSEKUTUAN
50480 KUALA LUMPUR
MALAYSIA

Tel : (603) 22802800
Fax : (603) 22742734
Email : info@searcct.gov.my

First published in 2024

CONTENTS

EDITOR'S NOTE

The 2024 edition of the *Selection of Articles (SOA)* arrives at a pivotal moment, amid rapid technological advances and complex geopolitical shifts. This collection brings together valuable insights on the evolving challenges in Preventing and Countering Violent Extremism (PCVE), addressing critical issues and emerging strategies within counter-terrorism.

One of the central themes in this edition is the importance of international cooperation, exemplified by partnerships like that between Malaysia and the Philippines, which strengthen resilience against shared security threats. This publication also examines the dual-edged nature of artificial intelligence (AI) in counter-terrorism, alongside the powerful influence of online platforms in amplifying extremist ideologies. Attention is given to the rise of far-right extremism, with a focus on Southeast Asia, Europe, and the United States, shedding light on the global scope of this issue. Additionally, the compilation also emphasises the importance of gender-sensitive approaches, recognising the unique perspectives and contributions women bring to counter-terrorism efforts.

Through this diverse array of topics, the *SOA 2024* aims not only to inform but to inspire policy-makers, practitioners, and scholars to embrace adaptive, inclusive, and forward-thinking approaches in countering terrorism and violent extremism. We hope that this edition serves as both a valuable resource and a meaningful addition to the broader body of knowledge on counter-terrorism and PCVE, fostering collaboration and innovation in the face of evolving threats.

I would like to extend my heartfelt appreciation to our contributors, who have shown unwavering support for SEARCCT and generously shared their expertise with our readers. My sincere thanks also go to the Research and Publication Division of SEARCCT for guiding this edition to completion, and to Prof. Ts. Dr. Zulkifli Abd Latiff, whose exceptional editorial work brought these articles together with clarity and insight.

Finally, to you, the readers of this monograph, it is my hope that the collection of articles in this edition will ignite your enthusiasm and inspire creative, practical solutions for countering the complex threats of terrorism and violent extremism today. As Ibn Khaldun wisely noted, "The knowledge that leads to action is superior to the knowledge that stops at the tongue."

Thank you.

DATO' GANESON SIVAGURUNATHAN
Director-General
Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT)
Ministry of Foreign Affairs, Malaysia

AN ALLIANCE FORGED IN MUTUAL RESPECT AND COOPERATION: THE CASE OF MALAYSIA AND THE PHILIPPINES

Amparo Pamela Fabe

ABSTRACT

The Philippines and Malaysia marked 60 years of staunch diplomatic relations in 2024 which is characterised by mutual respect and cooperation. Both countries can reinforce their bilateral relations through increased engagement in three priority areas: enhanced economic cooperation, commitment to the peace process and renewed maritime security governance. Advanced economic cooperation can be fostered in *halal* industry, food security and digital economy. The renewed commitment to the peace process is shown in the firm support, economic, social and security, for the Bangsamoro Autonomous Region of Muslim Mindanao (BARMM). The enhanced maritime security governance is reflected in various transborder cooperation through the international (SEACAT) regional Trilateral Cooperation Agreement (TCA) and bilateral maritime security cooperation. The strength of Philippine-Malaysian bilateral ties paves the way for peace, regional stability, and mutual prosperity in the Indo-Pacific. Indeed, the continued bilateral engagement of both countries stems from their intertwined history, culture, and heritage as brothers and sisters within the Southeast Asian region.

Keywords: Philippines, Malaysia, MADANI, Technology, Labor cooperation

INTRODUCTION

The era of enhanced mutual respect and cooperation between Malaysia and the Philippines has reached a high note. Last 2023, Malaysian Prime Minister Datuk Seri Anwar Ibrahim remarked that the bilateral cooperation is multi-sectoral, covering trade and investment, education, health and agriculture. New sectors such as the *halal* industry, food security and digital economy were identified as areas for potential economic cooperation. During a joint press briefing with Philippine President Ferdinand Marcos Jr and Prime Minister Anwar Ibrahim, the two countries have agreed to resume the 8th Joint Commission Meeting to be led by both Foreign Ministers. Prime Minister Anwar Ibrahim also spoke of the importance of deepening people-to-people ties between Malaysia and the Philippines and the strategic goal of maintaining vibrant cultural exchanges and tourism. Furthermore, Prime Minister Anwar Ibrahim had acknowledged the Philippine diaspora in Malaysia and their contribution to the economies of both countries and he further pointed out that the Philippines and Malaysia have ASEAN-centrality embedded into their respective regional outlooks (Office of the Prime Minister of Malaysia, March 1, 2023).

The Malaysia MADANI policy framework and government slogan reflects a sustained economic performance by the Malaysian Government which is currently being implemented on a national level. Moreover, the strength of economic cooperation is guaranteed by high economic growth rates for the Philippines as envisioned in the AMBISYON 2040, an industry roadmap which guarantees a stable and comfortable lifestyle for all Filipinos through a clean, efficient, and fair government. The Philippine Government utilises its tools of fiscal, monetary and regulatory policies to steer the development path towards enabling Filipinos to attain their AmBisyon. This pertains to all dimensions of development: economic, human and physical capital, institutional, social and cultural (NEDA, 2022).

Similarly, the Philippines has supported the economic growth of the Bangsamoro Autonomous Region of Muslim Mindanao (BARMM) through a generous annual block grant. (Refer to Table 1 BARMM Block Grant). Block grants are inspired by concerted efforts to increase government efficiency and programme effectiveness as part of decentralisation and partial devolution of decision-making authority from the central government to local governments. In most cases, these block grants are used in lieu of full-blown social and economic entitlements. Additionally, block grants have these essential characteristics: A. Exhibit better flexibility for the recipient groups at the local level of government by empowering them to design the spending programme; B. They tend to be formula based and contain some degree of automaticity once certain conditions are met; C. Foster involvement and engagement of citizens', local communities' as well as the participation of the local government units; and, D. They tend to be directed to specific sectors such as education, health and other activities with measurable targets (Mendoza and Yusingco, 2019).

Furthermore, block grants fund a plethora of projects, spanning income generation (e.g. employment based capacity building training, value chain analysis, business loans, vocational-technical skills), water and sanitation (e.g. drinking water, latrines, school lavatories), education (e.g. audiovisual equipment, computers, learning facilities), agriculture (e.g. post-harvest equipment, cold storage, and slaughterhouses), health (e.g. hospitals, small clinics, health centres, etc.), transport (e.g. farm to market roads, public terminals, bridges.) (IDA, 2019). These grants are known to show better economic and health outcomes. There needs to be a thorough evaluation and assessment study on the effectivity and efficiency in order to determine if this block grants have yielded economic dividends for all BARMM residents and not just its political leaders. The mid-term elections in 2025 may reflect the entire gamut of the citizen's perceptions of an improvement in their economic and social well-being under the Bangsamoro Parliament.

Year	(in billions PHP)
2020	65.9
2021	75.6
2022	79.8
2023	85.4
2024	98.5

Table 1. BARMM Block Grant, 2020-2024

ECONOMIC COOPERATION

The Philippines and Malaysia strengthened economic relations through the establishment of the ASEAN Economic Community (AEC) in 2015. The AEC represents an economic integration whose goals are free movement of goods, services, investment, and skilled workers, and freer movement of capital. With the creation of the ASEAN Free Trade Area (AFTA), Malaysia and the Philippines continue to target economic integration by enhancing its supply chains and by actively promoting the Free Trade Agreements with countries outside the ASEAN region. The AFTA secured its chief goal of lessening tariffs to 0–5% in 2002, and ASEAN six (6) achieved tariff elimination by 2010. AFTA has achieved a high rate of trade liberalisation (the percentage of tariff lines subject to elimination) of 98.6% (Ishikawa, 2022).

Moreover, the Philippines has increased its annual national budget for the Brunei Darussalam–Indonesia–Malaysia–Philippines East ASEAN Growth Area (BIMP-EAGA) area. Moreover, the spatial approach that was implemented by the BIMP-EAGA member countries is founded on the premise that a joint, integrated strategy for the promotion of cross-border value chains through economic zones equips the subregional economies to attract investment and promote trade and economic activity while maintaining social and environmental standards. It offers opportunities to address the growth bottlenecks that cannot be addressed by the governments acting alone and adds value to Special Economic Zone (SEZ) interventions through cross-border cooperation (Aggarwal, 2022). Through sustained peace process, the Bangsamoro Autonomous Region in Muslim Mindanao (BARMM) was created under Republic Act 11054, otherwise known as the Bangsamoro Organic Law in March 2019. One key feature of this law is the creation of a BARMM block grant which was intended to help resource the new autonomous region. This financing is needed to mobilise the public finance management architecture which will serve as the governance system for BARMM's finances (Mendoza and Yusingco, 2019).

The MADANI Project of Malaysia is aimed at supporting the economic growth of the BIMP-EAGA areas. The concept focuses mainly on good governance, sustainable development and racial harmony in the country. For example, the Peninsular Malaysian provinces on the west coast specialise in highly skilled manufacturing and services.

COMMITMENT TO THE PEACE PROCESS

The excellent role of Malaysia in providing constant facilitation for peace negotiations between the Government of the Philippines and the Moro Islamic Liberation Front (MILF) began in 2001 with Malaysia acting as the facilitator. Through a systematic process, a cease-fire agreement was reached in 2003, and the International Monitoring Team (IMT), headed by Malaysia, commenced in 2004. The MILF started its rebellion for an independent Islamic state in the mineral-rich region of Mindanao in 1978 and more than 150,000 people have since been killed. The MILF helped the Philippine National Police forces rescue a Filipina businesswoman seized by a kidnap-for-ransom gang in May (Philippine Daily Inquirer, June 27, 2011). Through the passage of the BARMM Law, the Philippines has enjoyed relative peace in the BARMM areas from 2020-2024. Although the peace dividends had been slow in coming, the BARMM region has shown an uptick in foreign direct investment inflows compared to the period of intense armed conflict.

MARITIME SECURITY GOVERNANCE

The Philippines and Malaysia promote maritime security governance by participating in regional maritime security exercises. For example, both countries participated in the Southeast Asia Cooperation and Training (SEACAT), a multilateral exercise designed to strengthen cooperation among Southeast Asian countries and provide mutual support toward a common goal of addressing crises, contingencies, and illegal activities in the maritime domain with standardised tactics, techniques, and procedures. The SEACAT, which took place in Singapore from August 9 to 24, 2024, offered security presentations, live question and answer sessions, panel discussions with distinguished representatives from participating nations and academic, international and non -governmental organisations (INDOPACOM, August 27, 2024).

A series of maritime piracy attacks by the Abu Sayyaf Group (ASG) seriously impacted the maritime security of three countries: Indonesia, Malaysia, and the Philippines. The ASG started hijacking ships and demanding ransom for the hostages of the crew. The Trilateral Cooperation Agreement (TCA) was formed in order to address maritime security threats and challenges and implement the following: (1) A holistic, comprehensive and integrated approach at every level; (2) Continue to actively participate in various bilateral, regional and multilateral forums; (3) Sharing best practices, developing CBMs, capacity; and, (4) to address widespread maritime threats i.e., armed robbery at sea around Sulu-Celebes Sea. Rustam, et al., (2022) stated that the effectiveness of the TCA comes from these factors: (1) the TCA is not classified as benign, indicating no inconsistencies, asymmetries, and cumulative splits in the formation of the TCA; (2) the regime has a good problem-solving capacity because of epistemic community support that tightly integrated into the regime; (3) level of collaboration between the regime members is high, through a strong compliance to the standard operating procedure (SOP) of the Indomalphi’s patrols; (4) the regime facing a political context which provides an advantage with indicated by smooth cooperation.

The TCA was modeled after the Malacca Strait patrol. Specifically, the TCA consisted of coordinated maritime security, joint military command, consistent maritime as well as aviation patrols, the formation of technical working groups for timely frameworks, the identification of transit corridors for sea routes, a robust intelligence exchange, and the information-sharing component of several databases (Espena, 2020). Therefore, The Trilateral Cooperation Agreement (TCA) addressed numerous maritime security threats and challenges in the Sulu-Celebes Sea. In addition, the TCA covers traditional and non-traditional security and other significant threats to national security, marine resources, and safety of navigation.

The TCA was broached by Indonesia. Then, after a series of consultations between the Foreign and Defence Ministers of Indonesia, Malaysia and the Philippines, it was then established. The TCA reflected a regional commitment to ensure maritime security especially combating piracy and armed robbery. In addition, it helped maintain a good regional image, increased regular and coordinated joint patrols, creating national focal points, and establishing hotline communications. Further, it included the preparation of Standard Operating Procedures and the provision of a transit corridor to secure line of navigation by sea convoy.

Moreover, the Philippines and Malaysia maritime police forces had signed a formal agreement for stronger maritime security cooperation against transnational crimes, terrorism, and emerging nautical concerns in 2018. The agreement covered areas of operations, undertaking coordinated maritime activities in law enforcement, and prevention of kidnapping, vessel hijacking, terrorism, trafficking of persons, smuggling of migrants, illicit drug trafficking, arms smuggling, and other illegal and criminal acts. This agreement was signed during the 2nd Bilateral Meeting of the Marine Police Force-Royal Malaysia Police (MPF-RMP) and the Philippine National Police-Maritime Group. The maritime agreement included a cooperation in protecting marine resources from poaching and the protection of the marine environment. Joint successful operations against illegal logging and poaching of critically-endangered marine wildlife in the maritime territory are also covered areas. Coordination protocols to fight transnational crimes and to forge a stronger relationship with the Malaysian maritime police counterparts is essential (Philippine News Agency, July 4, 2018).

CONCLUSION

Malaysia and the Philippines are strategic economic and security partners in the Indo-Pacific Region. The warm bilateral relations were evident during President Ferdinand R. Marcos, Jr.'s state visit to Kuala Lumpur, Malaysia from July 25 to 27, 2023 which aimed to strengthen stronger partnerships in priority areas such as agriculture, food security, tourism, digital economy, and overseas Filipinos' welfare. The state visits highlighted new areas of cooperation on the *Halal* industry and Islamic banking.

There are currently a total of 900,000 Filipinos residing and working in Malaysia. President Marcos and his official delegation received a warm State Welcome Ceremony from His Majesty King Al-Sultan Abdullah and Queen Azizah Aminah Maimunah, Prime Minister Dato' Seri Anwar Ibrahim and his wife, Dato' Seri Dr. Wan Azizah Wan Ismail. The multisectoral engagements of both countries in the areas of economic cooperation, commitment to the peace process and maritime security governance reflects a mature and enduring diplomatic relationship. Finally, the common legacy and history between the two countries is very useful in maintaining the positive exchange of traditional arts and culture, and cultural exchanges between these two countries.

REFERENCES

Aradhna Aggarwal. (2022). Special Economic Zones for Shared Prosperity-Brunei Darussalam-Indonesia-Malaysia-Philippines East Asian Growth Area. Philippines: ADB Publications.

Espena, J. B. (8 September 2020). INDOMAPLHI: A Future for Southeast Asian Security?. Atlas Institute for International Affairs.https://www.internationalaffairshouse.org/indomalphi-a-future-for- southeast-asian-security.

International Development Association, World Bank Group (IDA). 2019. "ABCs of IDA-Community Approach to Development." Washington,D.C. [Available at: https:// ida.worldbank.org/results/abcs/taking-community-approach-development].

INDOPACOM. (August 27, 2024). "SEACAT 2024 Concludes, Reinforcing Maritime Security Efforts Among Allies and Partners in Southeast Asia." Available at URL: https:// www.pacom.mil/Media/News/News-Article-View/Article/3885535/seacat-2024-concludes-reinforcing-maritime-security-efforts-among-allies-and-pa/

Ishikawa, Koichi. (2021). "The ASEAN Economic Community and ASEAN economic integration" Journal of Contemporary East Asia Studies, Volume 10., Issue 1, pages 24-41.

Mendoza, Ronald U. and Yusingco, Michael Henry, Dissecting the BARMM Block Grant (June 25, 2019). ASOG Working Paper 19-011. Available at SSRN: https://ssrn.com/ abstract=3409824 or http://dx.doi.org/10.2139/ssrn.3409824.

Mindanews. (December 26, 2023). "BARMM's 2024 budget: nearly P100-B a year before transition gov't steps down in favor of elected.https://mindanews.com/peace-process/2023/12/barmms-2024-budget-nearly-p100-b-a-year-before-transition-govt-steps-down-in-favor-of-elected/.

National Economic Development Authority. (2022). AMBISYON 2040. Pasig, Philippines: NEDA Publications.

Office of the Prime Minister of Malaysia. (March 1, 2023). Malaysia, Philippines to Explore Further Cooperation in Various Sectors – PM Anwar.

Philippine Daily Inquirer. (June 27, 2024). "Government, MILF peace negotiators meet in Malaysia." Available at URL: https://globalnation.inquirer.net/4944/ph-milf-peace-negotiators-meet-in-malaysia#ixzz8kAn9RddV

Philippine News Agency. (July 4, 2018). “PH, Malaysia to sign maritime security pact vs. transnational crimes.”

Rustam, I., Bustami, S. Y., & Sabilla, K. R. (2022). The Effectiveness of Indomalphi Trilateral Cooperation in Reducing Maritime Piracy by Abu Sayyaf Group in the Sulu-Sulawesi Sea. Papua Journal of Diplomacy and International Relations, 2(2), 163-183.https://nbn-resolving.org/urn:nbn:de:0168-ssoar-80705-3

CHALLENGES OF DEFINING EMERGING SECURITY THREATS FROM MALICIOUS USE OF ARTIFICIAL INTELLIGENCE

Muhammad Afiq bin Ismaizam

ABSTRACT

Artificial Intelligence (AI) has emerged as a transformative force across various industries, offering unprecedented potential for automation, data-driven decision-making, and personalised user experiences. Its applications span from finance to healthcare, revolutionising operational efficiency and fostering innovation. However, alongside its promises, AI introduces a new set of security challenges. One of the many concerns is the misuse of AI by terrorist groups or malicious actors that present significant security threats mainly through the manipulation of AI to disseminate disinformation and extremist propaganda, interactive recruitment, and cyberattacks. As AI technology becomes more advanced and widespread in this space, so does its technical jargon and terminologies. It is a challenge to not only define new and emerging threats that come from AI, but to also understand the impact of such threats. While the lexicon of AI technology is well understood among industry players and AI enthusiasts, government ministries and law enforcement agencies need to be constantly updated with the latest trends and terminologies. More importantly, public understanding of AI threats such as deepfakes and audiofakes varies widely. Definitions need to be clear and accessible to both security experts and the general public to ensure effective communication and awareness.

Keywords: Artificial intelligence, threats, security, awareness, education

INTRODUCTION

Artificial Intelligence (AI) has traversed a remarkable journey from its conceptual roots to becoming an integral part of modern technology. This journey is marked by significant milestones, periods of intense progress and stagnation, and the development of complex terminologies that reflect the interdisciplinary nature of the field.

This paper highlights specific terminologies that stem from security challenges brought forth by AI technology. Furthermore, it will also aim to showcase the importance of bridging the knowledge gap between experts in the field of AI technology and the general public. Given that AI technology continues to evolve at a rapid pace, the significance of understanding the associated terminologies and jargon cannot be understated. AI terms like Machine Learning, Generative Adversarial Network (GAN), and Large Language Model (LLMs) have been added to the vocabulary of everyday conversations, both in personal and professional settings. With regular usage of these AI terminology, one tends to overlook the actual definitions of these AI terms.

According to the International Organisation for Standardisation (ISO), AI is defined as “a machine or computer system’s ability to perform tasks that would typically require human intelligence. It involves programmeming systems to analyse data, learn from experiences, and make smart decisions – guided by human input”. The most familiar form of AI is virtual assistants like Siri or Alexa, but there are many iterations of the technology. This definition serves as a base for all AI iterations and applications moving forward.

The word term ‘artificial intelligence’ was officially coined in 1956 Marvin Minsky and John McCarthy (a computer scientist at Stanford) hosted the approximately eight-week-long Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) at Dartmouth College in New Hampshire (Haenlein and Kaplan, 3). It was during this conference that the term "artificial intelligence" was coined, marking the formal recognition of AI as a distinct field of research. This period saw the development of symbolic AI, which sought to replicate human thought processes using symbols and rules. The 1950s and 1960s were characterized by optimism and ambitious goals for AI.

The 1980s saw a resurgence of interest in AI with the rise of expert systems. These systems used rule-based approaches to mimic expert decision-making in specific domains. The success of expert systems in industrial applications revived interest and investment in AI. The late 1980s and 1990s witnessed the emergence of ‘machine learning’, a paradigm shift in AI research. Machine learning focused on developing algorithms that enable computers to learn from data. This shift laid the foundation for many of the AI technologies seen today. The 21st century has seen unprecedented advancements in AI, driven by breakthroughs in deep learning, the availability of big data, and increased computing power. ‘Deep Learning’, a subset of ‘machine learning’, utilises neural networks with many layers to model complex patterns in data. This has led to significant breakthroughs in areas such as image and speech recognition.

AI today has become ubiquitous in everyday life, from virtual assistants like Siri and Alexa to recommendation systems on platforms like Netflix and Amazon. The modern era of AI is characterized by its application across various industries, including healthcare, finance, and autonomous vehicles.

TERMINOLOGIES OF AI-DRIVEN THREATS

Before IS, based on specific literature review, there are several terminologies that are not intuitively known to the general public. This creates a knowledge gap, which can potentially be harmful in the long term. Some of these terminologies may not necessarily be part of a terrorist group’s operations. Definitions of these terminologies can be found in website homepages, blogs, and online news outlets. Such terminologies include:

- **“Deepfakes”** – AI-generated synthetic media, such as videos or audio recordings, that mimic real people. These can be used for misinformation, identity theft, and other malicious purposes. Deepfakes represent a significant AI risk, exemplifying the potential dangers of synthetic media manipulation. Leveraging artificial intelligence and machine learning algorithms, deepfakes can produce remarkably convincing videos, images, audio, and text depicting events that never occurred. While some applications of synthetic media are benign, the proliferation of deepfakes poses a grave threat due to people's inherent trust in visual information (Kundu, 2024);

- **“AI-Driven Phishing”** – The use of AI to create highly convincing and personalized phishing emails or messages, increasing the likelihood of deceiving targets;

- **“Autonomous Weapons”** – AI-controlled weapons systems that can select and engage targets without human intervention, posing risks of unintended escalation or misuse;

- **“Weaponized AI Bots”** – AI-driven bots that spread misinformation, manipulate social media discourse, or automate large-scale attacks on digital platforms;

- **“Prompt Injection”**: Prompt injection is a technique that involves inserting biased, malicious, or misleading prompts into LLMs to manipulate their outputs or behaviour. It can lead to the propagation of misinformation, reinforcement of biases, or even the generation of harmful content;

- **“Ransomware Powered by AI”** – AI can be used to enhance ransomware attacks by automating tasks such as selecting targets, crafting personalized ransom notes, and optimizing encryption processes;

- **“AI in Autonomous Vehicles”** – The use of AI in autonomous vehicles poses risks if these systems are hacked or manipulated, potentially leading to accidents or disruptions in transportation networks;

- **“AI-Enabled Cyber Espionage”** – AI can enhance espionage efforts by automating the collection and analysis of large volumes of data, leading to the theft of intellectual property or sensitive information;

- **“AI-Enhanced Disinformation Campaigns**” – AI can be used to generate and disseminate false information rapidly, affecting public opinion, political processes, or social stability;

- "**Weapons Automatisation**": The integration of AI into weapons systems, leading to the development of Lethal Autonomous Weapon Systems (LAWS), poses a grave risk to global security. LAWS operate with minimal human oversight, raising concerns about unchecked proliferation and the potential for catastrophic consequences, including civilian casualties and escalated conflicts. With political tensions driving technological rivalries, urgent action is needed to address the ethical implications and prevent the onset of a dangerous global arms race (Kundu, 2024).

- "**Hallucination**": LLMs that generate false information that appear plausible because LLMs are designed to produce fluent, coherent texts despite not having any understanding of the underlying reality that language describes (Lutkevich, 2023). LLMs use statistics to generate language that is grammatically and semantically correct within the context of the prompt; and

- "**ELIZA Effect**": In 1966, computer scientists at MIT noticed that most people interacting with their AI chatbot ELIZA spoke about it as though it were sentient. The 'ELIZA Effect, 'as it came to be known, is the tendency to ascribe human traits – e.g. empathy, motive, experience – to computer programme (European Centre for Counterterrorism and Intelligence, 2024).

RESEARCH STUDY: MISUSE OF AI BY TERRORIST GROUPS

In a separate research study, there has already been instances in which AI has been used by certain terrorist groups. Apart from SEARCCT, other prominent research institutions that are conducting similar research include Royal United Services Institute (RUSI), Global Network on Extremism and Technology (GNET), and the International Centre for Counter-Terrorism (ICT). The content for this section was part of an article that has been published in The Edge on 22 May 2024.

AI's duality presents both opportunities and dangers because AI is a tool that is directly dependent on the user. It has many known benefits and, at the same time, can inflict significant damage. This would be of particular interest for terrorist organisations, for example, as AI presents a new frontier of opportunities for them to enhance their terrorist activities. This raises the question: what are the potential ways in which AI can be misused by malicious actors?

While research on the misuse of AI is generally predictive and largely hypothetical, preliminary assessments indicate that there are three general ways in which terrorist organisations have misused AI: dissemination of propaganda, cyberattacks and deepfakes.

Deepfakes are in abundance nowadays and some videos are getting more realistic. During the outbreak of the Ukraine-Russia war, an infamous deepfake video was released supposedly depicting President Volodymyr Zelenskyy announcing a surrender to Russia (Burgess, 2022). This was immediately dismissed as fake due to the inconsistencies in the skin colouration and awkward head movements. Some may consider this entertainment but making a deepfake video of the president of a sovereign nation during wartime can potentially be harmful. Last February, a deepfake audio of London Mayor Sadiq Khan emerged supposedly making distasteful remarks regarding Armistice Day (Bristow, 2024). A BBC report stated that the recording originated from a TikTok account that has been sharing racist content.

Dissemination of propaganda is one of the easiest ways to misuse AI through the use of free AI tools such as ChatGPT alongside AI image generators to produce visually appealing content. This can already be seen with right-wing extremists, particularly Neo-Nazis. Tech Against Terrorism, a UK-based think tank, reportedly found propaganda posters supposedly created with AI by a media entity that is aligned with al-Qaeda.

Though AI platforms in and of themselves cannot be used to conduct a cyberattack, they are a functional prelude to the actual delivery of the attack. For example, ChatGPT has built-in policy safeguards that would disallow any answer that comes from a sensitive or ethically concerning prompt. However, it can be side-stepped through prompt modifications, such as rewording certain words or phrases, to generate convincing phishing emails or business email compromise (BEC) attacks. This can be done by anyone without any particular skill level. A recent report from the UK's National Cyber Security Center (NCSC) confirms that AI will "almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years." (Sangfor Technologies, 2024). The same report also states that AI has opened up the field of hacking to opportunistic cyber criminals who might not have the skills to orchestrate a cyber-attack alone. This means that AI is making hacking more accessible and easier to use – encouraging hackers to turn to AI technology to do or supplement their hacking.

There is an interesting case study of "Muhammad Qasim", supposedly an individual from Pakistan who employs AI tools to personify himself as the long awaited sole legitimate Islamic leader while denouncing predominantly Muslim nations such as Saudi Arabia and Turkey as 'apostates' (Siegel and Chandra, 2023). He utilises image generation tools and audio deepfakes to spread propaganda and disinformation among his followers online. He plays on the narrative of "us versus them", categorising people as either "true believers" or "idolaters". AI-generated images are used to glorify "Muhammad Qasim", depicting him as a hero to evoke emotional engagement, which can motivate users to share the content within their networks. This is just one example. Are there any similar instances? Not now, but possibly in the foreseeable future.

In light of the escalating threats posed by AI, there has been a concerted effort to implement regulations aimed at mitigating potential risks. Taking the lead in this endeavour is the European Union (EU), which has adopted a proactive and thorough approach. At the heart of this initiative lies the EU's AI Act, which was passed in June 2023 and is set to be finalised before the European Parliament elections in June 2024. This legislation proposes categorising AI systems based on risk levels and imposing corresponding regulations. Meanwhile, in the US, the White House has issued an executive order focused on ensuring the safety, security and reliability of AI, along with a blueprint outlining principles for an AI Bill of Rights.

In Malaysia, we are still awaiting the national strategic document known as the National Action Plan on Preventing and Countering Violent Extremism 2022–2025 from the government. It is under the direct purview of the Ministry of Home Affairs. It is hoped that the strategy document will at least acknowledge that AI technology can be misused in the hands of terrorists. After all, just because it is difficult to pinpoint, it does not mean that law enforcement officials should not be vigilant and proactive.

It is only a matter of time until we see AI being exploited by terrorist groups that actually threaten the global security order. As AI systems become increasingly autonomous and sophisticated, there arises the unsettling prospect of rogue AIs—artificial entities that act against human interests. Rogue AIs can cause strategic deception—that is, an attempt to systematically cause a false belief in another entity in order to accomplish some outcome or misalignment – a problem that arises when the goals of an AI model mismatch those intended or endorsed by its designers.

CHALLENGES OF DEFINING AI THREATS

The rapid advancement of AI presents a unique challenge in defining and managing emerging security threats. As AI technology evolves, it becomes increasingly difficult to anticipate and address the new risks that may arise. Each technological breakthrough introduces the potential for new vulnerabilities or misuse, making the task of threat assessment both dynamic and complex. The dynamic nature of AI threats further complicates the task of defining and managing them. Malicious actors are constantly adapting their strategies and tools in response to defensive measures, creating an ongoing cycle of threat evolution. This adaptability means that definitions and countermeasures must be continuously updated to stay ahead of emerging risks, adding to the already complex challenge of managing AI security threats.

Another significant obstacle is the lack of standardisation in the assessment of AI security threats. Currently, there is no universal framework that governments and organisations can rely on to evaluate and define these threats. As a result, different entities may adopt varying definitions and criteria, leading to inconsistencies in threat modelling and response strategies.

The absence of standardised approaches hinders the development of a cohesive and effective global response to AI-related security risks.

Public perception and communication present additional hurdles. There is often a significant gap between technical understanding and public awareness of AI threats. Misunderstandings, sensationalism, or misinformation can distort public perception, skewing the definition of threats and hindering effective communication and policy-making. Bridging this gap is essential to ensure that the public is accurately informed and that policy responses are grounded in a realistic understanding of the risks.

PROPOSED RECOMMENDATION

The process of understanding and simplifying AI threats requires a multi-party approach, involving private and public sector collaborations. Coordinating efforts across these sectors is beneficial, as each party brings its own perspectives and insights.

Public awareness and education are vital components of a comprehensive AI security strategy. Governments and organisations should implement awareness campaigns and educational programmes to inform the public, businesses, and policymakers about AI security threats. By increasing understanding of AI-related risks, these initiatives can help individuals and organisations take proactive measures to protect themselves. Additionally, educational programmes should focus on training the next generation of AI professionals with a strong emphasis on security and ethical considerations.

Secondly, it is timely now to introduce AI literacy programmes into Malaysia's primary and secondary school curricula. By teaching students about AI terminologies and security threats from a young age, the base knowledge will grow as technology evolves. Educational materials should be age-appropriate and engaging, using relatable examples and hands-on activities to illustrate key concepts.

Since AI and its threats are global, international collaboration in public education is essential. Governments and international organisations can share best practices, educational materials, and strategies for raising AI awareness. Collaborative efforts can lead to the development of standardised educational frameworks that benefit a global audience. By implementing these strategies, society can foster a more informed and proactive public that is equipped to understand and mitigate the security threats associated with AI. Educating the public not only enhances individual awareness but also strengthens collective resilience against the challenges posed by rapidly advancing AI technologies.

Since AI and its threats are global, international collaboration in public education is essential. Governments and international organisations can share best practices, educational materials, and strategies for raising AI awareness. Collaborative efforts can lead to the development of standardised educational frameworks that benefit a global audience. By implementing these strategies, society can foster a more informed and proactive public that is equipped to understand and mitigate the security threats associated with AI. Educating the public not only enhances individual awareness but also strengthens collective resilience against the challenges posed by rapidly advancing AI technologies.

Similarly, under the education and awareness fold, influencers, public figures, and content creators can be appointed as ambassadors. These individuals can help disseminate information about AI terminologies and security threats in a relatable and engaging way. By leveraging their reach, it is possible to connect with audiences that might not engage with traditional educational content.

REFERENCES

Burgess, Sanya. “Ukraine War: Deepfake video of Zelenskyy telling Ukrainians to ‘lay down arms’ debunked”, *Sky News*, March 2022, https://news.sky.com/story/ukraine-war-deepfake-video-of-zelenskyy-telling-ukrainians-to-lay-down-arms-debunked-12567789

Bristow, Tom. “London’s Sadiq Khan shaken by pro-Palestine deepfake”, *POLITICO*, February 2024, https://www.politico.eu/article/mayor-of-london-sadiq-khan-shaken-by-pro-palestine-deepfake/

Copeland, Simon**.** “Terrorist exploitation of artificial intelligence: current risks and future applications”, *Royal United Services Institute*, 2024

“Counter terrorism -“AI” Enabled Radicalization through the ELIZA Effect”, *European Centre for Counterterrorism and Intelligence Studies,* May 2024, https://en.europarabct.com/?p=80581

Haenlein, Michael and Kaplan, Andreas. “A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence”, *California Management Review*, July 2019

Kundu, Rohit. “AI Risks: Exploring the Critical Challenges of Artificial Intelligence”, *LAKERA*, March 2024

Sangfor Technologies, “Defining AI Hacking: The Rise of AI Cyber Attacks”, Sangfor Cybersecurity Blog, June 2024, https://www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks

Siegel, Daniel and Chandra, Bilva. ‘Deepfake Doomsday’: The Role of Artificial Intelligence in Amplifying Apocalyptic Islamist Propaganda, *Global Network on Extremism and Technology*, August 2023, https://gnet-research.org/2023/08/29/deepfake-doomsday-the-role-of-artificial-intelligence-in-amplifying-apocalyptic-islamist-propaganda/

Lutkevich, Ben. “AI hallucination”, *TechTarget*, June 2023, https://www.techtarget.com/whatis/definition/AI-hallucination

EMERGING THREATS AND TRENDS OF TERRORISM AND VIOLENT EXTREMISM ONLINE

Natechanok Sulaimarl and Niki Esse De Lang

ABSTRACT

Terrorists and violent extremists are increasingly exploiting the evolving landscape of the internet, using emerging technologies to enhance their efforts in radicalisation, recruitment, fundraising, and advancing their military skills. Groups and individuals linked with terrorism and violent extremism have long been known to utilise the Internet and social media to plan, recruit, train, exchange information, fundraise, acquire arms, transfer funds, and disseminate propaganda. Online forums often act as breeding grounds for violent extremist rhetoric, terrorist propaganda and campaigns, and increasingly facilitated by algorithms that can prioritise such content and potentially accelerate the process of radicalisation.

Keywords: Radicalisation, recruitment, fundraising, violent extremist rhetoric, terrorist propaganda

BACKGROUND

The brutal 22-minute video broadcast the world witnessed back in 2015 was when a Jordanian military pilot was caged engulfed with flames by the Islamic State (IS). The video was posted by the group using a Twitter account (now known as X) as a source for IS propaganda. The incident was evidence of how much IS could afford perpetrating information warfare,[1] by leveraging online platforms to sow fear and terror among populations as well as the proliferation of online manifestos that have the potential to inspire future attacks.

Terrorists and lone actors have long adapted to new advancements in Internet and social media technologies, particularly by live streaming their attacks to maximise their impact. An instance of this occurred during the 2019 mosque attack in Christchurch, New Zealand, followed by a similar incident during the 2022 attack at the Buffalo Mall in the United States.[2]

A terrorist group such as al-Qaeda (AQ) has also capitalised on the internet in instigating militant

---

[1] Jordan pilot hostage Moaz al-Kasasbeh 'burned alive'. (2015). *BBC News*. https://www.bbc.com/news/world-middle-east-31121160.

[2] United Nations Office of Counter-Terrorism (UNCCT) and the United Nations Interregional Crime and Justice Research Institute (UNICRI). (2024). Beneath The Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks. Retrieved from https://unicri.it/sites/default/files/2024-07/DW_BtS.pdf.

jihadism. Prominent al-Qaeda figures, such as the late infamous preacher Anwar al-Awlaki, encouraged followers to harness the inherent power of the Internet by becoming "*Internet Mujahideen*." He urged them to create dedicated websites focusing on specific aspects of jihad, like news on jihadist activities, operations, and jihadist literature, which he referred to as "*WWW Jihad*." Jihadist websites have become key tools in promoting militant Islam, recruiting potential followers, and encouraging terrorist activities.[3]

In July 2014, Abu Bakr al-Baghdadi declared the Islamic Caliphate in Iraq and Syria through Al Qaeda's Iraqi branch. This declaration was backed by a powerful media campaign and significant battlefield victories in Syria and Iraq. The combination of military success and strategic media manipulation amplified the Caliphate's influence on recruitment, financing, intimidation, and psychological warfare. The use of these platforms allowed the Caliphate to reach a wide target audience, while exploiting the ultimate freedom provided by the Internet. During the rise of ISIS, *electronic jihad* is divided into two main efforts. The first is the operational effort, where discussion boards are used to recruit and support violent extremist jihad, promote the idea among the public, defend the “honour” of mujahideen, share articles which misconstrue the true meaning of jihad, and disseminate training materials and tutorials on bomb-making, attack methods, use of weapons, including 3D printing and the use of drones. The second is the defensive-offensive effort, which involves hacking to attack websites and other cyber-attacks on information and communication technology (ICT) platforms to disrupt critical information infrastructures and leak sensitive information about government officials or members of the public.[4]

The territorial losses of the Islamic State in Iraq and Syria (ISIS) in 2017 may incapacitate the operational grounds and physical presence of ISIS, yet it increased the group’s online presence resulting in increased lone-actor radicalisation and recruitment. A recent plot by jihadists inspired by the Islamic State to attack in August 2024, during Taylor Swift concert in Vienna, Austria, highlighted the growing issue of online radicalisation among the perpetrators. Following Hamas' October 7 attacks and Israel's military response in Gaza, Europe has seen a surge in terror-related arrests, with nearly two-thirds of those arrested between October 2023 and June 2024 being teenagers. Social media, encrypted messaging, and video platforms are crucial tools for jihadi recruitment and planning, particularly targeting youth. Additionally, ISIS has begun using generative AI for creating and spreading extremist content, enhancing their tactics and modus

---

[3] Martine Rudner., (2017). “Electronic Jihad”: The Internet as Al Qaeda’s Catalyst for Global Terror. *Routledge Taylor & Francis Group*, VOL.40, NO. 1, 10-23. http://dx.doi.org/10.1080/1057610X.2016.1157403

[4] Shashi Jayakumar.,(n.d.) “Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness.” *International Centre for Counterterrorism (ICCT)*. Retrieved from https://www.icct.nl/sites/default/files/2023-01/Chapter-29-Handbook-.pdf.

operandi.[5] The use of these technologies has been prevalent among Al-Qaeda, ISIL/Daesh, and their affiliates with the aim to expand their propaganda and increase their influence worldwide.[6]

THE USE OF THE INTERNET BY TERRORIST GROUPS OR LONE ACTORS

Use of artificial intelligence

Terrorist groups are increasingly adopting generative AI to enhance and spread their propaganda, making it more efficient and tailored to specific audiences. This includes creating synthetic images, videos, or audio to intensify their messages and influence emotions. Generative AI enables the creation of false realities, leading to widespread misinformation and disinformation, especially on social media platforms. Recent examples include the use of AI-generated images to incite violence and spread disinformation, such as manipulated photos of injured individuals and fabricated content aimed at undermining the facts.[7] Additionally, terrorist organisations have started sharing guidelines on how to use AI for propaganda, with groups like ISIS and al-Qaeda using AI to create and disseminate extremist content, such as a technical support guide on how to use AI-generated image tools to create extremist memes and how to translate Arabic-language ISIS propaganda, speeches/messages into Arabic script, Indonesian, and English. In addition to propaganda, experts suggest that terrorists could utilise chatbots powered by large language models (LLMs)[8], such as ChatGPT, to engage with potential new recruits. Once the chatbot sparks interest, a human recruiter might then step in to continue the conversation.[9]

Dark Web and Encrypted Platforms

The dark web plays a central role in the cybercrime ecosystem, where various illicit services are exchanged. Malicious actors are increasingly using encrypted communication platforms to coordinate, trade illegal assets, and acquire criminal services, forming what could be described as a cybercrime underground[10].

---

[5] Tiktok Jihad: Terrorists Leverage Modern Tools to Recruit and Radicalize. The Soufan Center IntelBrief, August 9, 2024. Retrieved from https://mailchi.mp/thesoufancenter/tiktok-jihad-terrorists-leverage-modern-tools-to-recruit-and-radicalize?e=d06575ff66.

[6] Clarisa Nelu., (2024). Exploitation of Generative AI by Terrorist Groups. *The International Centre for Counterterrorism (ICCT)*. Retrieved from https://www.icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[7] Meili Criezis., (2024). "AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI." *Global Network on Extremism and Technology*. Retrieved from https://gnet-research.org/2024/02/05/ai-caliphate-pro-islamic-state-propaganda-and-generative-ai/.

[8] Weimann, G., Pack, A. T., Sulciner, R., Scheinin, J., Rapaport, G., & Diaz, D. (2024). Generating terror: The risks of generative AI exploitation. *Combating Terrorism Center*, VOL 17, (1).

[9] Cathrin, S. (2024, July 10). How extremist groups like 'Islamic State' are using AI. *Deutsche Welle*. https://www.dw.com/en/how-extremist-groups-like-islamic-state-are-using-ai/a-69609398.

[10] United Nations Office of Counter-Terrorism (UNCCT) and the United Nations Interregional Crime and Justice Research Institute (UNICRI). (2024). Beneath The Surface: Terrorist and Violent Extremist Use of the Dark Web and Cyber-

The Internet can be thought of as having different layers. The "upper" layer, known as the Surface Web, is easily accessible through standard search engines or by entering a known website address. Whilst the deeper layers, referred to as the Deep Web, contain content that is not indexed by typical search engines like Google. The innermost part of the Deep Web, called the "Dark Web", consists of content that has been deliberately hidden. A recent study revealed that 57% of the Dark Web is dedicated to illegal activities, including pornography, illicit financial dealings, drug marketplaces, weapons trafficking, counterfeit currency, terrorist communications, and other unlawful content.[11] Following the November 2015 attacks in Paris, ISIS's media outlet, Al-Hayat Media Center, shared a link and instructions for accessing their new Dark Web site on an ISIS-associated forum. The announcement was also circulated via Telegram, the encrypted messaging app used by the group.[12] *Isdarat* website was once used by ISIS as archives for propaganda and releases. After the Paris attack, however, the platform was constrained by hacktivists. ISIS later moved to a new platform and launched the website on Dark Web, an outlet of *Isdarat*.[13]

Although there is limited data on criminal activity related to the Dark Web that targets or originates from Southeast Asia, according to the UNODC's report on threats to Southeast Asia from darknet induced cybercrime, the available information indicates that it does exist and is likely to expand in scope and scale in the near future.[14] While these data may not clearly infer the number of terrorist-linked activities on the darknet, it has been observed that affiliates of both ISIS and al-Qaeda conduct terrorist-associated activities there, which are elaborated in the below.

Terrorist-associated activities on Dark Web

Terrorist organisations exploit the Dark Web as a secure platform for various activities that support their operations. It serves as a channel for **internal communication**, enabling covert information exchange essential for planning, organizing, deploying, and executing terrorist activities. Beyond communication, the dark web also acts as a tool for external propagation, allowing terrorists to spread extremist ideologies more broadly. Recruitment and training are key activities conducted on the dark web. Terrorist groups use this platform to **recruit new members** and **provide training** to followers around the world, offering courses on bomb-making and the execution of terrorist attacks. The anonymity provided by the dark web makes it challenging for counterterrorism agencies to detect and prevent radicalisation, especially among lone-wolf attackers.

---

[11] Weimann, G. (2016). Terrorist Migration to the Dark Web. *Perspectives on Terrorism*, 10(3), 40–44. http://www.jstor.org/stable/26297596

[12] Ibid, xi.

[13] Ibid, xi.

14 United Nations Office on Drugs and Crime (UNODC). (2020).Darknet Cybercrime Threats to Southeast Asia. Retrieved from https://www.unodc.org/roseap/uploads/documents/ Publications/2021 Darknet_ Cybercrime_ Threats _to_Southeast_Asia_report.pdf.

Fundraising and financial transactions are increasingly conducted on the dark web through digital cryptocurrencies like Bitcoin and Monero. These platforms allow terrorist organisations to raise funds via Bitcoin donations, online extortion, and even human and organ trafficking. For instance, Islamic State Khorasan Province (ISK-P) solicited donations in cryptocurrencies through the dark web.

The procurement of weapons is another significant use of the dark web by terrorist groups. Platforms like Silk Road and EuroGuns facilitate the illegal trade of firearms and ammunition. Additionally, terrorists can acquire dual-use elements such as chemicals and biological medicines, which can be used to create chemical and **biological weapons**. The dark web also provides access to manuals on bomb-making, fake documents, passports, and even nuclear materials like uranium and plutonium.

Lastly, terrorists are increasingly using AI tools in conjunction with the dark web to enhance their operations. AI technologies enable the creation of deepfakes, which can be used to **disseminate propaganda** more effectively. Moreover, AI programmes like Google Gemini and ChatGPT facilitate access to bomb-making manuals, while other programmes like 'Lavender' and 'Where is Daddy?' contribute to more sophisticated warfare methods. The integration of AI with dark web activities presents a growing challenge in the fight against terrorism.[15]

Social Messaging and Encrypted Applications

"*I shot people. For money. They delivered the arms to us themselves. They were people who wrote to me on Telegram. I don't know why they wrote to me. I was listening to a lesson. To a preacher*." [16]

This was the statement of one of the arrested suspects, Faridun Shamsiddin, during an interrogation following the March 2024 Crocus City Hall attack in Moscow, Russia. The Moscow attackers were reportedly recruited and directed through the online messaging app Telegram. One of the attackers admitted that an online preacher contacted him via Telegram, offering payment in exchange for carrying out the attack. This case, like others involving IS-K and the Islamic State (and their affiliates), underscores the growing role of virtual planning in modern terrorism, involving recruitment and guidance through online messaging apps.[17] Virtual planning involves one or more planners offering guidance to operatives in target countries through virtual

---

[15] Soumya Awasti. (2024). The Dark Web as Enabler of Terrorist Activities. *Observer Research Foundation*, Issue No.717. https://www.orfonline.org/public/uploads/posts/pdf/20240701105925.pdf.

[16] Den Braber, B., & Faizi, N. (2024, July 1). Islamic State Crocus City Hall attack: Analyzing the background and online responses. *Centre for Information Resilience*. Retrieved from https://www.info-res.org/post/islamic-state-crocus-city-hall-attack-analysing-the-background-and-online-responses.

[17] Rueben Dass. (2024). Islamic State-Khorasan Province's Virtual Planning. *Lawfare*. Retrieved from https://www.lawfaremedia.org/article/islamic-state-khorasan-province-s-virtual-planning.

channels to execute attacks. This guidance can vary in the areas of target selection, attack methods, and providing ideological or logistical support.[18]

Recent reports indicate that jihadists inspired by ISIS were plotting a terrorist attack on a 2024 Taylor Swift concert in Vienna, Austria. It has been revealed that some of those involved were radicalised online. Despite unclear evidence whether this radicalisation took place on TikTok or another platform, it is evident that ISIS and its global affiliates continue to radicalise, recruit, and encourage attacks in the West through online messaging and social media platforms, including 4chan, 8chan, Gab, and Telegram, among many others.[19] [20]

Gaming and Radicalisation

A report by the UN Counter-Terrorism Centre (UNCCT) on the link between gaming and violent extremism reveals that extremists have developed simulations in games such as The Sims and Minecraft, enabling players to experience the Christchurch massacre from the shooter's view-point.[21]

Revealed by the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) through the use of *horizon scanning*, the in-game communication features, can serve not only as a covert platform for disseminating extremist ideologies but also as a venue to reach young people in Southeast Asia for recruitment into terrorist groups or militant organisations.[22] This phenomenon is reflected in the report by Singapore's Internal Security Department (ISD) revealing that a 15-year-old, who wanted to behead those he deemed "disbelievers" and become a suicide bomber, was arrested under the ISA in December 2023. In January 2023, a 16-year-old who used footage from the online gaming platform Roblox to create ISIS propaganda videos was also issued a restriction order. Both individuals were in contact with 18-year-old Muhammad Irfan Danyal Mohamad Nor via an extremist channel on the messaging platform called Discord.[23]

---

[18] Ibid, xvii.

[19] TikTok Jihad: Terrorists Leverage Modern Tools to Recruit and Radicalize. (2024). *The Soufan Center Intel Brief*. Retrieved from https://mailchi.mp/thesoufancenter/tiktok-jihad-terrorists-leverage-modern-tools-to-recruit-and-radicalize?e=d06575ff66.

[20] IntelBrief: The Evolution of the Online Violent Extremist Landscape. (2022). *The Soufan Center*. Retrieved from https://thesoufancenter.org/intelbrief-2022-october-20/.

[21] United Nations Counter-Terrorism Centre (UNCCT).(2022).Examining the Intersection between Gaming and Violent Extremism. Retrieved from https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf.

[22] Mohamed Farid Noh. (2024). Terrorist groups using online video games to recruit young members. *New Straits Times*. https://www.nst.com.my/news/crime-courts/2024/05/1055185/terrorist-groups-using-online-video-games-%C2%A0recruit%C2%A0young-members.

[23] Jean Iau. (2023). 2 teens dealt with under ISA: How terrorist groups target youth online through games, chats. *The Straits Times*. https://www.straitstimes.com/singapore/2-teens-dealt-with-under-isa-how-terrorist-groups-target-youth-online-through-games-chats.

Additionally, the report by the UN Counter-Terrorism Centre (UNCCT) revealed that the propaganda videos distributed by terrorist groups were framed by mirroring the violence and visual styles presented in games like the FPS games.[24] This is a strategic choice of jihadist recruiters as many of the users of FPS are young men aged between 16 and 34, who are readily vulnerable to endorse violent ideology or violent jihadism as an attempt to identify themselves with specific type of masculine identity.[25]

Gaming and terrorist financing

Additionally, concerns have been raised about the potential for online gaming to facilitate money laundering and terrorist financing. The ability to exchange virtual currencies within games and, in some cases, convert them into real money outside the game could enable such activities to occur rapidly, discreetly, and with relative ease. The use of numerous small transactions could also support "low-cost" terrorism financing.[26]

Roblox, World of Warcraft, Fortnite, and many others are among the examples susceptible to money laundering for terrorism-linked purposes. The in-game digital currencies, such as 'loot boxes', 'skins', or other virtual items, allow users to trade, buy, or sell in-game items to other clandestine forums of the internet. Such a process is facilitated by the ease of the in-game currencies which can be converted easily into cryptocurrencies, with no traces of identity of the users. In some instances, the transactions can be done for real money outside the video game.[27] Hence, gaming virtual currencies are appealing for money laundering and terrorist financing because they allow funds to be transferred across borders rapidly, effortlessly, and with minimal visibility. The use of numerous microtransactions can help obscure these financial flows. This environment is especially conducive to funding "low-cost" terrorism.[28]

CONCLUSION AND RECOMMENDATION

The internet has significantly transformed the landscape of terrorism, providing extremist groups with unprecedented tools for communication, recruitment, and propaganda dissemination. The anonymity and global reach of online platforms enable these groups to operate with relative impunity, spreading their ideologies and coordinating activities across borders. The ease with

---

[24] A first person shooter (FPS) is a genre of action video game that is played from the point of view of the protagonist.

[25] United Nations Counter-Terrorism Centre (UNCCT).(2022).Examining the Intersection between Gaming and Violent Extremism. Retrieved from https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf.

[26] Suraj Lakhani, CIVIPOL. (2021). Video Gaming and (Violent) Extremism. *Radicalisation Awareness Network (RAN) Policy Support*. Retrieved from https://home-affairs.ec.europa.eu/document/download/67db2a03-5b45-44f2-b0e9-3b0544a08dfc_en?filename=EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf.

[27] Moshe Klein. (2024). Video Games Might Matter for Terrorist Financing. *Lawfare Media*. Retrieved from https://www.lawfaremedia.org/article/video-games-might-matter-for-terrorist-financing.

[28] Online Gaming in the context of the fighting against terrorism. (2020). *Council of the European Union*. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf.

which information and resources can be shared online also facilitates the financing of terrorism through various digital means, including crowdfunding, cryptocurrency, and other online financial systems. As a result, the internet has become an essential component in the operational strategies of modern terrorist organisations, posing complex challenges for governments, law enforcement, and international organisations.

To effectively combat the use of the internet for terrorist purposes, a multifaceted approach is required. Governments and international bodies must enhance collaboration to develop and enforce robust cyber laws and regulations that target terrorist activities online. Law enforcement agencies should be equipped with advanced technological tools and trained personnel to monitor and disrupt terrorist networks in the digital space. Furthermore, partnerships with technology companies and social media platforms are crucial to identify and remove extremist content quickly. Public awareness campaigns should also be implemented to educate individuals about the dangers of online radicalisation. By adopting a comprehensive and coordinated strategy, it is possible to mitigate the risks posed by the internet in facilitating terrorism and enhance global security.

GENDERED APPROACHES TO COUNTER-TERRORISM: WHY WOMEN'S PERSPECTIVE MATTER

Siti Aisyah Tajari

ABSTRACT

This article explores the significance of integrating gendered perspectives into counter-terrorism strategies, highlighting the critical roles women play as victims, perpetrators, and peacebuilders in terrorism-related contexts. Traditional counter-terrorism approaches, which often focus on military and security measures, frequently overlook the complex and multifaceted involvement of women in terrorist organisations. Women are not only disproportionately affected by gender-based violence and exploitation in conflict zones but are also actively engaged in recruitment, operational activities and the ideological propagation of terrorism. Using a gender-sensitive lens, the article emphasises the need to recognise and address women's unique experiences and contributions in both terrorism and counter-terrorism efforts. By analysing case studies from Indonesia, Kenya, and global initiatives like UN Security Council Resolution 1325, this work underscores the strategic value of involving women in Preventing and Countering Violent Extremism (PCVE) and counter-terrorism strategies. It also addresses the cultural, institutional, and structural challenges that hinder the effective implementation of gendered approaches, such as the underrepresentation of women in security and law enforcement sectors. The article ultimately argues that gender-sensitive counter-terrorism strategies are essential for creating more inclusive, effective, and sustainable security outcomes. By neglecting women's roles, counter-terrorism efforts risk perpetuating incomplete solutions that fail to address the deeper causes of radicalisation and the social structures that support violent extremism. Incorporating women's perspectives can strengthen counter-terrorism approaches by making them more comprehensive, targeted, and successful in the long term.

Keywords: Gender-sensitive, gender perspectives, terrorism prevention, women's security, UN Security Council Resolution 1325

INTRODUCTION

Counter-terrorism strategies have traditionally centred on military, intelligence and law enforcement efforts. These approaches while essential somehow often overlook a critical dimension which is the gender aspects of counter-terrorism. Focusing solely on men as either perpetrators or leaders of terrorist activities neglects the multifaceted roles women play. Overall, women can be the victims, perpetrators, enablers, and peacebuilders in the context of terrorism. Ignoring these gendered roles creates gaps in counter-terrorism efforts leading to incomplete solutions that fail to address the roots of radicalisation or the social structures that sustain it. By incorporating women's perspectives, counter-terrorism strategies can be more comprehensive,

targeted, and effective. This article explores how women's roles intersect with terrorism and counter-terrorism and examines the importance of adopting a gender-sensitive approach to create more holistic and inclusive counter-terrorism strategies.

UNDERSTANDING GENDERED ROLES IN TERRORISM

The traditional view often frames women as victims which while accurate in many cases but does not encompass the full extent of their involvement in terrorism. Women are disproportionately impacted by terrorism, particularly in conflict zones where gender-based violence, forced marriages, and sexual exploitation are rampant (UNODC, 2019). Groups like Boko Haram and ISIS have explicitly targeted women and girls for sexual slavery, using these violent acts to further their ideologies and destabilise societies. In these settings, women's trauma goes beyond physical harm; they are often stigmatised within their communities, rendering them vulnerable to further violence and ostracism. Terrorist organisations also exploit women's grievances as a recruitment tool. For example, ISIS propaganda has specifically targeted marginalised women, offering promises of empowerment, protection, and a sense of belonging (Winter et al., 2017). By positioning their participation in violent extremism as a way to fight back against oppression, terrorist organisations exploit women's victimhood for strategic gains. The recruitment narratives employed by these groups extend beyond individual women, contributing to the broader radicalisation of communities.

However, focusing only on women's victimisation risks ignoring their active roles in terrorism. Women have not only been participants in terrorist organisations but have taken on various roles, including combat, logistics, and propaganda dissemination. The Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka, for example, famously recruited women as suicide bombers and soldiers (Alison, 2004). Similar roles for women have been observed in organisations like ISIS and Al-Qaeda, where women serve as operatives, fundraisers, and online recruiters (Nacos, 2019). Women's involvement in terrorism often occurs through familial and community networks, where they play influential roles in radicalising others. Mothers, sisters, and wives can become key actors in fostering extremist ideologies within their households (Bakker and de Leede, 2015). This underscores the necessity of adopting a gender-sensitive approach in both understanding and countering radicalisation processes. Counter-terrorism strategies that ignore the roles women play as perpetrators may fail to address critical elements of recruitment and operational dynamics within terrorist groups.

In contrast to their roles as perpetrators, women also play crucial roles as peacebuilders. Their positions as caregivers, educators, and community leaders offer them a unique capacity to act as mediators and influencers in preventing violent extremism. Women in conflict-affected areas have led grassroots efforts to reintegrate former extremists into society, rebuild social cohesion, and

foster peace (Dharmapuri, 2011). For example, women in Nigeria have been instrumental in community-based efforts to disarm and rehabilitate Boko Haram insurgents. In Indonesia, women have also played key roles in preventing radicalisation within their communities. These examples highlight the importance of recognising women as agents of change and peacebuilders, capable of countering the violent ideologies that drive terrorism. Acknowledging these roles is crucial for developing counter-terrorism initiatives that leverage the power of women in rebuilding communities and preventing the spread of extremism.

WHY WOMEN'S PERSPECTIVES MATTER IN COUNTER -TERRORISM

Women's perspectives matter in counter-terrorism because they bring a comprehensive understanding of the radicalisation process, which can differ significantly between genders. Women's radicalisation often results from a combination of social, political, and personal factors, including experiences of gender-based violence, economic marginalisation, and social isolation (Gentry and Sjoberg, 2015). In some cases, women are coerced into terrorism through forced marriages or sexual exploitation, but in others, they join voluntarily and are motivated by ideological convictions or a desire for revenge. Without a gender-sensitive approach, counter-terrorism strategies may overlook these unique pathways to radicalisation and may result in interventions that are less effective at addressing the root causes of extremism. Gender-sensitive aspects in de-radicalisation programmes, which take into account the specific factors that lead women to extremism are essential for preventing their recruitment and participation in terrorist activities.

Additionally, women's inclusion in decision-making processes and community engagement efforts is critical for effective counter-terrorism strategies. In many communities, women hold significant influence within their families and social networks. By ignoring their perspectives, counter-terrorism efforts miss out on an important resource for early detection and also intervention. Women can serve as 'early warning systems' by identifying signs of radicalisation within their families and communities (OSCE, 2019). Programmes that engage women as partners in preventing and countering violent extremism (PCVE) efforts can foster trust between communities and law enforcement, promoting collaboration that is essential for preventing extremism. In Indonesia for example, mothers have played an integral role in identifying early signs of radicalisation in their children by helping to disengage them from extremist ideologies before violence occurs (Nilan, 2020). By equipping women with the knowledge and tools to detect radicalisation, these family-based approaches have proven successful in preventing recruitment into terrorist groups.

Women's participation is also essential in addressing the gender-specific needs of rehabilitation and reintegration programmes. Female ex-combatants or those associated with terrorist

organisations often face unique challenges during rehabilitation due to social stigma, psychological trauma, and community ostracism. Many of these women are ostracised by their families and communities for their involvement in terrorism, further complicating their reintegration process (Vale, 2019). Additionally, some women may have been coerced into terrorist activities through forced marriages or exploitation which can create psychological barriers to rehabilitation. Gender-sensitive rehabilitation programmes that provide psychological support, vocational training, and social reintegration pathways tailored to women are critical for helping these women rebuild their lives. Successful reintegration not only helps these women regain their agency but also reduces the likelihood of recidivism, contributing to broader societal stability (Cook and Vale, 2018).

In addition to the practical benefits of engaging women in counter-terrorism, shifting the narrative to include women as active participants in peacebuilding efforts can help break harmful gender stereotypes. The dominant narrative in counter-terrorism often casts women solely as victims, which can be disempowering and limit their potential contributions to peace and security. By recognising women as agents of change, policymakers can challenge these stereotypes and encourage greater participation of women in security sectors (O'Neil and Vargheese, 2011). For example, portraying women as leaders in community resilience-building can inspire others to take active roles in preventing extremism. A gender-inclusive narrative also promotes a more comprehensive understanding of the complex dynamics of terrorism, ensuring that counter-terrorism strategies address the full spectrum of actors involved.

CASE STUDIES: GENDER-SENSITIVE IN COUNTER-TERRORISM APPROACHES

Several countries have already begun to implement gender-sensitive counter-terrorism strategies with significant success. In Indonesia, the government’s family-based approach to counter-terrorism has emphasised the role of mothers in preventing radicalisation within their families. By educating women on the signs of radicalisation and providing them with the tools to intervene, Indonesia has effectively disengaged youth from extremist ideologies and prevented terrorist recruitment (Nilan, 2020). Mothers in particular, have been key in detecting early signs of radicalisation and guiding their children away from violent ideologies before they become fully entrenched. This model highlights the importance of engaging women in community-based counter-terrorism efforts.

Similarly, in Kenya, women’s networks have played a pivotal role in countering violent extremism at the grassroots level. Women’s groups have worked within their communities to address socio-economic grievances, promote alternative narratives, and support de-radicalisation efforts (Botha, 2014). These initiatives have been particularly effective in building trust between local communities and law enforcement, helping to create more resilient societies that are less

vulnerable to extremist ideologies. By empowering women to take active roles in PVE efforts, these programmes have contributed to a more comprehensive and sustainable approach to counter-terrorism.

The international community has also recognised the importance of gender in counter-terrorism through initiatives like UN Security Council Resolution 1325, which calls for the inclusion of women in peace and security processes (UNSCR 1325, 2000). The Women, Peace, and Security (WPS) agenda promotes the integration of gender perspectives into counter-terrorism and PCVE strategies, recognising that women's participation is essential for preventing conflict and terrorism. Countries that have adopted National Action Plans (NAPs) on WPS have integrated gender-sensitive approaches into their security strategies, ensuring that women are actively involved in peacebuilding and counter-terrorism efforts.

CHALLENGES IN IMPLEMENTING GENDERED APPROACHES

Despite these successes, there are still significant challenges in implementing gender-sensitive counter-terrorism approaches. Cultural and institutional barriers such as traditional gender norms and patriarchal structures can hinder women's participation in security sectors and community leadership roles (True and Eddyono, 2017). Overcoming these barriers requires both cultural shifts and institutional support for gender equality. Additionally, many security personnel and law enforcement agencies lack the training needed to incorporate gender perspectives into their operations. Gender-sensitive training is essential for equipping these personnel to recognise the specific roles women play in both terrorism and counter-terrorism allowing them to design more effective interventions (OSCE, 2019).

Finally, women remain underrepresented in security and defence sectors, limiting their ability to influence counter-terrorism strategies. Increasing women's participation in these fields is critical for ensuring that gender perspectives are adequately represented in policy development. Without representation, counter-terrorism strategies risk overlooking the full spectrum of women's roles in terrorism and counter-terrorism. Expanding women's involvement in security sectors, particularly at leadership levels, will ensure that gender-sensitive perspectives inform counter-terrorism policies.

CONCLUSION

Incorporating women's perspectives into counter-terrorism strategies is not only a matter of gender equality but a strategic imperative. Women play diverse and critical roles in terrorism which are as victims, perpetrators, and peacebuilder. Their involvement in counter-terrorism also can enhance the effectiveness of security efforts. A gendered approach acknowledges the

pathways through which women are radicalised, engages them as active participants in preventing extremism, and addresses their specific needs in rehabilitation and reintegration. By overcoming cultural and institutional barriers, providing gender-sensitive training and increasing women's representation in security sectors, governments and organisations can develop more comprehensive and effective counter-terrorism strategies. Gender-sensitive counter-terrorism initiatives are essential for achieving long-term peace and security, making it crucial for policy-makers to prioritise gender in their counter-terrorism frameworks.

REFERENCES

Alison, M. (2004). Women as agents of political violence: Gendering security. Security Dialogue, 35(4), 447–463. https://doi.org/10.1177/0967010604049522

Bakker, E., & de Leede, S. (2015). European female jihadists in Syria: Exploring an under-researched topic. International Centre for Counter-Terrorism. https://doi.org/10.19165/2015.1.02

Botha, A. (2014). Institute for Security Studies Papers, (265), 1–28. https://issafrica.org/research/papers/radicalisation-in-kenya-recruitment-to-al-shabaab-and-the-mombasa-republican-council

Cook, J., & Vale, G. (2018). From Daesh to 'diaspora': Tracing the women and minors of Islamic State. International Centre for the Study of Radicalisation. https://icsr.info/2018/07/23/daesh-to-diaspora/

Dharmapuri, S. (2011). Just add women and stir? Parameters, 41(1), 56–70. https://press.armywarcollege.edu/parameters/vol41/iss1/9/

Gentry, C. E., & Sjoberg, L. (2015). Beyond mothers, monsters, whores: Thinking about women's violence in global politics. Zed Books.

Nacos, B. L. (2019). Terrorism and counterterrorism (5th ed.). Routledge. https://doi.org/10.4324/9780429434415

Nilan, P. (2020). Youth identity and radicalization: Lessons from Indonesian Pesantren. Contemporary Islam, 14(3), 1–17. https://doi.org/10.1007/s11562-019-00437-x

O'Neil, S., & Vargheese, R. (2011). Women and terrorist radicalization: Final report. Women in International Security. https://wiisglobal.org/reports/wiis-2011-women-and-terrorist-radicalization-report/

OSCE. (2019). Understanding the role of gender in preventing and countering violent extremism and radicalization that lead to terrorism. Organization for Security and Co-operation in Europe. https://www.osce.org/secretariat/420563

True, J., & Eddyono, S. (2017). Preventing violent extremism: Gender perspectives and women's roles. Monash Gender, Peace & Security Centre. https://doi.org/10.4225/03/5a273c5d94d7b

UNODC. (2019). Handbook on gender dimensions of criminal justice responses to terrorism. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/terrorism/Handbook_on_Gender_Dimensions_of_Criminal_Justice_Responses_to_Terrorism.pdf

UNSCR 1325. (2000). United Nations Security Council Resolution 1325 on women, peace and security. https://undocs.org/S/RES/1325(2000)

Vale, G. (2019). Women in Islamic State: From caliphate to camps. International Centre for the Study of Radicalisation. https://icsr.info/2019/07/23/women-in-islamic-state-from-caliphate-to-camps/

Winter, C., & Margolin, D. (2017). The Mujahidat dilemma: Female combatants and the Islamic State. CTC Sentinel, 10(7), 23–28. https://ctc.usma.edu/the-mujahidat-dilemma-female-combatants-and-the-islamic-state/

OBSERVING ONLINE TRENDS ON THE FAR-RIGHT EXTREMISM IN SOUTHEAST ASIA AND ITS POTENTIAL THREAT

Kennimrod Sariburaja and Nik Nurdiana Zulkifli

ABSTRACT

While historically rooted in Western societies, far-right extremism (FRE) is increasingly permeating Southeast Asia through digital platforms, presenting new risks to regional stability. This article analyses the online proliferation of FRE in Southeast Asia, focusing on how Western far-right ideologies — such as ultra-nationalism and xenophobia — are being adapted to fit local socio-political dynamics. These ideologies are often recontextualised with local symbols, narratives, and grievances, facilitated by the global reach of the internet and social media. The article examines key case studies, including the influence of Western far-right memes and the rise of local extremist movements inspired by neo-Nazism. Additionally, it explores the significant challenges in regulating and combating this digital spread, including fragmented legal frameworks, insufficient social media oversight, and the complex balance between protecting free speech and ensuring public safety. The rising threat of FRE in Southeast Asia poses serious challenges to political stability and social cohesion, underscoring the need for stronger regulatory measures, enhanced inter-agency coordination, and international collaboration to address this growing issue.

Keywords: Far-right extremism (FRE), Southeast Asia, Digital platforms, Neo-Nazism, Radicalisation

INTRODUCTION

Far-right extremism (FRE), which is often characterised by authoritarianism, ultra-nationalism, xenophobia, racism, chauvinism, and reactionary ideologies, has traditionally been rooted in Western historical and political contexts (Camus and Lebourg, 2017). Historically, far-right ideologies have been region-specific, largely influencing Europe and North America. However, with the rise of the internet and digital platforms, these ideologies have transcended Western borders, reaching diverse global audiences. Southeast Asia, in particular, has seen the adaptation and reshaping of far-right ideologies to fit local socio-political dynamics, disseminated through social media, online forums, and digital communities. Despite these developments, much of the academic literature on extremism in Southeast Asia has predominantly focused on Islamist extremism, overlooking the significance of examining Western-style FRE in the region (Munira Mustaffa, 2021; Ferrarese, 2019). This article explores the spread of FRE in Southeast Asia, the factors fuelling its growth, and the potential threat it poses to the region's societal stability and political order.

AN OVERVIEW OF FAR-RIGHT EXTREMISM: FROM WESTERN NATIONS TO SOUTHEAST ASIA

FRE refers to political ideologies that advocate ultra-nationalism, authoritarianism, and the rejection of pluralism and liberal democracy (Camus et al., 2017). Although these movements vary in their specific political and cultural goals across different regions, they typically promote exclusionary principles based on race, ethnicity, religion, or nationality. FRE movements commonly express opposition to immigration, multiculturalism, globalism, and progressive social policies, often employing both inflammatory political rhetoric and violent methods to pursue their objectives (Mudde, 2019).

In recent years, FRE has been increasingly recognised as a global security threat, particularly in Western countries. A 2022 report by the United Nations Secretary-General to the United Nations General Assembly (UNGA) noted the rise of far-right or extreme right-wing terrorism as one of the fastest-growing global security risks. Between 2014 and 2018, far-right attacks increased by 320%, with incidents such as the 2011 Utøya massacre in Norway and the 2019 Christchurch Mosque shootings in New Zealand exemplifying the deadly potential of these ideologies (United Nations General Assembly, 2022).

The threat posed by FRE is particularly pronounced in Western nations, where far-right groups have gained visibility and influence. For example, in the United States, although the government was initially slow to designate far-right groups as terrorist organisations, recent developments signal a shift in policy. In June 2024, the Biden administration sanctioned the Nordic Resistance Movement (NRM), a neo-Nazi group based in Scandinavia, marking a significant step in combating far-right extremism globally. This followed a similar designation of the Russian Imperial Movement by the Trump administration in 2020 (Blazakis, 2024).

Europe has also witnessed the rise of far-right extremism in mainstream politics. Notable examples include Marine Le Pen's National Rally party in France, which made significant gains in the French elections, and Giorgia Meloni’s Brothers of Italy, a far-right party that won the 2022 general election, becoming a dominant political force in Italy (Sierakowski, 2024). These developments reflect a broader trend of far-right political movements gaining traction across Europe, raising concerns about the future of liberal democratic norms and political stability on the continent.

Despite its roots in Western political contexts, far-right extremism has proven to be adaptable, finding resonance in various regional contexts beyond the West. The internet and social media platforms have played a critical role in the global spread of FRE. These digital spaces enable the rapid dissemination of extremist content, conspiracy theories, and disinformation, allowing far-right groups to recruit, radicalise, and form transnational networks (Davey and Ebner, 2019).

Algorithms on these platforms often amplify divisive content, increasing the visibility of extremist movements (Neumann, 2013).

The influence of American cultural soft power has also been a significant driver of the international spread of far-right ideologies. The U.S., as a global ideological influencer, exports populist, nationalist, and xenophobic ideas, often through its media, political discourse, and social movements (Blee and Creasap, 2010). High-profile events such as the 2017 Unite the Right rally in Charlottesville and the 2021 Capitol riots gained worldwide attention and have inspired far-right groups across the globe. Southeast Asia has not been immune to these influences, with local actors mimicking Western far-right strategies to spread Islamophobic and xenophobic narratives (Sarwono, 2024). Controversial figures like Ian Miles Cheong from Malaysia and RadioGenoa from Cambodia have gained notoriety for promoting far-right, white supremacist, and Islamophobic content on platforms like X (formerly Twitter), catering primarily to Western audiences (Saddiq Basha, 2024).

While Southeast Asia has historically faced more immediate threats from Islamist extremist groups such as Jemaah Islamiyah (JI) and Daesh, far-right extremism is slowly emerging as a growing concern in the region. Localised far-right movements in Southeast Asia have often drawn inspiration from neo-Nazi ideologies. For instance, in Malaysia, a Neo-Nazi-inspired subculture known as "Malay Power" promotes Malay supremacist ideology and hosts exclusive concerts advocating for "one race, one leader, one nation" (Ferrarese, 2019). Similarly, in Myanmar, the 969 Movement, a nationalist Buddhist group, is known for its violent anti-Rohingya and anti-Muslim stance. The group has been compared to neo-Nazi movements and draws inspiration from Western far-right organisations like the English Defence League (Munira Mustaffa, 2021).

The spread of FRE in Southeast Asia, largely fueled by online radicalisation, underscores the region's growing vulnerability to this ideology. A notable example occurred in December 2020 when a 16-year-old Singaporean male was detained under the Internal Security Act (ISA) for plotting terrorist attacks on two mosques. Inspired by the 2019 Christchurch Mosque shootings, the youth had been radicalised online and sought to emulate the attack by livestreaming his actions, reflecting the transnational influence of far-right extremist ideology (Internal Security Department, 2021).

ONLINE TRENDS ON FAR-RIGHT EXTREMISM IN SOUTHEAST ASIA

The internet has become a critical space for the dissemination of far-right ideologies, with extremist groups and influencers leveraging social media platforms and websites to propagate their beliefs (Ang, 2021). An in-depth analysis of the far-right extremist (FRE) subculture in Southeast Asia by Jonathan Sarwono (cited in Saddiq Basha, 2024) highlights how Western far-right meme culture has been adapted to promote Austronesian racial supremacy. This

community primarily active in Indonesia, Malaysia, and the Philippines, incorporates Western meme aesthetics into local socio-political contexts. Key examples include a Filipino TikTok user posting a meme featuring Nazi propagandist Joseph Goebbels with the caption “Foreigners in my country”, expressing xenophobic views. Another user shared a video quoting Adolf Hitler in Bahasa Indonesia, merging Third Reich imagery with Southeast Asian nationalism (Sarwono, 2024).

Localised adaptation is a key feature of this subculture's posts. The hashtag “#austronesianclassic” showcases supremacist memes modelled after the Western far-right “Aryan Classics” trend. These memes incorporate local historical and cultural symbols, such as Indonesia's Surya Majapahit (Majapahit sun) and the Philippines’ eight-rayed golden sun, as parallels to the white supremacist black sun — a symbol originating in Nazi Germany and later adopted by neo-Nazis and other far-right groups. The black sun's design, featuring twelve radial sig runes, resembles the SS logo symbols, reinforcing the connection between these localised memes and global far-right ideologies.

The Great Replacement theory, a white nationalist far-right conspiracy theory popularised by French author Renaud Camus, has also gained traction in Southeast Asia. While the theory is most prominent in Europe, it is often linked with the “Eurabia” conspiracy theory, which claims that Muslims will eventually replace the white population of Europe. In Southeast Asia, this concept has been adapted to fit local xenophobic narratives. For instance, an Indonesian user shared a meme echoing the Western far-right’s “Great Replacement” theory, showing a future where Austronesian families are replaced by Rohingya and Chinese immigrants, fueling fears about ethnic displacement (Camus, 2012; Saddiq Basha, 2024).

Finally, violent Nazi dog whistles are a common feature of these online communities. Memes, such as one from Indonesia, depict an Austronesian man attacking Arab and Chinese characters with captions like “Totally Cheerful Day” — a localised version of the far-right’s violent slogans like “Total N****r Deaths”. These examples demonstrate how Western far-right memes, symbols, and narratives are localised in Southeast Asia’s extreme right online communities, amplifying ethno-religious supremacy in the region.

DISCUSSION

Several factors contribute to the rise of problematic content in Southeast Asia. One significant factor is content monetisation, which incentivises the creation of highly engaging, often sensationalist content, including fake news and provocative “rage bait”. This type of content aims to incite anger, confusion, and division among viewers. Research indicates that the potential for monetary gain drives the spread of irresponsible posts, making it difficult to distinguish between genuine far-right extremist propaganda and mere sensationalism (Phillips and Milner, 2017).

Furthermore, many internet users struggle to discern between satire and legitimate content, which increases their susceptibility to influence. Even when the content is intended as a joke, it contributes to the normalisation of harmful and extremist narratives (Marwick and Lewis, 2017).

The Southport riots serve as a stark example of how misinformation can incite real-world violence. In this case, Farhan Asif, a 31-year-old Pakistani software engineer, was charged with cyber terrorism in Lahore for disseminating false information on his website, Channel3Now. His article falsely accused a Muslim asylum seeker of involvement in a fatal knife attack in the UK, leading to anti-immigration riots targeting mosques and asylum accommodations. The actual suspect, Axel Rudakubana, was a UK-born individual of Rwandan descent. Asif's motives appeared to be driven by profit from sensational content (“Pakistan Man Faces Cyber Terror charge over false posts linked to UK riots”, 2024). He was later acquitted by a Pakistani court. This case illustrates how easily misinformation can fuel real-world violence and tensions.

Another significant factor is social media policies. Major platforms, many of which are based in the United States, often prioritise free speech, even at the expense of enabling hate speech and extremist politics. Social media giants, such as X (formerly Twitter), have become notorious for allowing far-right content to proliferate. Elon Musk, the CEO of X, has advocated for free speech, but his platform has become a prominent venue for pro-Nazi content. According to a report by NBC News, at least 150 paid “Premium” accounts and thousands of unpaid ones have been involved in promoting Nazi propaganda, including Holocaust denial and praise for the Nazi regime (Ingram, 2024). Despite platform policies aimed at curbing such content, these posts continue to gain substantial traction, with some reaching millions of views.

Beyond the influence of the internet and social media, the history and politics of Southeast Asia have also shaped the region’s adaptation of FRE. One major contributing factor is the strong opposition of far-right ideologies to Communism, which occupies the opposite end of the political spectrum. During the Cold War, Southeast Asia experienced Communist insurgencies, which fostered an alignment between anti-Communist sentiments and far-right ideologies. Both shared a mutual enmity toward Communism. This alignment also extends to the adoption of Sinophobic and antisemitic views, fueled by historical tensions with Communist China and the misconception among some Muslims in Southeast Asia that Zionism represents the entire Jewish population (Hoffman, 2019). A lack of historical awareness often leads to contradictions, such as expressing admiration for Nazi ideology while condemning Imperial Japan's World War II atrocities in South-east Asia, despite Japan being aligned with Nazi Germany during the war.

A lack of historical and political awareness further enables the spread of far-right ideologies like neo-Nazism in Southeast Asia. Many individuals in the region sympathise with neo-Nazi attitudes toward Jews or the Chinese without fully understanding the racial policies of the Nazi regime,

which included forced sterilisations and the extermination of those considered “Untermenschen” (sub-humans). The limited exposure to Western history, particularly the atrocities of Nazism, has made it easier for far-right extremism to resonate with Southeast Asian audiences.

Another key factor is the rejection of progressive Western liberalism. The “red-pilled” culture, popular in certain internet subcultures, plays a significant role in promoting far-right ideologies. Being “red-pilled” refers to the belief that one has awakened to hidden truths about society, politics, or culture, often leading to a rejection of mainstream narratives or progressive values. This concept, frequently associated with far-right, anti-feminist, or libertarian ideologies, encourages opposition to feminism, liberalism, multiculturalism, and other progressive ideals (Nagle, 2017). This cultural shift aligns many in Southeast Asia with far-right extremism, as they adopt counter-cultural beliefs that reject Western progressive ideas in favour of more reactionary positions.

CHALLENGES IN ADDRESSING FAR-RIGHT EXTREMISM IN SOUTHEAST ASIA

Addressing Far-Right Extremism (FRE) in the online space in Southeast Asia presents several challenges. One significant issue is the lack of literature specifically addressing FRE in Southeast Asian online spaces, as most research has focused on Islamist radicalism. Much of Southeast Asia's counter-terrorism efforts have centred around groups like Jemaah Islamiyah (JI) and Daesh, given their historical threat in the region. However, the recent radicalisation of a teenager in Singapore, who was inspired by Western far-right ideologies, underscores the growing influence of FRE via the internet in Southeast Asia (Lim, 2024). The failure to address this phenomenon risks normalising harmful far-right ideologies in the region’s online spaces, potentially creating a more accepting environment for extremism to thrive.

Another major challenge is regulating social media platforms, which operate across national borders, complicating the enforcement of local laws and content policies. Social media platforms like Facebook, YouTube, and X are widely used in Southeast Asia, making them fertile ground for the dissemination of far-right content. Moderating this content requires a balance between free speech and public safety, and this is made more difficult by the varying interpretations of harmful content (Deibert et al., 2022). According to Sriyai (2024) and Rapha (2024), many governments in Southeast Asia lack the technical capacity to effectively monitor and remove far-right content from these platforms. In some cases, regulatory frameworks are either too lenient or too vague, allowing extremists to exploit legal loopholes.

Coordination between national authorities, law enforcement agencies, and social media companies presents another significant challenge. In Southeast Asia, different government agencies often have overlapping responsibilities in areas such as cybersecurity,

counter-terrorism, and media regulation, which leads to bureaucratic inefficiencies and delays in responding to online FRE activities (Socquet-Clerc et al., 2023). Furthermore, the region's countries vary significantly in their legal frameworks and approaches to extremism. Some governments may prioritise suppressing Islamist extremism, while others may not even recognise far-right extremism as a serious issue. This lack of unified understanding and strategy both within and between countries complicates efforts to develop a comprehensive solution to counter the spread of far-right ideologies online (Weimann, 2023).

In addition, outdated legal frameworks in many Southeast Asian countries hinder efforts to tackle online FRE. Existing laws on hate speech and extremist content are often inadequately defined, making it difficult for authorities to prosecute offenders or request content removal from social media platforms. While governments may seek stricter regulations on these platforms, they frequently face pushback from tech companies, which argue for maintaining user privacy and free expression (Gorwa, 2021). This creates a regulatory gap that allows far-right groups to exploit digital platforms with relative freedom, further complicating the efforts of governments to regulate extremist content effectively (Deibert et al., 2022).

In summary, addressing FRE in Southeast Asia's online spaces is a complex task that requires stronger social media regulation, improved coordination between authorities, and clearer regulatory frameworks. Without these measures, efforts to curb online far-right extremism will continue to face significant obstacles.

CONCLUSION

The rise of far-right extremism (FRE) in Southeast Asia's online spaces presents a growing and destabilising threat. Once considered primarily a Western issue, FRE has spread globally through the internet and now infiltrates the socio-political landscapes of Southeast Asia. With the region's increasing internet penetration and ethnically diverse populations, Southeast Asia is particularly vulnerable to the influence of these extremist ideologies. The spread of FRE is reshaping political discourse, deepening social divisions, and radicalising individuals, posing long-term risks to regional stability.

Social media platforms are instrumental in the dissemination of far-right ideologies. Far-right online communities, influenced by Western movements, have localised their rhetoric to resonate with regional ethno-nationalist and religious tensions. For example, Austronesian supremacist groups in Indonesia and Malaysia have appropriated Western far-right symbols and language to promote ethnic and religious chauvinism, aggravating existing social fragmentation. This localised adaptation of FRE threatens to exacerbate already fragile ethnic and religious relationships in countries such as Myanmar, Malaysia, and Indonesia.

The potential for individual radicalisation is significant. The case of a Singaporean teenager, who was inspired by Western far-right content and plotted a Christchurch-style mosque attack, exemplifies the global connectivity of FRE and the influence of online propaganda. The availability of manifestos, videos, and extremist discourse online makes vulnerable individuals more susceptible to radicalisation. The transnational nature of FRE means that Southeast Asian extremists may see themselves as part of a broader global movement, further increasing the likelihood of lone-wolf attacks.

FRE also poses a threat to political stability by fostering authoritarianism, opposing pluralism, and promoting anti-democratic sentiments, all of which are at odds with Southeast Asia's emerging democracies. In some cases, far-right extremism aligns with historical anti-Communism, which could reignite old political tensions and fuel the resurgence of ultra-nationalist politics. Such developments would undermine democratic institutions and potentially increase governmental instability across the region.

Addressing the spread of FRE online is fraught with challenges, particularly due to insufficient regulation of social media platforms. Global platforms like Facebook, YouTube, and X struggle to effectively moderate extremist content due to their vast scale. Despite efforts to curb hate speech and extremist propaganda, enforcement gaps allow far-right ideologies to persist and proliferate. Additionally, governments in Southeast Asia face difficulties balancing the protection of free speech with ensuring public safety, and many lack the technical resources needed to regulate these global platforms effectively.

The fragmented regulatory response across Southeast Asia further complicates efforts to combat FRE. Multiple agencies, each responsible for different areas such as media, cybersecurity, and counter-terrorism, often work in silos, leading to inefficiencies and delays in addressing online extremism. Outdated legal frameworks compound the problem, as many of the existing laws are ill-equipped to address the nuances of digital extremism. Social media companies, citing concerns over privacy and free speech, frequently resist stricter regulations, leaving a regulatory vacuum that allows extremist content to spread with relative ease.

To mitigate these risks, Southeast Asian governments must take a multi-faceted approach. This includes strengthening social media regulations, enhancing coordination between national and regional authorities, and updating legal frameworks to reflect the complexities of the digital landscape. Effective collaboration with social media companies, civil society, and international partners will also be crucial in curbing the spread of far-right ideologies and safeguarding the region's socio-political stability. Without decisive action, far-right extremism will continue to pose a significant threat to Southeast Asia's peace and democratic future.

REFERENCES

Ang, Q. (2021, January 28). What is far-right extremist ideology and how did a Singaporean teen become radicalised? The Straits Times. https://www.straitstimes.com/singapore/askst-what-is-far-right-extremist-ideology-and-how-did-a-s-porean-teen-become-radicalised

Blazakis, J. M. (2024, July 1). US's terrorist listing of European far-right group signals fears of rising threat − both abroad and at home. The Conversation. https://theconversation.com/uss-terrorist-listing-of-european-far-right-group-signals-fears-of-rising-threat-both-abroad-and-at-home-232794

Blee, K. M., & Creasap, K. A. (2010). Conservative and right-wing movements. Annual Review of Sociology, 36, 269–286. https://doi.org/10.1146/annurev.soc.012809.102602

Camus, J.-Y., Lebourg, N., & Todd, J. M. (2017). Far-right politics in Europe. The Belknap Press of Harvard University Press

Davey, J., & Ebner, J. (2019). The Great Replacement: The violent consequences of mainstreamed extremism. Institute for Strategic Dialogue.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2022). Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. MIT Press.

Ferrarese, M. (2019, July 26). The neo-nazi punk and metal bands espousing "Malay power." South China Morning Post. https://www.scmp.com/lifestyle/arts-culture/article/3019249/whats-behind-malay-power-music-ethnic-malay-neo-nazis?module=perpetual_scroll_0&pgtype=article

Hoffman, B. (2019). Inside Terrorism. Columbia University Press.

Gorwa, R. (2021). "The Platform Governance Triangle: Conceptualising the Social Media Regulation Debate." Internet Policy Review, 8(2), 1-22.

Ingram, D. (2024, April 16). Verified pro-Nazi x accounts flourish under Elon Musk. NBCNews.com. https://www.nbcnews.com/tech/social-media/x-twitter-elon-musk-nazi-extremist-white-nationalist-accounts-rcna145020

Internal Security Department. (2021, January 27). Detention of Singaporean Youth Who Intended to Attack Muslims on the Anniversary of Christchurch Attacks in New Zealand. Ministry of Home Affairs. https://www.mha.gov.sg/newsroom/press-release/news/detention-of-singaporean-youth-who-intended-to-attack-muslims-on-the-anniversary-of-christchurch-attacks-in-new-zealand

Lim, K. (2024, February 17). Far-right views in Asia? Singapore cases may reflect movement's slow creep. South China Morning Post. https://www.scmp.com/week-asia/people/article/3252233/far-right-views-southeast-asia-how-2-singapore-cases-may-reflect-anti-woke-movements-slow-creep

Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. Data & Society Research Institute.

Munira Mustafa. (2021, July 14). Right-wing extremism has deep roots in Southeast Asia. GNET. https://gnet-research.org/2021/07/14/right-wing-extremism-has-deep-roots-in-southeast-asia/

Nagle, A. (2017). Kill All Normies: Online Culture Wars From 4chan and Tumblr to Trump and the Alt-Right. Zero Books.

Phillips, W., & Milner, R. M. (2017). The ambivalent internet: Mischief, oddity, and antagonism online. Polity Press.

Rapha, A. J. (2024, July 19). Surfing the web for effective content regulation in Southeast Asia. East Asia Forum. https://eastasiaforum.org/2024/07/18/surfing-the-web-for-effective-content-regulation-in-southeast-asia/

Saddiq Basha. (2024, April 8). The creeping influence of the extreme right's meme subculture in Southeast Asia's TikTok Community. GNET. https://gnet-research.org/2024/04/08/the-creeping-influence-of-the-extreme-rights-meme-subculture-in-southeast-asias-tiktok-community/

Sarwono, J. S. (2024, February 13). 'Yup, Another Far-right Classic': The Propagation of Far-right Content on TikTok in Malaysia, Indonesia, and the Philippines. GNET. https://gnet-research.org/2023/11/08/yup-another-far-right-classic-the-propagation-of-far-right-content-on-tiktok-in-malaysia-indonesia-and-the-philippines/.

Sierakowski, S., Ehrenreich, M., Laïdi, Z., Legrain, P., Muzikárová, S., & Žižek, S. (2024, July 12). A far-right resurgence in Europe?. Project Syndicate. https://www.project-syndicate.org/onpoint/a-far-right-resurgence-in-europe

Socquet-Clerc, K., Su-Yen, S. K., Fitriani, Gomez, M. A., & Viet Lam, N. (2023, November). Cybersecurity Governance in Southeast Asia: Thematic SSG Brief. DCAF - Geneva Centre for Security Sector Governance. Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/Cybersecurity_Governance_in_Southeast_Asia_Thematic_Brief.pdf

Sriyai, S. H. (2024, August 27). How Means for Digital Repression in Southeast Asia Have Unfolded in Recent Times. ISEAS - Yusof Ishak Institute. Retrieved from https://www.iseas.edu.sg/wp-content/uploads/2024/08/ISEAS_Perspective_2024_65.pdf.

The Guardian. (2024, August 21). Man charged in UK over Pakistan misinformation that fueled Southport riots. The Guardian. https://www.theguardian.com/world/article/2024/aug/21/man-charged-pakistan-misinformation-southport-uk-riots

United Nations General Assembly. (2022). (rep.). Terrorist attacks on the basis of xenophobia, racism and other forms of intolerance, or in the name of religion or belief. Retrieved from https://documents.un.org/doc/undoc/gen/n22/450/52/pdf/n2245052.pdf.

Weimann, G. (2023). Terrorism in Cyberspace: The Next Generation. Columbia University Press

TRENDS AND INDICATORS OF TERRORISM MOVEMENT IN EUROPEAN UNION SINCE 2020: A REFLECTION

Krešimir Mamić and Robert Mikac

ABSTRACT

Terrorism poses a significant security threat to the European Union, its Member States, citizens, and core values. Characterised by its ever-evolving nature and the diverse range of actors involved, terrorism is a complex phenomenon that necessitates ongoing research and analysis. This review aims to provide a comprehensive overview of key indicators and trends related to terrorism within the European Union from 2020 to the present. The selected starting point of 2020 is particularly relevant as it marks a pivotal year that witnessed notable changes in the methods and patterns of terrorist activity, largely driven by the impacts of the COVID-19 pandemic. The pandemic not only altered the operational landscape for terrorist groups but also influenced the socio-political context in which these groups operate. Moreover, this review will include an academic reflection on the evolving nature of terrorism, as well as normative solutions aimed at the prevention and suppression of such threats. By examining recent trends and responses, this analysis seeks to contribute to a deeper understanding of terrorism in the European context and to inform future policy-making efforts.

Keywords: Terrorism, prevention and suppression, European Union, COVID-19 pandemic

INTRODUCTION

Terrorism is a dynamic phenomenon that evolves based on various contextual factors, including geographical, political, social, and temporal elements. Terrorism often reflects the specific political and social conditions of a region. For instance, in areas with ongoing conflicts, such as the Middle East, terrorist groups in some cases emerge as a response to state failure or foreign intervention. In contrast, in Europe, more specifically in the European Union (EU) terrorism in many cases manifests through radicalisation linked to social integration issues or political grievances. Political context may influence terrorism in very different ways. The way governments respond to terrorism can influence its evolution. For example, heavy-handed security measures may suppress immediate threats but can also lead to increased resentment and radicalisation among marginalised communities. Conversely, inclusive policies that address underlying grievances may reduce the appeal of extremist ideologies. The political climate can also affect the ideologies that underpin terrorism. For instance, the rise of right-wing extremism in the EU has been linked to anti-immigrant sentiments and nationalist movements, which have gained traction in recent years. Social context is also significant. Social cohesion or fragmentation within communities can impact the prevalence of terrorism. In cohesive communities, there may be

ground for extremist ideologies to take root. Finally, temporal elements like major historical events, such as the September 11, 2001 attacks or the Arab Spring, can reshape the landscape of terrorism. These events often lead to a surge in extremist ideologies and can inspire new groups or movements to emerge in response to perceived injustices. Also, situations like the COVID-19 pandemic have altered the operational landscape for terrorist groups. The pandemic has led to increased social isolation and economic hardship, creating conditions that can foster radicalisation. Extremist groups have adapted by shifting their recruitment strategies to online platforms, exploiting the vulnerabilities of individuals during crises. The aforementioned is the research focus of this work.

The COVID-19 pandemic has significantly influenced various aspects of society, including the emergence of new forms of extremism and terrorism in the EU. The pandemic has led to social isolation and increased time spent online, particularly among young people and minors. This environment has made them more susceptible to radicalisation, as extremist groups have exploited these conditions to recruit and spread their ideologies. The isolation experienced during lockdowns created a fertile ground for individuals to seek out online communities, some of which may promote extremist views. While the overall number of terrorist attacks in the EU decreased during the pandemic, the nature of extremist activities evolved. The propaganda efforts of groups like the so called Islamic State of Iraq and Syria and other extremist organisations intensified during this time, adapting to the digital landscape to reach potential recruits. This shift indicates that while physical attacks may have diminished, the threat of radicalisation and online extremism has not disappeared. The pandemic has exacerbated existing political and social tensions within European societies. Issues such as government responses to the pandemic, economic hardships, and social inequalities have fueled discontent. Extremist groups have capitalised on these grievances, framing their narratives around anti-government sentiments and societal division, which can lead to increased support for radical ideologies. Also, the pandemic has also posed security challenges for law enforcement agencies. With resources diverted to manage the health crisis, monitoring and countering extremist activities became more difficult. This situation has raised concerns about the potential for a resurgence of extremist violence as restrictions ease and societies reopen.

To explore prevention and suppression of terrorism within the European Union after 2020 (including that year too), the paper is divided into three sections following the Introduction. The first section, titled indicators of terrorism trends in the European Union, will be based on Europol's (the European Police Office) annual reports, which provide a comprehensive context for the entire Union in one place. The next section is titled academic reflection on the subject area and analyses scholarly works on this topic produced after 2020. The final section, titled normative solutions in the prevention and suppression of terrorism, presents an overview of key documents from the European Union that all EU Member States, candidate countries, and EU institutions are

to adhere to in their joint efforts to prevent and suppress terrorism.

INDICATORS OF TERRORISM TRENDS IN THE EUROPEAN UNION

The best view of the terrorism indicators trends in the European Union can be obtained by examining Europol's annual EU Terrorism Situation and Trend Report (TE-SAT). In these reports, an overview of the terrorism phenomenon in the EU in a given year is provided. The TE-SAT categorises terrorism based on ideological preferences into the following types: jihadist terrorism, right-wing terrorism, left-wing and anarchist terrorism, ethno-nationalist and separatist terrorism, and other types of terrorism.

The 2021 TE-SAT report presents figures, major developments, and trends pertaining to the terrorism situation in the EU in 2020. In 2020, restrictions on travel and gatherings due to the COVID-19 pandemic limited physical opportunities within the EU, including the movement of people to and from the EU, as well as the return of foreign terrorist fighters to Europe. As a result, in the analysis of jihadist terrorism, interactions were mainly observed to take place online. "Jihadists sought to exploit the COVID-19 pandemic for propaganda purposes, framing the disease in line with their long standing narratives" (Europol, 2021: 42). Significant online propaganda activities were recorded, aiming to facilitate the radicalisation process, recruit new members, and facilitate terrorism activities (ibid: 51). The COVID-19 pandemic has been noted to hasten the dissemination of right-wing extremist propaganda through online platforms, as opposed to traditional offline methods. Right-wing extremists took advantage of the pandemic to bolster their narratives surrounding accelerationism and conspiracy theories, which included anti-Semitic, anti-immigration, and anti-Islamic sentiments. There was a marked increase in the use of video games and related communication applications for the propagation of right-wing terrorist and extremist propaganda, particularly among youth people (ibid: 78-91). In relation to left-wing and anarchist terrorism, alongside persistent concerns, extremists from these groups introduced new subjects in 2020. These included scepticism towards technological and scientific advancements, opposition to COVID-19 containment measures, and environmental matters. The Internet remained the primary platform for left-wing and anarchist terrorists, as well as violent extremists, to assert responsibility for their attacks (ibid: 92).

From the 2022 TE-SAT report about terrorism situation in the EU in 2021, we can see a continuation of the terrorism indicators trends from the previous year. The limitations imposed by COVID-19 have significantly hindered various physical activities, including networking, training, recruitment, and the procurement of weapons. Additionally, traditional methods of financing terrorism and the physical movement of funds have been adversely affected. In this context, online financial services and virtual assets have gained prominence in the financing of terrorism, particularly within jihadist and right-wing extremist circles. The pandemic has intensified the online presence of individuals while simultaneously fostering social isolation, which has

heightened their vulnerability to radicalisation. Extremist ideologies have seized this crisis as an opportunity to promote their narratives. Since the beginning of the pandemic, Jihadist groups, along with right-wing, left-wing, and anarchist extremists, have adapted COVID-19 themes to align with their ideologies. New propaganda topics have emerged among both right-wing and left-wing extremists, including conspiracy theories regarding the origins of the pandemic, misinformation about vaccination efforts, and claims of mass surveillance by governmental authorities. Various platforms, including websites, blogs, social media, and encrypted messaging applications, have been instrumental in the spread of propaganda during this period. The combination of social isolation and increased online engagement has heightened the risks associated with violent extremist propaganda and terrorist content, particularly among youth and minors. Furthermore, gaming platforms and services are increasingly being utilised by right-wing terrorists to disseminate propaganda aimed at a younger audience (Europol, 2022: 5-15).

The 2023 TE-SAT report on the terrorism landscape within the EU for the year 2022 indicates a continuation of certain trends in terrorism indicators observed in the previous year, alongside the emergence of new indicators. Terrorism remained a significant threat to the EU throughout 2022. Notably, the affiliation with specific groups such as the so called Islamic State and al-Qaeda is becoming less pronounced among jihadist supporters. Right-wing terrorists and extremists disseminate a wide array of narratives, predominantly through online channels. Despite their diverse ideologies and backgrounds, terrorists and violent extremists share common interests and methodologies. The internet and technological advancements have continued to serve as essential facilitators for propaganda, as well as for the radicalisation and recruitment of susceptible individuals into terrorism and violent extremism. The most prominent responses to the Russian aggression against Ukraine were observed in the initial months of the conflict, primarily within the right-wing extremist community, manifesting in online communications and a limited number of right-wing extremists travelling to participate in the conflict. The utilisation of technology and the internet – including social media, instant messaging services, online forums, and gaming platforms – remains vital in the processes of radicalisation and recruitment, as well as in the dissemination of propaganda across a broad ideological spectrum (Europol, 2023: 6-19).

ACADEMIC REFLECTION ON THE SUBJECT AREA

The academic production of texts that explore and describe the prevention and suppression of terrorism within the European Union is very extensive. According to the Google Scholar database, more than 17,000 different texts dealing with this topic have been published since 2020. Through a more in-depth search using keywords (“prevention and suppression”; “terrorism”; “European Union”), a total of 462 papers were found. Upon reviewing all of these papers, 15 works specifically addressing the topic from the area of interest of this research were identified.

Cristina Ejova (2023) explores and emphasises the importance of the international political-legal regulation of cooperation for countering terrorism in Europe comprehensively, examining various specific components of the process of countering terrorism within the complex activities of the Council of Europe, European Union, and Organization for Security and Co-operation in Europe (OSCE). Viviana Sachetti (2021) examines the need to strengthen the legal framework and instruments of the European Union in order to effectively tackle the challenges arising from the widespread dissemination of terrorist content online. The author asserts that the EU is in the early stages of confronting the specific issue of the unlawful utilisation of the internet by terrorist entities. She highlights that the European Commission's proposal to expand the jurisdiction of the European Public Prosecutor's Office (EPPO) to include transnational terrorist offences has aptly acknowledged the absence of a European-level prosecution system and the lack of authoritative influence over domestic authorities. Consequently, the EPPO should serve as the primary authority empowered to issue directives to national prosecutors and to facilitate their collaborative efforts in this domain. Furthermore, she advocates for the enhancement of Eurojust and Europol roles as specialised agencies, leveraging their established expertise in this critical area. Mira Savilaakso (2021) also addresses the need for stronger and more precise legal norms in the prevention and suppression of terrorism. The author explores and elaborates on how the European Union, in dealing with terrorism, should also address changes in other legal frameworks, such as Asylum Law. She believes that it is necessary to exclude members of terrorist organisations from refugee status due to their participation in acts contrary to the purposes and principles of the UN.

The subsequent five articles investigate the frameworks and potential strategies for curbing the financing of terrorism. Oldřich Bureš (2023) asserts that in the aftermath of the 9/11 attacks, the European Union has established various tools aimed at combating the financial aspects of terrorism. Many of these tools were specifically crafted to implement and/or strengthen two principal counter-terrorism financing (CTF) frameworks that have influenced global CTF initiatives since 9/11: the "smart" sanctions model promoted by the United Nations (UN) Security Council and the anti-money laundering framework advocated by the G-7's Financial Action Task Force (FATF). The author evaluates the effectiveness of the EU in introducing and executing its own CTF measures post-9/11. However, official EU documents, such as the 2004 and 2008 strategies for countering terrorist financing, provide limited insight into assessing the preventative, deterrent, investigative, and analytical roles of its CTF initiatives. Consequently, the author concentrates on specific CTF objectives for EU Member States that can be measured: the ratification and implementation of United Nations Security Council Resolutions (UNSCRs) and FATF recommendations, as well as the drafting, adoption, and execution of the EU's own legal frameworks. Michał Matyasik (2023) examines the efforts of two organisations involved in Counter-Terrorism Financing: The Council of Europe and the Organization for Security and Cooperation in Europe. He provides an overview of the Financial Action Task Force, including its

history and regulatory framework. Additionally, the author highlights how specific nations, including the Czech Republic, Poland, and Slovakia, incorporate the counter-terrorism financing guidelines established by international bodies into their national legal frameworks. Fiamma Terenghi (2023) examines the connection between drug trafficking and terrorism financing, emphasising the necessity of disrupting this link at various levels as much as possible. The subsequent two authors investigate the fight against money laundering and terrorist financing. Ágata M. S. Hermida (2020) highlights the challenges that arise in the quest for effective regulations to combat money laundering. Within the European Union, various legal instruments have been established in accordance with the recommendations from the United Nations, the Council of Europe, and the Financial Action Task Force (FATF). These initiatives have successfully identified preventive measures and protections for the financial system, as well as tools aimed at addressing criminal activities. Nevertheless, while the EU has been proactive in the financial and economic domain, enhancements to criminal law instruments have only recently been realised through Directive (EU) 2018/1673, which seeks to harmonise the definition of money laundering as a crime. The author analyses the provisions of this Directive to strengthen the fight against money laundering within the criminal context across EU Member States. Maria Bergström (2024) investigates the limitations faced by the EU in combating money laundering and terrorist financing in an increasingly digital and fragmented environment. She underscores the absence of a universally accepted definition of money laundering, which poses a significant challenge for the implementation of legal frameworks and the actions of relevant authorities. Despite this, she asserts that the EU and its Member States must intensify their efforts to curtail money laundering activities in general, particularly those that contribute to terrorist financing.

The following three papers address the issues surrounding the definitions of terrorism and their application within various legal frameworks. Tamás Pék (2022) provides an overview of the different definitions of terrorism in international criminal law. Regrettably, despite the gravity of this threat, there is no universally accepted definition of terrorism within the realm of global international criminal law. This absence of a common definition presents a significant obstacle to effective collaboration among states and criminal authorities, adversely affecting the efficacy of counter-terrorism initiatives. The author outlines several proposals and potential avenues for a new regulatory approach aimed at alleviating this issue by establishing an accepted common definition in legislation and criminal law. Emerka C. Adibe (2020) conducts a critical examination of the legal and judicial frameworks present in the current laws of the international community for addressing offences classified as international crimes. The author argues that there are barriers within international legal norms that hinder the successful prosecution of terrorism, emphasising the urgent need for reform. Lastly, Rastislav Kazansky, Lucia Rysova, and Nina Mijoč (2021) focus on the foundational aspects of research concerning terrorism and radicalisation, highlighting the evolution of the term and the refinement of its terminology. The authors aim to identify research bases for studying the online space and the pervasive radicalisation associated

with terrorism.

Ultimately, the last four papers address various yet significant topics. Kamila Zarychta-Romanowska (2023) explores the issues surrounding hybrid threats that the European Union increasingly encounters. She points out that EU law enforcement agencies – Eurojust (the European Union Agency for Criminal Justice Cooperation), Europol, and OLAF (the European Anti-Fraud Office) – lack the executive authority necessary to conduct criminal investigations and prosecutions, leading to their perception as primarily supportive expert centres or administrative verification offices. She argues that this situation is not practically beneficial and cites the positive example of the European Public Prosecutor's Office (EPPO), a new independent EU entity that will possess executive powers, marking a significant advancement. Victoria H. McCloud (2023) investigates the role of social media intelligence in combating extremist and terrorist support, offering suggestions for enhancing effectiveness in this domain. Emina Kuhinja (2020) describes and emphasises the importance of the European Union's support for Western Balkans states in their counter-terrorism efforts. She highlights that the democratic institutions and mechanisms in the Western Balkans engaged in counter-terrorism are primarily financed by the European Union as part of the accession process. Finally, Florian Bieber and Lura Pollozhani (2021) examine the roles of governments and civil society in preventing terrorism. They stress the necessity for collaboration between governments and civil society organisations to develop and implement strategies across three categories: (1) Prevention and moderation; (2) Repression of radicalisation and violent extremism; and (3) De-radicalisation.

NORMATIVE SOLUTION IN THE PREVENTION AND SUPPRESSION OF TERRORISM

Development of the EU normative framework for prevention and suppression of terrorism was triggered by certain security events or new and emerging threats.

Lack of common EU approach for prevention and suppression of terrorism before 9/11 was changed by adopting first consolidated EU legislation on prevention and suppression of terrorism – Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism. That was for the first time that the EU decided to set up minimal legal standards for national legislation of Member States in the area of fighting terrorism. Main idea was to establish a common response to the emerging terrorist threat.

In upcoming years, with terrorist attacks in Madrid and London, terrorism become the main topic for discussion on security related matters. That resulted in adoption of the EU Counter-Terrorism Strategy in 2005, as a first strategic document of the EU for prevention and suppression of terrorism. Strategy was based on four main pillars – prevention, protection, pursuit and response, emphasising prevention of terrorism as main counter terrorism activity.

Next decade in counter terrorism was marked with intensive fight against Al-Qaida and other terrorist organisations and groups promoting radical/political Islam ideologies. In the EU legal framework development on prevention and suppression of terrorism, that period resulted in additional fragmentation of EU counter terrorism legislation. Year 2015 was remembered as a year of terrorist attacks on European territory with two terrible attacks in France, continued with attacks in Belgium, Germany and other EU Member States in upcoming years. Year 2015 also shown that the EU was not prepared for new terrorism challenges – so called Lone Wolves attacks prepared by highly radicalised individuals known as Home Grown Terrorists, mass use of the internet, social media and communication platforms for radicalisation, foreign terrorist fighters etc. That resulted in new discussion within EU authorities on the need for a new EU legal framework for prevention and suppression of terrorism. After long discussions on expert and political level, Council of European Union and EU Parliament on 17 March 2017 adopted Directive on Combating Terrorism as a new comprehensive piece of EU counter terrorism legislation. Directive criminalises new phenomenon such as foreign terrorist fighters, receiving of terrorist training, misuse of the internet for terrorist purposes etc. In the incoming 18 months all Member States implemented Directive in their national legislations, but new challenges urged EU authorities to new legal developments.

Early 2020 and global COVID-19 pandemic with lock-downs and global social deprivation resulted in new security challenges. Lock-downs moved life to virtual space where various forms of cybercrime, online radicalisation, child pornography, foreign political influence, conspiracy theories, hybrid threats and other insecurities grew in a short period. EU response for new challenges resulted in adoption of the Security Union Strategy in July 2020. Security Union Strategy was main EU strategic document in the area of internal security for period from 2020 till 2025, based on four main areas – (1) fighting terrorism and organised crime (focused on radicalisation, terrorism, extremism and all forms of international organised crime); (2) future-proof security environment (focused on protection of critical infrastructures and fight against cybercrime); (3) building strong security ecosystem (focused on strengthening research and innovation, cooperation and information exchange, skills and awareness raising and building strong borders), and (4) tackling evolving threats (focused on hybrid threats, cybercrime, illegal content online and development of modern law enforcement).

Based on the Security union strategy as a key strategic document of EU security, during December 2020 EU authorities adopted the main strategic document EU on prevention and suppression of terrorism – Counter-Terrorism Agenda for the EU. New Agenda promotes four main counterterrorism areas – Anticipate, Prevent, Protect and Respond. The new approach moved the EU focus on counterterrorism in earlier phase than the 2005 EU Counter-Terrorism Strategy to ‘anticipate’ before ‘prevent’. That approach allows national legislative mechanisms of EU Member States to build new national legal instruments for fighting terrorism in a more

effective way.

The global COVID-19 pandemic and new security challenges, mostly related to virtual space, spreading of conspiracy theories, foreign political influence, hybrid threats resulted in new forms of extremism ideologies. Individuals and groups connected under ideas of Violent Anti-System Extremism (VASE), all forms of Right-Wing Extremism (RWE), ideas of Anarchism, but also traditional Jihadi-type terrorism, strengthened their online activities in radicalisation, spreading of ideologies, recruitment and preparation of violent actions. That resulted in a new legal response of the EU – April 2021 Council of the EU and European Parliament adopted Regulation on preventing the dissemination of terrorist content online as a main legal document for prevention of growing terrorism threat in virtual space.

At the end, it should be mentioned that terrorism threat was the main trigger for development of various legal documents in the area of EU's internal security, primarily focused on the other security areas. For example Directive of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, enabled creation and using of databases of air passengers in, out and within EU for purposes of prevention terrorism and serious crime. Changes of Schengen Borders Code enabled temporary reintroduction of border controls between EU Member States, Entry/Exit System Regulation, together with ETIAS Regulation established new mechanisms for control of entry, stay and exit of third nationals in EU as well as databases of personal data and biometrics of third nationals. All these legal developments were triggered by the rising threat of terrorism and violent extremism in the EU, but that is not the end of the list. Namely, there are few important proposals of the Council of European Union for new legal documents based on the growing terrorist threat such as proposals for new legislation in the area of Terrorism Financing, change mandate of Europol and European Public Prosecutor Office etc. That approach shows that terrorism and violent extremism threat in the EU, especially after 2020, is a growing challenge and effective base for legislation development.

CONCLUSION

The European Union as organisation sui generis is an area with 27 Member States, organised to enable economic prosperity, free movement of people and goods, to realise equal opportunities for all citizens is a challenging area for security issues. Growing terrorist threat in the EU has led to development of specific approaches in the fight against terrorism. EU agencies such as Europol, Eurojust, Frontex and Cepol play the main role in cooperation and exchange of information, as well as raising awareness and building national capacities of Member States' counter terrorism authorities.

The global COVID-19 pandemic and lockdowns developed new forms of violent extremist ideologies. New global insecurities such as war in Ukraine, conflict in Middle East, foreign political impact of certain third countries, global political polarisation impact on new global security paradigm. The EU as an important political player in the global world continued to develop its capacities on prevention and suppression of terrorism, violent extremism, protection of critical infrastructures, countering hybrid threats and many other security related areas, to ensure main principles of life in multi-state organisation of ~ 450 million of people.

This paper presents the current state of affairs regarding key indicators of terrorism trends in the European Union, academic reflections, and normative solutions for the prevention and suppression of terrorism since 2020. The goal is to provide an overview of the most important topics related to the prevention and suppression of terrorism within these three selected areas.

REFERENCES

Adibe, Emerka C. (2020), Towards a new approach to dealing with terrorism as an international crime. Journal of Law and Conflict Resolution, 11(2), pp. 33-43, https://academicjournals.org/journal/JLCR/article-full-text/894F78A65734

Bergström, Maria (2024), The EU's Fight against Money Laundering and Terrorist Financing in a Digital and Fragmented World. In: The Borders of the European Union in a Conflictual World: Interdisciplinary European Studies, pp. 177-203. Cham: Springer Nature Switzerland. https://library.oapen.org/bitstream/handle/20.500.12657/90425/1/978-3-031-54200-8.pdf#page=184

Bieber, Florian; Pollozhani, Lura (2021), Compared perspectives on radicalisation and violent extremism in MENA, the Balkans and the European Union. In: Torrekens, C., & de le Vingne, D., Perspectives on radicalisation and violent extremism in MENA, the Balkans and the European Union. Perspectives, 3, 3., https://h2020connekt.eu/wp-content/uploads/2021/05/D3.3-Regional-Report-compressed.pdf

Bureš, Oldřich (2023), EU Measures to Combat Terrorist Financing. In: Romaniuk, S. N., Kaunert, C., & Fabe, A. P. H. (Eds.), Countering Terrorist and Criminal Financing: Theory and Practice (1st ed.). CRC Press. Boca Raton: Routledge.

Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0475

Counter-Terrorism Agenda for the EU, https://home-affairs.ec.europa.eu/document/download/9b54c533-139a-4662-99cf-b5f72220bb18_en?file-name=09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf

Counter-Terrorism Strategy of the EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33275

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, https://eur-lex.europa.eu/eli/dir/2016/681/oj

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541&qid=1723869969422

Ejova, Cristina (2023), International political-legal regulation of cooperation for countering terrorism in Europe. Editura Universității din Oradea: Annals of the University of Oradea. International Relations and European Studies (RISE), No. 15, Year 2023, pp. 259-270, https://www.ceeol.com/search/article-detail?id=1211564

Europol (2023), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

Europol (2022), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

Hermida, Ágata M. S. (2020), The Fight Against Money Laundering Through Criminal Law in the European Union. Journal of Applied Business and Economics, 22(3), https://articlearchives.co/index.php/JABE/article/view/951

Kazansky, P. Rastislav, Rysova, P. Lucia & Mijoč, M. Nina (2021), Practical and Epistemological Basis for Research into the Security Threats of Terrorism and Radicalization in the Online Space. SAFE AND SECURE SOCIETY, 77-87, http://icsss.eu/wp-content/uploads/2021/12/Bezpecna_spolecnost_2021_proceedings.pdf#page=77

Kuhinja, Emina (2020), Justice, Freedom and Security? Analyzing the Counter-Terrorism Efforts of Western Balkan States towards EU Accession, University of Sarajevo: Sarajevo Social Science Review, No 2, Year 2020, page 79-99, https://www.ceeol.com/search/article-detail?id=962459

Magyar Rendészet: A Nemzeti Közszolgálati Egyetem Rendészettudományi Szakmai Folyóirata, 22(1), 65-78, https://real.mtak.hu/142699/1/04-pek-65-78-mr-2022-1.pdf

Matyasik, Michał (2023), Counter-Terrorism Financing Activities Introduced by the Council of Europe and the Organisation for Security and Cooperation in Europe. In: Romaniuk, S. N., Kaunert, C., & Fabe, A. P. H. (Eds.), Countering Terrorist and Criminal Financing: Theory and Practice (1st ed.). CRC Press. Boca Raton: Routledge.

McCloud, Victoria H. (2023), Social Media Intelligence to Combat Extremist and Terrorist Support. In: Romaniuk, S. N., Kaunert, C., & Fabe, A. P. H. (Eds.), Countering Terrorist and Criminal Financing: Theory and Practice (1st ed.). CRC Press. Boca Raton: Routledge.

Pék, Tamás (2022), Overview of the Definitions of Terrorism in International Criminal Law

Regulation on preventing the dissemination of terrorist content online, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32021R0784

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2226

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, https://eur-lex.europa.eu/eli/reg/2018/1240/oj

Sachetti, Viviana (2021), The EU Response to Terrorist Content Online: Too Little, (Maybe not) Too Late?, European Papers, Vol. 6, No 2, pp. 967-986, https://www.europeanpapers.eu/it/system/files/pdf_version/EP_eJ_2021_2_14_Articles_SS2_1_Viviana_Sachetti_00509.pdf

Savilaakso, Mira (2021), EU Countering Terrorism through Asylum Law: Serious Reasons to Exclude Members of Terrorist Organisations from Refugee Status Due to Their Participation in Acts Contrary to the Purposes and Principles of the UN, Åbo Akademi University, https://urn.fi/URN:NBN:fi-fe2021062840262

Security Union Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605

Terenghi, Fiamma (2023), Drug Trafficking and Terrorism Financing. In: Romaniuk, S. N., Kaunert, C., & Fabe, A. P. H. (Eds.), Countering Terrorist and Criminal Financing: Theory and Practice (1st ed.). CRC Press. Boca Raton: Routledge.

Zarychta-Romanowska, Kamila (2023), Creating an EU “Homeland Security”. In: Romaniuk, S. N., Kaunert, C., & Fabe, A. P. H. (Eds.), Countering Terrorist and Criminal Financing: Theory and Practice (1st ed.). CRC Press. Boca Raton: Routledge.

RETIRED AND DANGEROUS: WHY VETERANS JOIN ANTI-GOVERNMENT EXTREMIST GROUPS IN THE UNITED STATES?

Siti Hajar binti Roslan

ABSTRACT

Anti-government (AG) far-right extremist groups' have been involved in criminal and extremist acts in the United States (U.S.), including playing a significant role in the Capitol Insurrection on 6th January 2021. Their capabilities were widely contributed by having veterans as group members to increase their skills and efficiency. However, most reports on radicalisation factors often focused on soldiers instead of veterans and are not specific to particular extremist groups. Therefore, this paper centres on the factors behind veterans radicalisation and decision to join AG groups, specifically the Oath Keepers (OK) and the Three Percenters (III%), with an analysis on experiences faced throughout their military career as potential radicalisation factors.

Six (6) factors were discovered including (1) Adherent individuals with existing connections to the AG movement, join the military for the experience to support the movement's cause; (2) The military culture of valorising hyper-masculine, elitism, and the normalisation of 'othering' cemented veterans' extremist beliefs; (3) Veterans experienced crisis during active-duty adopted AG ideology and join AG groups to support their grievances; (4) The AG groups organise attractive activities that appeal to veterans' and offer them important roles in the group which makes them feel valued; (5) Veterans join the AG groups for personal gains; and (6) The AG groups provide support to veterans facing re-assimilation challenges into civilian life. These findings can facilitate preventive and deradicalisation efforts because even a small number of veterans involved could lead to dangerous extremist attacks.

Keywords: Far-right movement, extremism, radicalisation, The Oath Keepers, The Three Percenters, veterans

INTRODUCTION

Anti-government (AG) groups from the far-right movement in the United States (U.S) are known for their strong anti-democratic beliefs and distrust toward the Federal Government (FG). They have manifested it into numerous extremist attacks that goes from the 1995 Oklahoma City Bombing, shootings, stand-offs, various criminal activities, and the January 2021 Capitol Insurrection.

Out of the 700 people charged with the Insurrection, more than 31 affiliated were soldiers and

veterans from AG groups including the Oath Keepers (OK) and the Three Percenters (III%). Their involvement contributed in planning strategies of infiltration, provision of weapons and carrying out the attack (CISAC, 2022; Clifford and Lewis, 2022a; Moskalenko, 2021; SPLC, 2022a).

It is reported that within the 38,000 members of the OK (ADL 2022a; CISAC, 2022; SPLC, 2022a) and 10,000 members of the III% (NLI, 2022; SPLC, 2022c, 2022a), a large percentage of the members were individuals with military background, mainly veterans. Could this mean that veterans are far more susceptible to radicalisation? What could be the factors behind this issue that lead them to be radicalised, joining extremist groups and eventually carry out violent attacks?

ROAD TO RADICALISATION

The radicalisation process requires three (3) components; a vulnerable alienated individual, a legitimising ideology and an enabling community (Jackson, 2016; Southers, 2013; Valeri et al., 2018). Yet personal and social factors are required to become catalysts that pushes individuals from just harbouring alternative ideologies, into doing the extremist acts (Horgan, 2005; Stout, 2004; Van Assche, 2009).

In the context of this paper, a vulnerable veteran may begin identifying with extremist ideologies to explain their alienation in their community and other grievances. They experienced moments of crisis that lead to ‘cognitive opening’, making them more receptive to extremist ideologies and believing them to be legitimate. The process may take place throughout a Soldier's Life Cycle (SLC) from recruitment, active-duty and the End of Active Service or retirement phase (Haugstvedt et al., 2021; Walleman et al., 2014). Once retired, these veterans find a like-minded community that sustains these beliefs. With strong in-group and out-group practices involved, it promotes the sanctioning of hostile acts against those they consider ‘others’.

Yet, reports on veterans’ radicalisation often focus at the retirement phase with poor social mobility, unemployment, difficulties re-assimilating, exposure to misinformation and previous criminal involvement being the factors (Ellenberg, 2023; Hall, 2023; Haugstvedt et al., 2021; Moskalenko, 2021; Schager, 2023). The scope of analysis should be expanded in seeing the possibility of radicalisation occurring at any point in the veteran’s SLC with the possibility of military identity, norms and beliefs being the crucial factors (Bryman, 2016; Devetak et al., 2022; Guzzini, 2016; Sarantakos, 2012).

RADICALISATION OF VETERANS

This paper focuses on analysing **the factors behind veterans’ radicalisation and the decision to join AG groups mainly the Oath Keepers (OK) and the Three Percenters (III**%). The analysis comes from reports of **62 military veterans** and factors behind their involvement with the two specific AG groups. **33 veterans were named**, **while 29 remained anonymous and**

labelled as Veterans (V). List of veterans as per Appendix.

Through Process-Tracing method, six (6) factors were discovered which linked Cause (A); Veterans exposed to personal and social radicalisation factors throughout SLC, to the Outcome (B); Veterans being radicalised and join the AG groups (Beach, 2017; Beach and Pedersen, 2019; Collier, 2011; Punton and Welle, 2015; Roslan, 2023). The factors are illustrated in the following diagram:

<table>
<tr><td rowspan="2">Cause (A)</td><td colspan="4">Soldier Life Cycle (SLC)</td><td rowspan="2">Outcome (B)</td></tr>
<tr><td>Recruitment</td><td>Active-Duty</td><td colspan="2">End of Active Service/ Retirement</td></tr>
<tr><td colspan="6">Radicalisation Factors</td></tr>
<tr><td>Veterans exposed to personal and social radicalisa-tion factors throughout SLC</td><td>(1) Adherent individuals with existing connections to the AG movement, join the military for the experience to support the movement’s cause</td><td>(2) The military culture of valorising hyper-masculine, elitism, and the normalisation of ‘othering’ cemented veterans’ extremist beliefs

(3) Veterans experienced crisis during active-duty adopted AG ideology and join AG groups to support their grievances</td><td>(4) The AG groups organise attractive activities that appeal to veterans’ and offer them important roles in the group which makes them feel valued</td><td>(5) Veterans join the AG groups for personal gains

(6) The AG groups provide support to veterans facing re-assimilation challenges into civilian life</td><td>Veterans being radicalised and join the AG groups</td></tr>
</table>

Figure 1: Factors on veterans’ radicalisation

Factor 1: Adherent individuals with existing connections to the AG movement, join the military for the experience to support the movement's cause

Family members, peers, and communities are people's Primary Social Groups (PSG). In the context of radicalisation, PSG's discourses facilitated in shaping an adherent individual's worldview and if the narrative contains extremist beliefs, it will be planted early in the individual's lives. For the AG movement, PSG could also be facilitated in pushing them to join the military as a means to achieve the movement's goals.

Small American communities in other far-right movements were reported to have engaged in militiatia-like activities and adult figures have pushed their beliefs into the younger generation with the aim to continue the movement (Southwell, 2018). In order to remain in the in-group, adherent individuals would align themselves with that belief which increases the risk of continuation in extremism (Carson et al., 2019). Their recruitment into the military is often successful as they do not consider themselves as 'anti-government' extremists or hold any anti-American beliefs. They see themselves as protectors of the country and the Constitution (Ellenberg et al., 2023).

Veteran 1 (V1) from the OK stated his family highly regards his recruitment into the military and often discussed how his learned skills would benefit the AG movement (BRADY, 2021).

Exposure to extremist content also radicalised adherent individuals and influenced them to join the military. Spokespersons including Alex Jones, Infowars and the WorldNetDaily (Cooper, 2022; Krepel, 2010) played with followers' concerns and grievances such as migration issues, guns control and New World Order (NWO) conspiracies causing viewers to develop anti-establishment beliefs (Simi et al., 2013; SPLC, 2022a). The III% founder and leaders, Charles Dryer (ADL, 2022a; Neiwert, 2022) and Chris (C.) Hill (NYT, 2016) promoted AG ideology and spread the fear of gun control onto their online followers. Apart from boasting their previous military experience, they push followers to join the military for leadership, weapons, and strategic experience (CSIS, 2021; Jones, 2018).

Factor 2: The military culture of valorising hyper-masculine, elitism, and the normalisation of 'othering' cemented veterans' extremist beliefs

The military environment is often an overlooked enabling community and a crucial factor to veteran's radicalisation. To ensure the success of missions, the military is required to create high-group cohesion amongst soldiers. This is achieved through forming a collective identity, instilling camaraderie and group values as well as reducing internal dissent and empathy to outsiders (Koehler, 2022). As a soldier's own survival depends on being accepted in the in-group,

they have to align themselves with the dominant norms present.

With milieu-specific subculture including white hyper-masculine, elitism and dominant warrior culture present in an environment dominated by white men, the combination creates a dominant in-group with strong 'othering' values, suitable for the cultivation of various extremist beliefs and radicalisation of adherent individuals (EER, 2019; Haugstvedt and Koehler, 2021; Koehler, 2019). The insulative nature of the military environment also created echo chambers (Koehler, 2022; Youngblood, 2020) resulting in adherent individuals hearing only one extreme argument, causing cognitive rigidity and limiting the acceptance of alternative arguments.

Despite limited reports on veterans, as many as 12 Army soldiers, 6 Navy, 4 Marines, 4 Air Force and 2 National Guards (ADL, 2022b) were reported to have contacted the AG groups and offered to spread AG ideology in the camps to their peers and subordinates (ADL, 2022b; The Atlantic, 2020).

Factor 3: Veterans experienced crisis during active-duty adopted AG ideology and join AG groups to support their grievances

Veterans experienced a higher-than-average level of exposure to crisis and stressors during active-duty including internal crises, long-exposure to violence and unsuccessful career development. These become crucial factors towards radicalisation.

Elections of President Barack Obama, who was African-American (ACLED, 2020; Hedges, 2021; Furtunato, 2022) and President Joseph Biden, whom adherent individuals believed stole the election (Gutman, 2021; Lokay et al., 2021; SPLC, 2022b) were reported to cause internal crisis in soldiers. These events pushed soldiers to adopt AG ideology where they believe the movement's interpretation of the Constitution are more legitimate and the FG were beginning to issue unconstitutional orders alongside left-wing groups allies that will usher in a NWO (ADL, 2022b; HSToday, 2022; Kempert, 2021; The Atlantic, 2020). However, these soldiers were able to serve 'two-masters' as they have the vocation to protect their interpretation of the Constitution all the while resenting the unfavourable President (ADN, 2021).

This was reported by veterans from the OK include McDaniel (Abdollah, 2021), Eastman (TWP, 2022), V2, V3 and V6 (ADL, 2022b).

Veterans who experienced trauma from deployment to war zones were desensitised towards violence and more vulnerable towards radicalisation. U.S.-led wars such as Vietnam, Afghanistan and Iraq have caused many deaths and warranted torture and human rights abuse by American soldiers (ADN, 2021; Clifford and Lewis, 2022a; CSIS, 2021; NYT, 2022; GWU, 2021). Veterans

see the FG as the culprit behind their grievances and overwhelming xenophobic beliefs were developed during deployment (Perliger, 2020).

These were shown by V4 from the III% (Hedges, 2021) and V22, V23, and V24 from the OK (ADL, 2022b).

Unsuccessful career development in the military had also contributed to radicalising veterans. Joining the military is considered very patriotic and valorised. However, soldiers who did not experience a 'heroic' deployment, discharged or were given an underwhelming post created a crisis within them as it clashes with their expectation of becoming a war hero. This left them feeling embarrassed, and experienced a loss of identity and purpose. Veterans then searched for alternative places to reclaim the military career lost and aimed to serve in a similar way (Simi et al., 2013; Simi et al., 2016; SPLC, 2021a).

Watkins of the OK, (AXIOS, 2022) was discharged from the military for being a transgender. She joined the OK to reclaim her military identity that was lost and was given the opportunity to lead her own Chapter.

Factor 4: The AG groups organise attractive activities that appeal to veterans' and offer them important roles in the group which makes them feel valued

Veterans' bond through shared experiences and their career have shaped them to be more inclined in being leaders or engaging in volunteerism. Being involved in a familiar environment created by the AG groups makes them feel good and the opportunity given to share their skills and experience makes them feel valued. They also chose to remain as it satisfies their need to be alongside other veterans since retiring from the military.

Veterans are attracted to AG groups for the military-like experience or activities organised which reminisce their former military life. Training includes reconnaissance, tactical, firearms and ammunition, emergency drills, survival skill and camping (CSIS, 2021; Hedges, 2021; Lokay et al., 2021; Milton and Mines, 2021; NYT, 2016; Perliger, 2021) and natural disaster drills including fires, floods, food shortages, economic collapse, radio outage and medical emergencies (Teirstein, 2023). This was evident in the military-like formations and tactics used during the Capitol Insurrection including 'stack' formation to breach the building, 'reconnaissance' at Washington prior to the attack and the preparation of 'Quick Reaction Force' for after the attack (TWP, 2022).

Veterans from the OK, Arroyo (Teirstein, 2023) established the Arizona chapter and organised regional community service programmes, Young (CBS, 2021a; POLITICO, 2022) joined for

community service activities and Whitehead (The Guardian, 2021) joined to become ‘community protector’ alongside local authorities. Veterans from the III%, Kosin (Gutman, 2021) were involved in the group’s disaster response efforts and V5 (HCVA, 2021) for firearms and survival outings.

Some veterans joined AG groups because they were offered leadership or other significant roles including chapter leaders, management or instructors (Abdollah, 2021; Crump, 2016; Ellenberg et al., 2023; Lokay et al., 2021; McQueen, 202). This puts them in a higher status than others and being treated as icons of valour and patriotism satisfies the ‘war hero’ imagery that was unachievable during active-duty (Simi et al. 2013).

Veterans include Rhodes, Caldwell, Watkins, Schaffer, Arroyo and Master Sergeant Selph from the OK (CBS, 2021b; Ellenberg et al., 2023; Teirstein, 2023) and C. Hill, Chappell, Seddon and Kosin from the III% (Crump, 2016; NYT, 2020; Hedges, 2021) were some of the group's founders, chapter leaders or instructors.

Factor 5: Veterans join the AG groups for personal gains

Veterans join AG groups for their personal gains including regaining the sense of camaraderie and purpose lost, having a platform to express their AG ideologies and having opportunities to extend their military career.

The military values instilled and the soldier identity formed remained even when retired. The close social interactions and high level of trust experienced were difficult to be replicated in normal society and veterans feel that civilians struggle to understand their experience while serving in the military (Gutman, 2021; HCVA, 2021; HSToday, 2022; ICSVE, 2021; Milton et al., 2021). This created the desire to connect (Milton et al., 2021) with people that have a similar level of understanding as them, in this case, the AG groups. By joining, veterans can reconnect with their previous soldier life, re-established a sense of purpose, identity, and camaraderie, and engage in the habitus of military lifestyle including routine, structures, and the use of familiar jargon (Gutman, 2021; Lane, 2022).

Kosin and V7 from the III% (Gutman, 2021), and Courtney (TWP, 2021) and Dana (Abdollah, 2021) from the OK have expressed these reasons.

Some veterans view AG groups as a platform to express their beliefs. Involvement as veterans was the safer option as they were not tied to any military regulations and logistical hurdles of deployment (Milton and Mines, 2021; Perliger, 2021). Some of the AG ideologies motivating them as follow:

a. The FG was illegitimate with the election of Obama and Biden. This was expressed by Durfee (NYT, 2021a), Caldwell, James, Crowl, Harrelson, Rhodes (ICSVE, 2023), and V9 (ADL, 2022b) from the OK and Gieswein (NYT, 2021b), Seddon (Hedges, 2021), Brock (Perliger, 2021), C. Hill (NYT, 2016), Hostetter and Taylor (TWP, 2021a) from the III%

b. AG beliefs including upholding the Constitution, preventing gun control legislation, opposing policies that reduce civil liberties, protecting the country from domestic and foreign influence, and preventing the influx of immigrants into the country (ADL, 2022a; CBS17, 2018; ICSVE, 2023; Jones, 2018; Kempert, 2021; NYT, 2016; Perliger, 2020).

   This was shown by Dolan (Reuters, 2021), V13, V15, V16, V17, V24, and V25 from the OK (ADL, 2022b) and Kaleb (K.) Hill (Crump, 2016), Bemis (CBS17, 2018), Ritz heimer (TWP, 2021b) and Mosher (Hedges, 2021) from the III%

c. Conspiracy theories including the impending Martial Law (Lokay et al., 2021), the rise of leftist groups and global cabals (McQueen, 2021; The Atlantic, 2020), invasion by the United Nations (UN) into the U.S. (ADL, 2022a) and the impact of teaching critical race theory in public schools (SPLC, 2022b).

   This was shown by Sen. Rogers (Lokay et al., 2021), Hedges (The Guardian, 2021), V12 (ADL, 2022b) from the OK and Chappell (Crump, 2016) from the III%

In addition, veterans join AG groups as an extension to their military career (HCVA, 2021; SPLC, 2021b). The human capital learned in the military remains even after retiring and it is a challenge to channel them into other endeavours (Hall, 2021). Most civilian work does not require infantry skills and those who were hired by private military companies were often former higher-ranking soldiers (Ellenberg, 2023; Hall, 2023). Veterans turn to AG groups that would appreciate their capabilities.

V8, V10, V14, V18, V19, V20 and V21 from the OK have offered organisational, tactical, strategic, logistic, weapons, interrogation, SWAT tactics, survival, vehicle, tank, and helicopter operator, and recruitment skills (The Guardian, 2021; ADL, 2022b) to help achieve the group's goals.

Factor 6: The AG groups provide support to veterans facing reassimilation challenges into civilian life

Civilian society struggles to understand the veteran experience and the latter may need a 'special community' where they can express their emotions and opinions freely. As a large percentage of

AG group members are individuals with military background, they provided emotional and moral support needed by the veterans. This makes the connection on grievances and reassimilation challenges more relatable and easier for them.

From combat-related traumas, social anxiety, survivor's guilt, identity losses, physical injuries, and disabilities (Hall, 2023; Koehler, 2022; Lane, 2022; Milton and Mines, 2021), these issues have caused 'bad transition' to veterans (ICSVE, 2023). The norms practised by the groups created an environment that could assuage veterans' hyper-reactivity and hyper-vigilance by having an appearance military-like characteristics. Group members were comfortable with violence and practise other norms such as drinking which helps them to subdue their trauma and relate to being in a constant state of combat mode (ICSVE, 2023).

In addition, veterans returning from morally damaging deployment or U.S.-led wars such as war in Vietnam, Iraq and Afghanistan experienced difficulties re-assimilating back into society. They go through social stressors for being involved (Simi et al., 2013) and developed strong belief on being abandoned by the FG (ICSVE, 2021; SPLC, 2021b). Hence, they turn to AG groups for moral support.

Veterans involved included Turner (NYT, 2022), V27 (The Atlantic, 2020), V28, V11 and V29 (Gutman, 2021) from the OK and V26 from the III% (Lane, 2022).

Retired and Extremely Dangerous

The factors discovered shows that exposure towards personal and social radicalisation factors throughout SLC have contributed to veterans' radicalisation and caused them to join the AG groups. The environment and situations they were exposed to throughout their career as soldiers have increased their susceptibility to radicalisation, instead of it happening mostly during retirement. By understanding how the process of becoming a soldier affected veterans' character, perception, beliefs, and needs, it helps us understand why the AG movement is appealing to them. These findings can facilitate in preventive and deradicalisation efforts as even a small number of veterans involved could lead to dangerous extremist attacks.

List of Veterans in the Anti-Government (AG) Extremist Groups

No.	Veteran	Group Affiliation	Causes (C)
1.	Alan Hostetter	* III%	4
2.	Andrew Turner	**OK	4
3.	Charles Dryer	III%	1
4.	Chris Hedges	OK	4
5.	Chris Hill	III%	1, 3
6.	Courtney (no known last name)	OK	4
7.	David Eastman	OK	2
8.	Dominic Chappell	III%	3
9.	Donovan Crowl	OK	4
10.	Edward Durfee Jr.	OK	4
11.	Graydon Young	OK	3
12.	James Dana	OK	4
13.	Jason Dolan	OK	4
14.	Jessica Watkins	OK	2, 3
15.	Jim Arroyo	OK	3
16.	Jon Ritzheimer	III%	3
17.	Jon Ryan Schaffer	OK	4
18.	Joshua James	OK	4
19.	Kaleb Hill	III%	4
20.	Kenneth Harrelson	OK	4
21.	Larry Brock	III%	4
22.	Master Sergeant Andrew Holloway Selph	OK	3
23.	Michael Mosher	III%	4
24.	Phillip Whitehead	OK	3
25.	Robert Gieswein	III%	4
26.	Russell Taylor	III%	4
27.	Scott McDaniel	OK	2
28.	Scott Seddon	III%	3
29.	Sen. Wendy Rogers	OK	4
30.	Stewart Rhodes	OK	3
31.	Theodore Kosin	III%	3
32.	Thomas Caldwell	OK	3
33.	Wade Bemis	III%	4
34.	***V1	OK	1
35.	V2	OK	2

36.	V3	OK	2
37.	V4	III%	2
38.	V5	III%	3
39.	V6	OK	3
40.	V7	III%	4
41.	V8	OK	4
42.	V9	OK	4
43.	V10	OK	4
44.	V11	OK	4
45.	V12	OK	4
46.	V13	OK	4
47.	V14	OK	4
48.	V15	OK	4
49.	V16	OK	4
50.	V17	OK	4
51.	V18	OK	4
52.	V19	OK	4
53.	V20	OK	4
54.	V21	OK	4
55.	V22	OK	2
56.	V23	OK	2
57.	V24	OK	2
58.	V25	OK	4
59.	V26	III%	4
60.	V27	OK	4
61.	V28	OK	4
62.	V29	OK	4

Notes:
*The Three Percenters (III%)
**The Oath Keepers (OK)
*** Veterans (V)

REFERENCES

Abdollah, T. (2021) They were trusted to train law enforcement officers, but they were members of an anti-government militia group, USA Today News. Available at: https://eu.usatoday.com/story/news/2021/11/04/oath-keepers-hack-includes-police-trainers-membership-list/8576919002/ (Accessed: 2 August 2023).

ACLED (2020) Standing By: Right-Wing Militia Groups and the United States Election, ACLED. Available at: https://acleddata.com/acleddatanew/wp-content/uploads/2020/10/ACLEDMilitiaWatch_StandingByMilitiaGroups_2020Web.pdf (Accessed: 2 August 2023).

ADL (2022a) The Oath Keepers, Anti-Defamation League (ADL). Available at: https://www.adl.org/resources/backgrounder/oath-keepers (Accessed: 20 June 2023).

ADL (2022b) The Oath Keepers Data Leak: Unmasking Extremism in Public Life, Anti-Defamation League (ADL). Available at: https://www.adl.org/resources/report/oath-keepers-data-leak-unmasking-extremism-public-life (Accessed: 20 June 2023).

ADN (2021) 70 West Point alumni call on Wasilla Rep. David Eastman to resign, Anchorage Daily News (ADN). Available at: https://www.adn.com/politics/2021/11/22/70-west-point-alumni-call-on-rep-david-eastman-to-resign/ (Accessed: 2 August 2023).

AXIOS (2022) How the Oath Keepers were radicalised, AXIOS. Available at: https://www.axios.com/2022/11/30/oath-keepers-trial-radicalization (Accessed: 31 July 2023).

Beach, D. (2017) 'Process-Tracing Methods in Social Science', Oxford Research Encyclopaedia of Politics [Preprint]. Available at: https://doi.org/10.1093/ACREFORE/9780190228637.013.176.

Beach, D. and Pedersen, R.B. (2019) Process-Tracing Methods. Ann Arbor: University of Michigan Press.

Bryman, A. (2016) Social research methods. 5th ed. Oxford: Oxford University Press.

CBS (2021a) Oath Keeper becomes first to plead guilty to conspiracy in Capitol riot case, agrees to cooperate, CBS News. Available at: https://www.cbsnews.com/news/january-6-capitol-riot-graydon-young-oath-keeper-guilty-plea/ (Accessed: 12 July 2023).

CBS (2021b) Oath Keepers member first to plead guilty in Capitol riot, CBS News. Available at: https://www.cbsnews.com/news/jon-schaffer-iced-earth-oath-keepers-first-guilty-plea-capitol-riots/ (Accessed: 10 July 2023).

CBS17 (2018) Who are the Three Percenters?, CBS17. Available at: https://www.cbs17.com/news/local-news/orange-county-news/who-are-the-three-percenters/ (Accessed: 13 July 2023).

CISAC (2022) Oath Keepers, Center for International Security and Cooperation (CISAC). Available at: https://cisac.fsi.stanford.edu/mappingmilitants/profiles/oath-keepers (Accessed: 20 June 2023).

Clifford, B. and Lewis, J. (2022a) '"This is the Aftermath" Assessing Domestic Violent Extremism One Year After the Capitol Siege', Program on Extremism, The George Washington University [Preprint].

https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This%20is%20the%20Aftermath.pdf (Accessed: 30 November 2022).

Clifford, B. and Lewis, J. (2022b) '"This is the Aftermath" Assessing Domestic Violent Extremism One Year After the Capitol Siege', Program on Extremism, The George Washington University [Preprint]. Available at: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This%20is%20the%20Aftermath.pdf (Accessed: 30 November 2022).

Collier, D. (2011) 'Understanding Process Tracing', PS: Political Science & Politics, 44(4), pp. 823–830. Available at: https://doi.org/10.1017/S1049096511001429.

Cooper, A. (2022) How Alex Jones helped spread the Oath Keepers' message to millions, CNN. Available at: https://edition.cnn.com/videos/media/2022/01/15/stewart-rhodes-oath-keepers-alex-jones-griffin-ac360-pkg-vpx.cnn (Accessed: 31 July 2023).

Crump, J. (2016) We Interview The Three Percenters' Leaders on Bogus ALT Right Claims, Ammoland. Available at: https://www.ammoland.com/2016/12/interview-three-percenters-leaders/#axzz728KbjUlZ (Accessed: 13 July 2023).

CSIS (2021) Violent Domestic Extremist Groups and the Recruitment of Veterans, Center for Strategic & International Studies (CSIS). Available at: https://www.congress.gov/117/meeting/house/113968/witnesses/HHRG-117-VR00-Wstate-JonesS-20211013.pdf (Accessed: 31 July 2023).

Devetak, R. et al. (2022) Theories of international relations. Sixth edition. Edited by Richard Devetak, Jacqui True, and Scott Burchill. Red Globe Press.

EER (2019) An Interview with Daniel Koehler, German Institute on Radicalization and De-Radicalization Studies, European Eye on Radicalization (EER). Available at: https://eeradicalization.com/an-interview-with-daniel-koehler-german-institute-on-radicalization-and-de-radicalization-studies/ (Accessed: 12 May 2023).

Ellenberg, M. et al. (2023) Far-Right Violent Extremist Radicalization Among Veterans and Active-Duty Servicemembers by the Numbers, Homeland Security Today. Available at: https://www.hstoday.us/featured/perspective-far-right-violent-extremist-radicalization-among-veterans-and-active-duty-servicemembers-by-the-numbers/ (Accessed: 21 June 2023).

Furtunato, O. et al. (2022) 'Examining the Impact of the Obama and Trump Candidacies on Right-Wing Domestic Terrorism in the United States: A Time-Series Analysis', Interpret Violence, 37, pp. 23–24. Available at: https://pubmed.ncbi.nlm.nih.gov/35236192/ (Accessed: 2 August 2023).

Gutman, A. (2021) Filling the void: For some veterans, militias offer a misguided sense of purpose, Inquirer. Available at: https://www.inquirer.com/opinion/commentary/veterans-militias-military-extremism-qanon-20211209.html (Accessed: 2 August 2023).

Guzzini, S. (2016) 'A Reconstruction of Constructivism in International Relations', http://dx.doi.org.nottingham.idm.oclc.org/10.1177/1354066100006002001, 6(2), pp. 147–182. Available at: https://doi.org/10.1177/1354066100006002001.

Hall, A. (2023) Murder, the Military and Radicalization: How Much Is Tied to a Lack of Support for

Veterans?, KQED. Available at: https://www.kqed.org/news/11952237/murder-the-military-and-radicalization-how-much-is-tied-to-a-lack-of-support-for-veterans (Accessed: 21 June 2023).

Hall, A. et al. (2021) 'Militarized Extremism', The Independent Review, 26(2), pp. 225–242. Available at: https://doi.org/10.2307/48647351.

Haugstvedt, H. et al. (2021) 'Armed and Explosive? An Explorative Statistical Analysis of Extremist Radicalization Cases with Military Background', Terrorism and Political Violence, 35(3), pp. 518–532. Available at: https://doi.org/10.1080/09546553.2021.1957675.

HCVA (2021) 'Domestic Violent Extremist Groups and the Recruitment of Veterans', The Majority Staff of the House Committee on Veterans' Affairs (HCVA) [Preprint]. Available at: www.start.umd.edu/pubs/Final%20Report%20for%20SAF%20 (Accessed: 20 December 2022).

Hedges, C. (2021) Hedges: Why They Hate Us, Scheer Post. Available at: https://scheerpost.com/2021/01/18/hedges-why-they-hate-us/ (Accessed: 2 August 2023).

Horgan, J. (2005) The psychology of terrorism. London: Routledge (Cass series on political violence).

HSToday (2022) The Oath Keepers Wanted a Coup, Homeland Security Today (HSToday). Available at: https://www.hstoday.us/subject-matter-areas/counterterrorism/perspective-the-oath-keepers-wanted-a-coup/ (Accessed: 26 June 2023).

ICSVE (2021) The Challenge of Extremism in the Military Is Not Going Away Without a New Perspective, International Centre for the Study of Violent Extremism (ICSVE). Available at: https://www.icsve.org/the-challenge-of-extremism-in-the-military-is-not-going-away-without-a-new-perspective/ (Accessed: 26 June 2023).

Jackson, Richard, (2016) Routledge handbook of critical terrorism studies. Edited by Richard Jackson. Abingdon: Routledge.

Jones, S.G. (2018) 'The Rise of Far-Right Extremism in the United States', Center for Strategic & International Studies (CSIS) Briefs [Preprint]. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181119_RightWingTerrorism_layout_FINAL.pdf?MyC9DjLLRftoeUKvq6qxFPsCPFoTkBpH (Accessed: 2 December 2022).

Kempert, T. (2021) Who are the Oath Keepers, Three Percenters?, Daily Independence. Available at https://www.yourvalley.net/stories/kampert-who-are-the-oath-keepers-three-percenters,216873 (Accessed: 2 August 2023).

Koehler, D. (2019) 'A Threat from Within? Exploring the Link between the Extreme Right and the Military', International Centre for Counter-Terrorism (ICCT) [Preprint]. Available at: https://doi.org/10.19165/2019.2.06.

Koehler, D. (2022) 'From Superiority to Supremacy: Exploring the Vulnerability of Military and Police Special Forces to Extreme Right Radicalization', Studies in Conflict and Terrorism [Preprint]. Available at: https://doi.org/10.1080/1057610X.2022.2090047.

Krepel, T. (2010) WorldNetDaily Condones Child Abuse - Again, HuffPost. Available at: https://www.huffpost.com/entry/worldnetdaily-condones-ch_b_772923 (Accessed: 31 July 2023).

Lane, A. (2022) 'Military-member right-wing extremism-Overview of an emerging strategic threat', Defence Research and Development Canada (DRDC) [Preprint].

Lokay, A. et al. (2021) 'The Oath Keepers', Dynamics of Asymmetric Conflict, 14(2), pp. 160–178. Available at: https://doi.org/10.1080/17467586.2021.1912375.

McQueen, E. (2021) Examining Extremism: The Oath Keepers, Center for Strategic and International Studies (CSIS). Available at: https://www.csis.org/blogs/examining-extremism/examining-extremism-oath-keepers (Accessed: 1 December 2022).

Milton, D. and Mines, A. (2021) "This is War"- Examining Military Experience Among the Capitol Hill Siege Participants, Program on Extremism, The George Washington University. Available at: https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/This_is_War.pdf (Accessed: 3 August 2023).

Moskalenko, S. (2021) 'Zip-tie guys: military-grade radicalization among Capitol Hill insurrectionists', Dynamics of Asymmetric Conflict, 14(2), pp. 179–191. Available at: https://doi.org/10.1080/17467586.2021.1912374.

Neiwert, D. (2022) The rise and fall of 'July4Patriot' Charles Dyer, the Oath Keepers' original far-right celebrity, Daily Kos. Available at: https://www.dailykos.com/stories/2022/11/27/2137360/-The-rise-and-fall-of-July4Patriot-Charles-Dyer-the-Oath-Keepers-original-far-right-celebrity (Accessed: 31 July 2023).

NLI (2022) The Three Percenters: A Look Inside an Anti-Government Militia, New Lines Institute (NLI). Available at: https://newlinesinstitute.org/far-right-extremism/the-three-percenters-a-look-inside-an-anti-government-militia/ (Accessed: 20 June 2023).

NYT (2016) A Militia Gets Battle Ready for a 'Gun-Grabbing' Clinton Presidency, New York Times (NYT). Available at: https://www.nytimes.com/2016/11/05/us/a-militia-gets-battle-ready-for-a-gun-grabbing-clinton-presidency.html (Accessed: 31 July 2023).

NYT (2020) Veterans Fortify the Ranks of Militias Aligned With Trump's Views, The New York Times (NYT). Available at: https://www.nytimes.com/2020/09/11/us/politics/veterans-trump-protests-militias.html (Accessed: 13 July 2023).

NYT (2021a) An Oath Keeper Was at the Capitol Riot. On Tuesday, He's on the Ballot, The New York Times (NYT). Available at: https://www.nytimes.com/2021/10/27/nyregion/oath-keeper-nj-assembly.html (Accessed: 2 August 2023).

NYT (2021b) Investigators Eye Right-Wing Militias at Capitol Riot, The New York Times (NYT). Available at: https://www.nytimes.com/2021/01/18/us/politics/capitol-riot-militias.html (Accessed: 12 July 2023).

NYT (2022) Extremists in Uniform Put the Nation at Risk, The New York Times (NYT). Available

at:https://www.nytimes.com/2022/11/13/opinion/us-police-military-extremism.html#:~:text=Extremists%20bearing%20badges%20can%20put,to%20good%20order%20and%20discipline. (Accessed: 2 August 2023).

Perliger, A. (2020) American Zealots. New York: Columbia University Press. Available at: https://doi.org/10.7312/perl16710.

Perliger, A. (2021) Police, soldiers bring lethal skill to militia campaigns against US government, Yahoo!News. Available at: https://news.yahoo.com/police-soldiers-bring-lethal-skill-195348940.html? (Accessed: 3 August 2023).

POLITICO (2022) 'Sorry for what I did': Oath Keeper who pleaded guilty for Jan. 6 breach breaks down on the stand, POLITICO. Available at: https://www.politico.com/news/2022/10/31/graydon-young-oath-keeper-apology-00064287 (Accessed: 12 July 2023).

Punton, M. and Welle, K. (2015) 3 Process-Tracing Methods, Institute of Development Studies. Available at: https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/5997/CDIPracticePaper_10_Annex.pdf?sequence=2 (Accessed: 7 November 2022).

Reuters (2021) Florida Marine veteran and Oath Keeper pleads guilty in Jan. 6 riot, Reuters. Available at: https://www.reuters.com/legal/government/florida-oath-keepers-member-pleads-guilty-jan-6-capitol-riot-charges-2021-09-15/ (Accessed: 7 August 2023).

Roslan, H. (2023). Retired But Dangerous: Why Do Veterans Join Anti-Government Extremist Groups in the United States? [Postgraduate dissertation, University of Nottingham]. University of Nottingham Research Data Repository. https://rdmc.nottingham.ac.uk/

Sarantakos, S. (2012) Social Research. London, United Kingdom: Bloomsbury Publishing Plc. Available at: http://ebookcentral.proquest.com/lib/nottingham/detail.action?docID=4763630.

Schager, N. (2023) The Chilling Threat of Radicalized U.S. Military Vets, The Daily Beast. Available at: https://www.thedailybeast.com/against-all-enemies-review-the-chilling-threat-of-radicalized-military-vets (Accessed: 23 June 2023).

Simi, P., Bubolz, B.F. and Hardman, A. (2013) 'Military Experience, Identity Discrepancies, and Far Right Terrorism: An Exploratory Analysis', Studies in Conflict & Terrorism, 36(8), pp. 654–671. Available at: https://doi.org/10.1080/1057610X.2013.802976.

Simi, P. et al. (2016) 'Recruitment and Radicalization among US Far-Right Terrorists', National Consortium for the Study of Terrorism and Responses to Terrorism (START) [Preprint]. Available at: https://www.start.umd.edu/pubs/START_RecruitmentRadicalizationAmongUSFarRightTerrorists_Nov2016.pdf (Accessed: 20 June 2023).

Southers, E. (2013) Homegrown Violent Extremism. Taylor & Francis Group, London.

SPLC (2021a) Extremism Among Active-Duty Military and Veterans Remains a Clear and Present Danger, Southern Poverty Law Center (SPLC). Available at: https://www.splcenter.org/hatewatch/2021/10/12/extremism-among-active-duty-military-and-veterans-remains-clear-and-present-danger (Accessed: 20 June 2023).

SPLC (2021b) SPLC Action statement Veterans Affairs Committee, The Southern Poverty Law Center (SPLC). Available at: https://www.splcactionfund.org/sites/default/files/SPLC_Action_statement_Veterans_Affairs_Committee_hearing_on_Domestic_Violent_Extremist_Groups_and_the_Recruitment_of_Veterans_final.pdf (Accessed: 7 August 2023).

SPLC (2022a) Anti-government Movement, Southern Poverty Law Center (SPLC). Available at: https://www.splcenter.org/fighting-hate/extremist-files/ideology/antigovernment (Accessed: 25 March 2023).

SPLC (2022b) 'The Year in Hate & Extremism 2021', Southern Poverty Law Centre (SPLC) Available at: https://www.splcenter.org/20220309/year-hate-extremism-report-2021 (Accessed: 25 March 2023).

SPLC (2022c) Three Percenters, Southern Poverty Law Center (SPLC). Available at: https://www.splcenter.org/fighting-hate/extremist-files/group/three-percenters (Accessed: 20 June 2023).

Stout, C.E. (2004) Psychology of terrorism : coping with the continuing threat. Edited by C.E. Stout. Westport, Conn.; London: Praeger Publishers.

Teirstein, Z. (2023) When disaster strikes, far-right groups see an opportunity to gain trust, GRIST. Available at: https://grist.org/extreme-weather/boots-on-the-ground-fema-oath-keepers-natural-disaster/ (Accessed: 3 August 2023).

The Atlantic (2020) A Pro-Trump Militant Group Has Recruited Thousands Of Police, Soldiers, And Veterans, The Atlantic. Available at: https://www.theatlantic.com/magazine/archive/2020/11/right-wing-militias-civil-war/616473/ (Accessed: 2 August 2023).

The George Washington University (2021) '"This is Our House!"', Program on Extremism, The George Washington University [Preprint]. Available at: www.extremism.gwu.edu (Accessed: 30 November 2022).

The Guardian (2021) US militia group draws members from military and police, website leak shows, The Guardian. Available at: https://www.theguardian.com/us-news/2021/mar/03/us-militia-membership-military-police-american-patriot-three-percenter-website-leak (Accessed: 9 June 2023).

TWP (2021) Why veterans look at the Oregon occupation and see 'loose cannon clowns', The Washington Post (TWP). Available at: https://www.washingtonpost.com/news/checkpoint/wp/2016/01/06/why-veterans-look-at-the-oregon-occupation-and-see-loose-cannon-clowns/ (Accessed: 13 July 2023).

TWP (2022) We're training our own insurrectionists, The Washington Post (TWP). Available at: https://www.washingtonpost.com/outlook/2022/01/15/oath-keepers-stewart-rhodes-sedition/ (Accessed: 2 August 2023).

Valeri, R. and Borgeson, K. (2018) Terrorism in America. Terrorism in America (1st ed.). Routledge. Available at: https://doi.org/10.4324/9781315456010 (Accessed: 20 June 2023).

Van Assche, T. (2009) Review of The Mind of the Terrorist: The Psychology of Terrorism from

the IRA to Al-Qaeda, Political Psychology, 30(5), 835–837. Available at: http://www.jstor.org/stable/41502463 (Accessed: 19 August 2023).

Walleman, J. et al. (2014) Soldier Life Cycle changes way Army preps troops for eventual transition, The United States Army. Available at: https://www.army.mil/article/129757/soldier_life_cycle_changes_way_army_preps_troops_for_eventual_transition (Accessed: 20 June 2023).

Zimmerman, M. and Stevenson, F. (2055) 'A framework for understanding healthy development in the face of risk', Annual Review of Public Health, 26, pp. 399–419. Available at: http://nottingham.idm.oclc.org/login?url=https://www.proquest.com/scholarly-journals/adolescent-resilience-framework-understanding/docview/235233320/se-2 (Accessed: 14 August 2023).

ARTIFICIAL INTELLIGENCE: A GAME CHANGER IN THE FIGHT AGAINST TERRORISM?

Rasheka Mahendra and Sai Ganesh Laxmi Kant

ABSTRACT

Artificial Intelligence (AI) has become a pivotal element in modern security, significantly enhancing counter-terrorism efforts and global peace initiatives. This article delves into the dual-use nature of AI, exploring its transformative potential in detecting, preventing, and responding to terrorist threats, particularly through surveillance, cybersecurity, and autonomous weaponry. However, alongside these benefits, AI introduces significant risks, particularly when exploited by terrorist organisations for propaganda, recruitment, and cyber-attacks. The misuse of AI highlights the ethical and legal challenges associated with its deployment, raising concerns about privacy, surveillance, and the development of autonomous weapons. This article argues for a balanced approach to AI governance, emphasising the need for robust regulatory frameworks, ethical standards, and media responsibility to harness AI's positive contributions while mitigating its potential threats to global security.

Keywords: Artificial Intelligence, Counter-Terrorism, Cybersecurity, Autonomous Weapons, Surveillance

INTRODUCTION

Artificial Intelligence (AI) has rapidly evolved into a critical component across various sectors, significantly transforming industries like education, healthcare, entertainment, and scientific research. Generative AI, a subset of AI that can create new content, including text, images, and videos in response to prompts, has garnered particular attention for its potential to revolutionise how we interact with technology. However, alongside its many benefits, AI introduces new challenges and risks, especially in terms of ethical considerations and security concerns. One of the most pressing issues arising from the growth of AI is its potential exploitation by terrorist organisations. Terrorism, broadly defined as the unlawful use of violence and intimidation, especially against civilians, to achieve political, religious, or ideological objectives, has long involved the use of technology to enhance operational effectiveness. The recent advancements in AI, particularly in generative AI, have made this technology an attractive tool for terrorists, who may use it for various malicious purposes. This article explores the intersection of AI and terrorism, shedding light on how terrorist organisations might leverage AI for propaganda, recruitment, and other harmful activities. As AI becomes increasingly sophisticated, understanding its dual-use nature, both for beneficial and malicious purposes, is critical for policy-makers, security experts, and society at large. Discussing the potential risks and implications of

AI in the context of terrorism is essential to developing strategies that mitigate these threats while preserving the positive contributions AI can make to global progress.

AI has become an indispensable tool in modern counter-terrorism strategies, providing significant advancements in the detection, prevention, and response to potential threats. In the realm of surveillance and monitoring, AI systems analyse vast amounts of data from sources such as social media, CCTV footage, and communication networks to identify behaviour patterns that may indicate terrorist activities. These systems' ability to process data in real-time allows for the swift identification and assessment of potential threats, enabling authorities to intervene before an attack occurs. Furthermore, AI's continuous learning capability ensures that it becomes more adept at recognising new patterns over time, enhancing its effectiveness in preempting terrorist activities both in physical spaces and online. In the digital age, terrorism is not confined to physical spaces, but, cyber terrorism has become a significant threat. AI plays a crucial role in enhancing cybersecurity measures to protect against such attacks. AI-driven systems can detect and respond to cyber threats much faster than human analysts. By recognising patterns associated with cyber-attacks, such as unusual login attempts or data breaches, AI can quickly identify and neutralise threats before they cause significant damage. The role of AI in cybersecurity extends to protecting critical infrastructure, such as power grids, financial systems, and communication networks, which are often targeted by terrorists aiming to cause widespread disruption. Additionally, AI is being used to develop more secure encryption methods, making it harder for terrorists to exploit digital vulnerabilities. As cyber threats evolve, AI's ability to adapt and respond to new challenges will be essential in maintaining cybersecurity and protecting against terrorist activities in the digital realm.

Facial recognition and biometric technologies further bolster counter-terrorism efforts by identifying and tracking terrorists. AI-driven tools scan and compare faces against extensive databases of known terrorists and suspects, enabling swift identification in high-security areas like airports and borders. Biometric data, such as fingerprints and iris scans, are analysed with remarkable accuracy, even in challenging conditions. These technologies are not only reactive but also proactive, tracking suspects' movements across locations and predicting their next moves based on behaviour patterns. This proactive capability is particularly valuable in tracking individuals within terrorist networks who frequently use false identities to evade capture. The integration of AI in these domains significantly increases the speed and accuracy of identifying potential threats, making it a vital asset in counter-terrorism strategies. Terrorist organisations have increasingly leveraged AI technology to advance their agendas, employing it in ways that raise significant security, ethical, and legal concerns. Terrorist organisations such as ISIS and Al-Qaeda have used AI to amplify their recruitment and propaganda efforts. By understanding and exploiting social media algorithms, ISIS has been able to spread its message to a broader audience, optimising content to create viral propaganda tailored to specific demographics.

Automated bots are another AI-driven tool in their arsenal, allowing them to flood social media platforms with content, maintain visibility, and engage with potential recruits. Al-Qaeda has similarly utilised AI in media production, creating polished and psychologically impactful videos designed to recruit and radicalise individuals more effectively. Hamas has also reportedly used AI to analyse social media trends, enabling them to craft messages that resonate with specific populations and adjust their strategies in real-time.

The potential for terrorist organisations to develop and deploy autonomous weapons is a growing concern in the field of counter-terrorism. AI could be potentially used to create autonomous drones, robotic soldiers, or other weapons that operate without direct human control. These technologies pose a significant threat due to their ability to execute attacks with precision and at scale. The implications of such developments are dire, as they could lead to more frequent and devastating terrorist attacks without the need for human operatives on the ground. AI is also a powerful tool for conducting sophisticated cyber-attacks, which have become a significant aspect of modern terrorism. Organisations like Hezbollah have engaged in cyber warfare activities that include using AI-driven tools to spread disinformation and manipulate media through techniques like deepfakes. These tools enable terrorists to undermine trust in information and create confusion, which can have far-reaching consequences for national security. The ability of AI to automate and enhance hacking techniques allows terrorists to carry out cyber-attacks with greater efficiency and anonymity, targeting critical infrastructure and causing widespread disruption.

However, the use of AI in counter-terrorism also raises important ethical and legal questions, particularly concerning privacy and surveillance. The deployment of AI for monitoring and identifying terrorist activities often involves collecting and analysing vast amounts of personal data, which can infringe on individual privacy rights. Moreover, the legal frameworks governing the use of AI in counter-terrorism are still evolving, leading to challenges in ensuring that these technologies are used responsibly and within the bounds of the law. There is a pressing need for clear regulations and oversight mechanisms to address these concerns and prevent abuses of AI in the name of security. The real-world application of AI in counter-terrorism has seen both successes and limitations. For example, AI has been instrumental in identifying and neutralising terrorist threats through advanced surveillance and predictive analytics. However, there have also been instances where AI failed to prevent attacks or was misused, leading to unintended consequences. These examples underscore the need for continuous evaluation and improvement of AI technologies to ensure they are effective and ethical tools in the fight against terrorism. In this modernised era, AI represents a transformative change in society, global security, and peacebuilding. AI operates at the intersection of data-driven analysis, predictive modelling, and strategic decision-making. Beyond mere automation, AI enables nuanced understanding and anticipatory actions in global geopolitical landscapes. AI’s advanced

algorithms can sift through vast datasets, identifying subtle patterns and early warning signs of conflict, thus enabling preemptive diplomatic interventions. For instance, the United States Department of Defense has utilised AI for global peace regulation and threat detection.

In peace negotiations, AI can serve as a neutral arbitrator by providing proposals and counterproposals to foster more equitable outcomes. Additionally, AI enhances the effectiveness of humanitarian efforts by optimising resource allocation, ensuring aid distribution is both timely and contextually appropriate. However, the deployment of AI in global peace initiatives necessitates a rigorous ethical framework to prevent misuse, which could inadvertently reinforce systemic inequalities or provoke new conflicts. AI's role in the fight against terrorism extends to enhancing the ability to detect, analyse, and respond to threats with unprecedented precision. AI-driven tools process and analyse vast amounts of data from various sources, including social media, communication networks, and financial transactions, to identify patterns indicative of terrorist activity. These systems can predict potential threats, track the movement of terrorist cells, and even disrupt online recruitment and propaganda efforts by detecting extremist content in real-time. AI's capabilities also extend to the battlefield, where it is used for counter-terrorism operations, such as drone surveillance, targeting, and neutralising threats with minimal collateral damage.

Nevertheless, the misuse of AI in daily activities, such as propagandas, can be highly disruptive to global peace and security. Propaganda, often disseminated by extremist groups, can include misleading information that jeopardises global peace. AI plays a crucial role in this by generating pictures, slogans, and information that appear realistic but are false and misleading. The affordability and accessibility of AI make it a powerful tool for such malicious purposes, necessitating stricter regulations. Algorithms and data mining have become powerful tools that, when combined with AI, can significantly impact global security in troubling ways. AI-driven algorithms can analyse vast amounts of data to identify patterns and predict potential threats with unprecedented accuracy. However, this capability can also be weaponised to create sophisticated cyber-attacks. For example, malicious actors can use AI to exploit vulnerabilities in critical infrastructure, launch coordinated cyber espionage campaigns, and manipulate public opinion through targeted disinformation campaigns. These threats are amplified by AI's ability to continuously learn and adapt, making it difficult for traditional security measures to keep pace. Data mining techniques, when applied with AI, can also jeopardise global security by enabling the collection and exploitation of sensitive information. By sifting through enormous databases, AI can uncover personal information and behavioural patterns that can be used for blackmail, coercion, or other forms of manipulation. Social media platforms like Instagram and TikTok are notable examples where data mining and algorithms have raised concerns about privacy and security. In the wrong hands, this capability can destabilise political systems and cause economic instability.

The integration of AI into modern weaponry has revolutionised warfare by enhancing the precision and effectiveness of drones and missiles. Autonomous drones equipped with AI algorithms can conduct surveillance, reconnaissance, and targeted strikes with minimal human oversight. These drones use machine learning to analyse data from sensors and cameras, allowing them to identify and engage targets with high accuracy. AI-enabled drones can operate in complex environments, making real-time decisions to avoid obstacles, adapt to changing conditions, and execute missions with precision. However, the rise of autonomous weapons raises ethical concerns, particularly regarding the potential for unintended civilian casualties and the accountability of AI-driven systems in warfare. Missiles have also seen significant advancements due to AI integration. AI algorithms enhance the targeting capabilities of missiles, allowing them to identify and track targets with greater accuracy. Additionally, AI enables missiles to adjust their flight paths in real-time, responding to changes in the target's movement or environmental conditions. These advancements make modern missiles more effective in hitting their intended targets, reducing the likelihood of collateral damage. However, the increasing reliance on AI in weapons systems also raises concerns about the potential for these technologies to be used in ways that violate international laws and norms.

AI plays a crucial role in cybersecurity by detecting and responding to threats in real-time, identifying suspicious activities, and mitigating risks before they escalate into major incidents. AI-driven cybersecurity solutions analyse vast amounts of data to identify patterns and anomalies that may indicate a cyber-attack. These systems continuously learn from new threats, enabling them to adapt and respond to evolving tactics used by hackers. Additionally, AI enhances encryption methods, making it more difficult for unauthorised parties to access sensitive information. The integration of AI into cybersecurity measures is essential for protecting critical infrastructure, financial systems, and personal data from cyber threats. The media's responsibility in covering AI-related issues is to provide accurate, unbiased, and informative reporting. The media plays a crucial role in shaping public perceptions of AI and its potential impact on society. Journalists must strive to understand the complexities of AI technology and its implications for various sectors, including security, privacy, ethics, and global stability. Media coverage should not only highlight the benefits of AI but also address the potential risks and challenges associated with its use. This balanced approach helps the public make informed decisions about the adoption and regulation of AI technologies.

However, the media can also be a double-edged sword when it comes to AI and security. Sensationalist reporting or the dissemination of misinformation about AI can create unnecessary fear or confusion, potentially leading to public distrust of AI technologies. It is essential for the media to avoid spreading alarmist narratives and instead focus on providing well-researched, evidence-based information about AI's role in society. This approach fosters a more informed and rational discourse about the challenges and opportunities presented by AI. Moreover, the media should be vigilant in reporting on the ethical implications of AI use, particularly in areas such as

surveillance, privacy, and autonomous weapons. By holding governments, corporations, and other stakeholders accountable for their use of AI, the media can help ensure that these technologies are developed and deployed in ways that align with societal values and respect pro-human rights. The continued advancement of AI technology holds both promise and peril for global security. On the one hand, AI has the potential to revolutionise counter-terrorism efforts, improve cybersecurity, and enhance global peace initiatives. On the other hand, the misuse of AI by malicious actors poses significant risks, from cyber-attacks and disinformation campaigns to the development of autonomous weapons. As AI continues to evolve, it is crucial for policymakers, technologists, and the media to work together to address these challenges and ensure that AI is used responsibly and ethically in the service of global security.

In conclusion, the rapid advancement of artificial intelligence presents a complex duality of benefits and risks within the realm of global security. On one hand, AI offers transformative potential in enhancing counter-terrorism efforts, from sophisticated surveillance and predictive analytics to bolstering cybersecurity and improving peacekeeping initiatives. The ability of AI to process vast amounts of data and adapt to new threats provides unprecedented tools for identifying and mitigating risks associated with terrorism. Its applications in monitoring, threat detection, and even autonomous weaponry illustrate its profound impact on modern security strategies. However, the same technologies that offer these advancements also pose significant risks. The potential misuse of AI by terrorist organisations to spread propaganda, recruit individuals, and execute cyber-attacks underscores a growing threat landscape. The development of autonomous weapons and the exploitation of AI for disinformation highlight the darker side of technological progress, raising ethical and legal concerns that must be addressed.

To navigate these challenges, it is crucial for policymakers, technologists, and security experts to collaborate in creating robust frameworks that balance the benefits of AI with the need for regulation and oversight. The media also plays a vital role in informing the public and holding stakeholders accountable, ensuring that the deployment of AI aligns with ethical standards and respects individual rights. As AI continues to evolve, it is essential to remain vigilant and proactive in managing its dual-use nature. By fostering a balanced approach that promotes innovation while mitigating risks, we can harness the positive aspects of AI to enhance global security and address the evolving threats posed by terrorism and cyber warfare.

REFERENCES

Bazarkina, D. (2023) 'Current and Future Threats of the Malicious Use of Artificial Intelligence by Terrorists: Psychological Aspects', in Pashentsev, E. (ed.) *The Palgrave Handbook of Malicious Use of AI and Psychological Security*. Cham: Palgrave Macmillan. Available at: https://doi.org/10.1007/978-3-031-22552-9_10 (Accessed: 14 August 2024).

Cairn.info. (2023). *AI and Cybersecurity: The European Perspective*. Available at: https://shs.cairn.info/revue-l-europe-en-formation-2023-1-page-85?lang=fr [Accessed 20 Aug. 2024].

Carnegie Endowment (n.d.) *Artificial Intelligence*. Available at: https://carnegieendowment.org/programs/technology-and-international-affairs/artificial-intelligence?lang=en (Accessed: 26 August 2024).

Capitol Technology University (2024) *AI and Counterterrorism: Potential, Pitfalls, and the Path Forward*. Available at: [URL] (Accessed: 17 August 2024).

Chatham House. (2019). *Artificial Intelligence and Counterterrorism*. Available at: https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf [Accessed 19 Aug. 2024].

Cisco. (n.d.). *Common Cyberattacks*. Available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html [Accessed 9 Aug. 2024].

Clarke, C.P. (2017) 'How Hezbollah Came to Dominate Information Warfare', *RAND Corporation*, 19 September. Available at: https://www.rand.org/pubs/commentary/2017/09/how-hezbollah-came-to-dominate-information-warfare.html (Accessed: 20 August 2024).

Deloitte (n.d.) *Surveillance and Predictive Policing Through AI*. Available at: https://www.deloitte.com/za/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html (Accessed: 26 August 2024).

ENISA (n.d.) *Artificial Intelligence*. Available at: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence (Accessed: 26 August 2024).

European Commission. (n.d.). *Tracking and Preventing Radicalisation Using AI (SPY)*. Available at: https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/tracking-and-preventing-radicalisation-using-ai-spy [Accessed 9 Aug. 2024].

Georgetown Journal of International Affairs (GJIA). (2024). *War, Artificial Intelligence, and the Future of Conflict*. Available at: https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict/ [Accessed 20 Aug. 2024].

GNET Research. (2024). *The Digital Weaponry of Radicalisation: AI and the Recruitment Nexus*. Available at: https://gnet-research.org/2024/07/04/the-digital-weaponry-of-radicalisation-ai-and-the-recruitment-nexus/ [Accessed 29 Aug. 2024].

Hemrajani, A. (2024) 'The Use of AI in Terrorism', *RSIS*, 26 August. Available at: https://www.rsis.edu.sg/rsis-publication/rsis/the-use-of-ai-in-terrorism/ (Accessed: 28 August 2024).

International Centre for Counter-Terrorism (ICCT). (n.d.). *Exploitation of Generative AI by Terrorist Groups*. Available at: https://www.icct.nl/publication/exploitation-generative-ai-terrorist-groups [Accessed 19 Aug. 2024].

Klein, E. and Patrick, S. (2024) 'Envisioning a Global Regime Complex to Govern Artificial Intelligence', *Carnegie Endowment for International Peace*, 21 March. Available at: https://carnegieendowment.org/2024/03/21/envisioning-global-regime-complex-to-govern-artificial-intelligence-pub-92022 (Accessed: 26 August 2024).

NEC (2024) 'NEC's Facial Recognition Technology Achieves NIST Performance Certification', *NEC Corporation*, Tokyo, Japan, 8 February. Available at: https://www.nec.com/en/press/202402/global_20240208_01.html#:~:text=NIST%20is%20a%20U.S.%20government,technological%20innovation%20and%20industrial%20competitiveness.&text=The%20test%20involves%20identifying%20a,people%20enrolled%20in%20a%20database (Accessed: 26 August 2024).

Nelu, C. (2024) 'Exploitation of Generative AI by Terrorist Groups', *ICCT*, 10 June. Available at: https://www.icct.nl/publication/exploitation-generative-ai-terrorist-groups (Accessed: 17 July 2024).

Sánchez, C.M., Sánchez, I.M., & Lozano, M.P. (2023). *Ethics and Artificial Intelligence in the Military Domain*. Available at: https://revistascientificas.us.es/index.php/ies/article/view/24281/22324 [Accessed 26 Aug. 2024].

ScienceDirect. (2023). *Artificial Intelligence and Radicalisation Prevention*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0160791X23000672 [Accessed 13 Aug. 2024].

Shah, M. (2024) 'The Digital Weaponry of Radicalisation: AI and the Recruitment Nexus', *GNET Research*, 4 July. Available at: https://gnet-research.org/2024/07/04/the-digital-weaponry-of-radicalisation-ai-and-the-recruitment-nexus/#:~:text=The%20ability%20of%20AI%20to,psychological%20vulnerabilities%20with%20unprecedented%20efficiency (Accessed: 14 August 2024).

Simplilearn. (n.d.). *Types of Cyber Attacks*. Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks [Accessed 9 Aug. 2024].

Siegel, D. and Doty, M.B. (2023) 'Weapons of Mass Disruption: Artificial Intelligence and the Production of Extremist Propaganda', *GNET Research*, 17 February. Available at: https://gnet-research.org/2023/02/17/weapons-of-mass-disruption-artificial-intelligence-and-the-production-of-extremist-propaganda/ (Accessed: 17 July 2024).

Pashentsev, E. (2023) 'Destabilization of Unstable Dynamic Social Equilibriums and the Malicious Use of Artificial Intelligence in High-Tech Strategic Psychological Warfare', in Pashentsev, E. (ed.) *The Palgrave Handbook of Malicious Use of AI and Psychological Security*. Cham: Palgrave Macmillan. Available at: https://doi.org/10.1007/978-3-031-22552-9_9 (Accessed: 14 August 2024).

Tech Against Terrorism (n.d.) *Generative AI and Terrorism*. Available at: https://techagainstterrorism.org/gen-ai (Accessed: 26 August 2024).

TechTarget. (n.d.). *Cyber Attack*. Available at: https://www.techtarget.com/searchsecurity/definition/cyber-attack [Accessed 9 Aug. 2024].

The Guardian (2023) 'Artificial Intelligence and the US Elections', *The Guardian*, 20 July. Available at: https://www.theguardian.com/us-news/2023/jul/20/artificial-intelligence-us-elections (Accessed: 26 August 2024).

UNICRI and UNCCT (2021) *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes*. Available at: https://unicri.it/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf (Accessed: 24 July 2024)

UNOCT and INTERPOL (2023) *Establishing Law Enforcement Agencies: A Guide*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_establishing_law_enforcement_web.pdf (Accessed: 26 July 2024).

United Nations. (n.d.). *Countering Terrorism Online with AI: UNCCT-UNICRI Report*. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf [Accessed 2 Aug. 2024].

U.S. Department of Defense. (n.d.). *Defence and AI*. Available at: https://www.defense.gov/ [Accessed 21 Aug. 2024].

U.S. Department of State. (n.d.). *Artificial Intelligence*. Available at: https://www.state.gov/artificial-intelligence/ [Accessed 19 Aug. 2024].

Ward, A. (2018) 'ISIS's Use of Social Media Still Poses a Threat to Stability', *RAND Corporation*, 11 December. Available at: https://www.rand.org/pubs/commentary/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html (Accessed: 26 July 2024).

Winkler, C. and El Damanhoury, K. (2022) 'Proto-State Media Systems: A History of Al-Qaeda and ISIS', in *Proto-State Media Systems: The Digital Rise of Al-Qaeda and ISIS*. New York: Oxford Academic. Available at: https://doi.org/10.1093/oso/9780197568026.003.0002 (Accessed: 17 July 2024).

NOTES ON CONTRIBUTORS

Professor Amparo Pamela Fabe of the National Police College, Philippines, is a maritime security researcher and a counterterrorist financing expert. Her expertise covers maritime domain awareness, cognitive warfare, terrorism financing, underwater maritime domain awareness, Women, Peace and Security and ordnance disposal. She is on the Editorial Board of the Indonesian Police Agency. Her 50 publications are featured in CRC Press, Routledge, Cambridge Scholars Publishing, Palgrave Macmillan, Brill and Springer.

Muhammad Afiq Ismaizam works as a Research Officer at the Southeast Regional Centre for Counter Terrorism (SEARCCT), under the Ministry of Foreign Affairs. His research focuses on the development of Artificial Intelligence (AI) and its misuse by terrorist groups. Afiq was a former Research Fellow under the "Think Next, Act Next" – The Next Gen of EU-ASEAN Think Tank Dialogue", that was co-funded by the European Union. Prior to this, Afiq was a senior manager of research and public affairs at the Asian Strategy and Leadership Institute (ASLI). While at ASLI, Afiq published research articles on topics such as mental health, political literacy and digital diplomacy. He also has work experience in management consulting and investment analysis. Afiq has an MA in International Affairs from King's College London.

Natechanok Sulaimarl is a Research Associate for the Counter-Terrorism Programme at the United Nations Office on Drugs and Crime (UNODC), Regional Office for Southeast Asia and the Pacific. She is based in Bangkok, Thailand. Currently her research focuses on preventing and countering terrorism and violent extremism in Southeast Asia and the Pacific. During her first master's degree in English Applied Linguistics from Chulalongkorn University, she published a study titled "Portrayal of Muslims in Relation to Thailand's Southern Conflict in English Newspaper Headlines," using a linguistic approach to analyse the factors underlying the conflict. In 2016, she received the prestigious Chevening Scholarship to pursue a Master of Science in Security Studies at University College London, UK. Over the years, she has conducted research on various topics, including political violence and terrorism, counterterrorism strategies, and peace processes. Her comparative study of "The Peace Processes in the Philippines' Moro Region and Thailand's Deep South" earned her a Merit Award. Her current research interests include the intersection of terrorism and technology, the nexus between insurgency and transnational organised crime, and the effective rehabilitation and reintegration of former terrorists.

Niki Esse De Lang, is the Regional Research & Programme Coordinator for the Counter-Terrorism Programme of UNODC's Regional Office for Southeast Asia and the Pacific. He is based in Jakarta, Indonesia. He has worked with UNODC for the last 7 years on counter-terrorism and its financing mainly focusing on Indonesia, the Philippines, Malaysia and Thailand. Before joining UNODC, Niki worked for over three years for the UN-backed Special Tribunal for Lebanon - Office of the Prosecutor in the Hague, the Netherlands as an Evidence Reviewer. Niki started his career with the UN as an intern with the UN Office of the High Commissioner for Human Rights in Bangkok. He has also undergone traineeships in the Netherlands with the Appeals Court (Criminal law department) and with a law firm. Niki also worked with two non-governmental organisations in Thailand and Myanmar. Niki obtained his law degree at the University of Amsterdam, specialising in criminal law and international law.

Siti Aisyah Tajari is a Research Officer at the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) under the Ministry of Foreign Affairs, Malaysia. She holds a Bachelor's degree in Strategic Studies from the National Defense University of Malaysia (NDUM) and is currently pursuing her Master's in Strategic Analysis and Security at the National University of Malaysia (UKM). During her undergraduate years, she was commissioned as a second lieutenant after completing three years of training with the Reserve Officer Training Unit (ROTU) and served as a Reserve Officer in the Territorial Army Regiment of the Malaysian Army. Her research focuses on the integration of gender-sensitive approaches in counter-terrorism, with a special emphasis on Preventing and Countering Violent Extremism (PCVE) in Southeast Asia. Specifically, she examines the role of women in PCVE efforts across Malaysia and Indonesia, exploring their contributions to community engagement, early warning systems, counter-narratives, and rehabilitation programmes.

Kennimrod Sariburaja is the Director of the Research and Publications Division at the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), under the purview of the Ministry of Foreign Affairs, Malaysia. He holds a Bachelor of Arts (Honours) in Southeast Asia Studies, with a minor in International and Strategic Studies, from the University of Malaya. In 2015, he received the prestigious Chevening Scholarship to pursue a Master of Letters (M.Litt.) in Terrorism and Political Violence at the University of St Andrews, Scotland. He has authored numerous monographs and articles on terrorism, counter-terrorism, international security, and global politics. His current research focuses on online radicalisation, foreign terrorist fighters (FTF), border security, and the evolving role of new technologies in terrorism and violent extremism. In 2024, he oversees the development of the SEARCCT Centre for Research Excellence and Online Repository (SCORE), further advancing SEARCCT's role in fostering resilience against extremism through research collaboration and knowledge dissemination.

Nik Nurdiana Zulkifli is currently serving as MySTEP personnel at the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) under the Research & Publications Division. She holds a Bachelor of Human Sciences in Political Science with honours from the International Islamic University Malaysia (IIUM). Her final-year thesis focused on China's Maritime Strategy and Taiwan's Centrality in Near Seas Territorial Disputes through the lens of structural realism. Nik Nurdiana has engaged in various fields throughout her professional journey, gaining multidisciplinary exposure while refining her areas of interest. During her internship with EMIR Research, an independent think-tank specialising in strategic policy recommendations, she contributed articles on diverse topics—including elderly abandonment, cross-strait tensions, and cyber-paedophilia—featured in multiple news outlets. In addition, she serves as an Inspector in the Police Volunteer Reserve Corps, a role that builds on her three years of training with the Police Undergraduate Voluntary Corps (SUKSIS) in the university. Following her graduation, she briefly worked as a part-time administrative clerk at the Perak State Finance Office before transitioning into her current position at SEARCCT.

Dr Robert Mikac is an Associate Professor. He teaches at the Faculty of Political Science, University of Zagreb, and the Croatian Military Academy "Dr. Franjo Tuđman". Prior to his academic career, he worked at the Ministry of Defence of the Republic of Croatia, the Ministry of the Interior of the Republic of Croatia, and the state agency responsible for civil protection. To date, he has authored or co-authored seven books (in Croatian, English, and Macedonian) and over 60 scientific papers.

Krešimir Mamić is Head of Counter Terrorism Service of the Ministry of Interior of the Republic of Croatia. He is the co-author of two books, and author and co-author of more than 20 scientific papers.

Siti Hajar binti Roslan is an Administrative and Diplomatic Officer (PTD) currently posted at the Research, Planning and Policy Division, the Public Service Department (JPA). Having served prior at the Research Division (RD) and National Security Council (MKN), Prime Minister's Department (JPM), Hajar recently finished her studies in Masters of International Security and Terrorism at the University of Nottingham, United Kingdom under the Chevening Scholarship Program.

Rasheka Mahendra is a dedicated youth advocate and justice enthusiast, with a fervent passion for Model United Nations conferences and travel. Currently in her third year at Cardiff University, she has already made significant strides in the field of strategic communications, having served as a trainer under the United Nations Office of Counter-Terrorism. Rasheka's accolades include being a BP 2020-2021 scholar for the AFS BP Global STEM program and a delegate at the 28th Youth Assembly hosted by the United Nations in New York. As a mentor for the AFS

Accelerators 2023 and a returning facilitator for the 2024 cohort, she continues to inspire and guide the next generation of leaders.

Sai Ganesh Laxmi Kanth is a 3rd-year law transfer student at the University of Liverpool, with a passionate focus on counter-terrorism and keeping the world at peace. Aspiring to become a lawyer, Sai has actively participated in Model United Nations competitions and was a debater during his school years. He also took part in essay and choral speaking competitions during high school. Sai loves crafting compelling argumentative essays and proving their validity, as well as drafting resolutions in Model United Nations competitions. His writing often explores legal and security issues, reflecting his dedication to the field of law. In addition to his academic pursuits, Sai has published multiple articles online during his internship with Richard Wee Law firm, showcasing his growing expertise and commitment to his future career.

SOUTHEAST ASIA REGIONAL CENTRE FOR COUNTER-TERRORISM (SEARCCT)
MINISTRY OF FOREIGN AFFAIRS
NO 516, PERSIARAN TUANKU JA'AFAR, BUKIT PERSEKUTUAN
50480 KUALA LUMPUR
MALAYSIA

Tel : (603) 22802800
Fax : (603) 22742734
Email: info@searcct.gov.my
Website: www.searcct.gov.my