ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

The Commonwealth

Special Section on Artificial Intelligence

Violent Extremism and Artificial Intelligence: A Double-Edged Sword in the Context of ASEAN

Wan Rosalili Wan Rosli[1]

Abstract

Digital integration and the emergence of new technologies such as artificial intelligence (AI) are providing new tools for insurgents to use in spreading their propaganda through violent extremism. The Association of Southeast Asian Nations (ASEAN) has come to represent a conduit for insurgents in planning and carrying out their extreme agendas. This article provides a deeper understanding of the double-edged sword effect of AI in relation to violent extremism in the ASEAN context. It reveals that, even though AI has been very important in countering violent extremism, it has simultaneously facilitated terrorists in spreading their propaganda in more innovative and covert ways. The legal framework governing AI is still in its infancy and challenges such as the double-edged sword effect in the use of the technology require specific guidelines or legislation for use in effective governance.

Introduction

Violent extremism and radicalism are not a new phenomenon. They entail diverse beliefs without a specific definition and are not exclusive to any religion, nationality or system of belief (UNDP, 2016). Violent extremism is a broader term than terrorism but encompasses manifestations of terrorism, including ideologically motivated violence (UNODC, 2018). The US defines violent extremism as encouraging, condoning, justifying or supporting the commission of a violent act to achieve political, ideological, religious, social or economic goals (FBI, 2021). The UK Home Office (2023) defines it as vocal and active opposition to fundamental values, which include the rule of law, liberty and mutual respect towards different beliefs and faiths.

1 Wan Rosalili Wan Rosli is an Assistant Professor at the School of Law, University of Bradford, United Kingdom.
Email: w.r.wanrosli@bradford.ac.uk / rosalili2301@gmail.com

Counterterrorism started to evolve with the 9/11 War on Terror, which has had a strong focus on coercive measures, including hard military action, increasing policy powers and expanding intelligence services (CCE, 2023). However, the approach has shifted to become more non-coercive, including the formulation of strategies to prevent individuals from supporting terrorism (ibid.). The United Nations contends that the key elements to countering violent extremism (CVE) involve the use of non-coercive means to drive individuals or groups from using violence and to mitigate recruitment, support, facilitation or engagement (UNODC, n.d.). Neuman (2004) highlighted that CVE strategies involved a non-exhaustive list of activities by governmental and non-governmental entities in the fight to combat radicalisation, such as counter-messaging exercises through social media channels, community engagements, advisory council discussions, capacity-building, women and youth empowerment, and education and training of stakeholders.

In recent years, violent extremism has shifted from an approach of holding specific territories in specific jurisdictions to real-time communications on social media platforms, where those involved seek to spread their ideologies and propaganda. The internet has no border control or checks and the lure of anonymity has changed the characteristics of violent extremism (Jacobsen, 2022; Khodzhanovna, 2023). Terrorist organisations see the internet as a safe way to recruit individuals and disseminate their ideology, especially through social media platforms such as Facebook, Twitter, YouTube and Instagram (Broeders et al., 2023).

Meanwhile, emerging technology such as artificial intelligence (AI) has contributed to the evolution of violent extremism. This article analyses the role of emerging technologies such as AI in facilitating the commission of acts of terror.

What is violent extremism?

Violent extremism has been a major issue in countries' policies and development programmes in the past few decades. The term was coined to shift the focus away from an over-militarised approach after 9/11 and to enable a more moderate approach in countering and preventing extremism (Saraiva and Erfe, 2023). The United Nations Plan of Action to Prevent Violent Extremism 2015 aims to develop resilience in sections of communities that are prone to violent extremism (UNOCT, 2015).

Although the concept is recognised across international communities, a uniform definition has never been agreed upon. As a result, the concept is easily manipulated, which poses a critical challenge to authorities and can sometimes also lead to the over-securitisation of specific sectors to further legitimise the war against terror (Stephens et al., 2021). The United Nations Special Rapporteur on the protection of human rights concluded that 'the lack of semantic and conceptual clarity that surrounds violent extremism remains an obstacle to any in-depth examination of the impact of strategies and policies to counter violent extremism on human rights as well as on their effectiveness in reducing the threat of terrorism' (Emmerson, 2016: para. 55).

Violent extremism includes elements of radicalisation, which is a process of embracing religious, political and social ideation that causes violent acts between members or groups (Doosje and van Eerten, 2017; Borum, 2023). Alcalá et al. (2017) contend that the promotion and adoption of extremist beliefs to advance violence leads to violent radicalisation, which has a critical effect on religion and society. Recent research has also highlighted that there are many aspects to extremist behaviour, emerging from cultural, educational and psychological factors. Interestingly, Stankov et al. (2018) contend that the ideology of extremism and radicalisation depends on mindsets, and extremist behaviours can be found in all humans. This contention supports the concept of extremism immunity, which entails embedding ideas, feelings and behaviours against radicalisation and extremism across all sectors of communities and social categories (ibid.).

Hamin et al. (2021) highlight that violent extremism is multidimensional and very complex, as there is no one agreed definition and different commentators often use the concept interchangeably with terrorism and radicalism. However, despite the lack of a specific meaning, the concept suggests a willingness of individuals or groups to use or support violence.

The proliferation of the internet in the past few decades has also changed how violent extremism is committed. Policy-makers and major stakeholders are strongly aware of the impact of the internet in supporting terrorism and violent extremism. Scrivens et al. (2020) highlight that law enforcement agencies have focused on learning how propaganda and extremist ideas are disseminated and cross into the real world; at the same time, major social media companies are concerned about how their platforms are seen as an important radicalising agent and become the main conduit in promoting real-world violent extremism. Commentators have also described how violent extremists have adopted new digital paradigms in their modus operandi to spread their hateful ideologies and propaganda, recruit new members worldwide and receive funding and tactical support (Salleh et al., 2016; Pressman and Ivan, 2019; Lakomy, 2023). The use of such technologies in violent extremism has been seen in Southeast Asia as well of other parts of the world.

The emergence of artificial intelligence

In the past decade, technology has invaded our everyday lives and dependency has soared. Challenges related to operations and capacity within law enforcement and counterterrorism agencies mean the use of AI has been seen as a holy grail in combatting violent extremism. AI's capacity to process vast amounts of data faster and with greater ease, and to correlate such data and discover patterns and themes, means intelligence agencies see it as an appealing commodity to confront the problem of managing information overload (Bazarkina, 2023). AI can support CVE through automating repetitive tasks, which in turn reduces workloads; predicting future violent extremist incidence; identifying suspicious transactions to detect terrorism financing; monitoring and moderating content within cyberspace; and other automation of capacities (Gutiérrez-Castillo, 2022). This serves as a game-changer, as all this surpasses human capabilities

Emerging technologies such as AI have been utilised in all sectors, from manufacturing to health to defence. Within the criminal justice context, AI has facilitated investigations through facial recognition; by assisting judges in granting bail and giving out sentences, parole and probation; and in matching DNA to perpetrators (Bazarkina, 2023). Machine learning is used to predict future criminal behaviour and identify patterns and risks of recidivism. AI is also fundamental in the prevention of cybercrime and has proven effective in preventing cyberattacks such as phishing, hacking and terrorism (Garcia, 2019).

Within the context of security, AI has played a crucial part in the fight against terrorism. AI has been used mainly for content moderation since terrorists have taken their operations to the internet (Gunton, 2022). AI and machine learning are believed to have the capacity to reduce terrorist content online and provide a safe place for users to operate within the cyberspace realm (Bamsey and Montasari, 2023). In the Southeast Asian context, such digital transformation requires adaptation, and the increased digitalisation rate exposes the countries to risks, given the established presence of violent extremist groups in the region (Ilyas, 2022).

Generative artificial intelligence

Generative AI is also an issue: these technologies can generate fictional faces and deepfakes. Deepfakes were invented in 2017, as a type of synthetic media that cannot be distinguished from authentic content (Gunton, 2022). Deepfakes are a powerful weapon that violent extremists can utilise, especially in information warfare, when people can no longer rely on what they see and hear online and offline (ibid.). Deepfakes have been used as a tool to commit malicious and criminal activities, usually politically motivated, such as destroying the credibility and reputation of a known individual, harassment, humiliation, extortion and blackmail. This can lead to social unrest and political instability (Bamsey and Montasari, 2023).

Natural language processing

Natural language processing is a deep learning application that analyses a huge amount of natural human language data, reading and defining the meaning in human languages. The technology involves speech recognition and natural language understanding, generation and translation (Bamsey and Montasari, 2023).

Combatting violent extremism via artificial intelligence

Nations all around the world see AI as a solution to prevent and counter violent extremism. The Council of Europe has adopted the Convention on the Prevention of Terrorism and compiled a Database on Cyberterrorism to mitigate cyberterrorist attacks (Ige et al., 2022). In the UK, steps have been taken to highlight the use of AI in moderating content and providing AI solutions in combatting terrorism online (McKendrick, 2019).

Other countries' governments are also confident that the use of AI is the ultimate response to violent extremism.

As well as countries putting in place technology-led solutions to combat extremist content on the internet, major content providers and service providers are creating partnerships to counter violent extremism online (McKendrick, 2019). The Global Internet Forum to Counter Terrorism is an industry-led initiative led by major online platforms such as Microsoft, X (formerly known as Twitter), Facebook and YouTube to combat violent extremism content (Fernandez and Alani, 2021). The aim is to disrupt terrorist activities online and develop tools and capacity to mitigate the impacts of terrorism. AI has also been at the forefront in combatting terrorism: states around the world are using AI in fighting extremist content online (Tech Against Terrorism, 2023). The mechanics of AI, which allow it to analyse and process enormous amounts of data, facilitate law enforcers to track and identify extremist content and activities. Content moderation via AI enables the monitoring and removal of extremist content and the breaking of networks, and the protection of vulnerable individuals who are prone to extremism.

Violent extremism in the Association of Southeast Asian Nations

In the ASEAN context, violent extremism has a long history, dating back to 1948, when the government had to counter new extremist elements during the challenging anti-colonial and post-independence era (El-Muhammady, 2023). The presence of Jemaah Islamiyah, affiliated with Al Qaeda, took root in 1940, and intensified after the 9/11 attacks in New York and Washington, DC. In the 1980s, Indonesia and Malaysia became a platform for violent extremists to participate in multinational jihad against the West. This led Jemaah Islamiyah to set up base in Indonesia, which then became a transnational Southeast Asian terror network committed to a pan-Southeast Asian Islamic State. Such ideologies spread across the whole region, from southern Thailand across Malaysia into Singapore and Indonesia to the east, and the southern Philippines. This move also led to the Bali bombing of 2002, with more than 200 fatalities. In August 2014, the Malaysian authorities managed to foil planned attacks within the country's capital (Hamzani, 2020).

The Global Terrorism Index, published in 2022, indicates that, of Southeast Asian countries, the Philippines and Myanmar are ranked within the top 20 countries that have been severely impacted by terrorism. Certain online incidents have also led the Indonesian government under the Ministry of Communications and Information Technology to set up a specialised team of moderators to moderate terrorist content in the country (Wilujeng and Risman, 2020). The ASEAN countries (Brunei Darussalam, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Cambodia and Vietnam) are aware of the growing complexity of violent extremism, especially with the advancement of social media and the internet, resulting in new patterns of radicalisation (ibid.). The major concerns of ASEAN include lone wolf terrorists, regional groups that

pledge allegiance to ISIS, Daesh and other terrorist organisations and the return of foreign terrorist fighters to the region (Tay, 2023).

Governing violent extremism in ASEAN

In 2016, the United Nations General Assembly adopted Resolution A/RES/70/291 by consensus to reinforce efforts to fight terrorism and violent extremism. The General Assembly also recommended member states set up regional and national plans of action to be applied within the local context. To align its efforts with those of the rest of the world, ASEAN has put in place and implemented strategies and plans for governance in combatting violent extremism under the ASEAN Comprehensive Plan of Action on Countering Terrorism (Gunaratna, 2018). In 2017, ASEAN adopted the Manila Declaration to Counter the Rise of Radicalisation and Violent Extremism, which includes pledges to implement sustainable and proactive capacity-building, information-sharing between member states, mutual legal assistance on criminal matters and extradition, and the strengthening of mechanisms to address terrorism and violent extremism through collaboration and exchange of experiences with all major stakeholders (Gunaratna, 2018; Habulan et al., 2018).

The ASEAN region has used the soft law approach, given the emphasis on non-interference between the states within the zone (Tan and Nasu, 2016). The ASEAN Convention on Counterterrorism is a framework to govern and co-ordinate member states to adopt a regional treaty on counterterrorism (Shah et al., 2022). Despite the existence of common initiatives throughout the region, Southeast Asian governments have not dealt with terrorism the same way. Indonesia and Singapore adopt a more non-militaristic approach, whereas Malaysia and Thailand rely on more coercive methods.

Malaysia has in place the Prevention of Crime Act 1959, the Prevention of Terrorism Act 2015 and the Special Measures against Terrorism in Foreign Countries Act 2015 to confront the threat of violent extremism by monitoring the activities of foreign terrorist fighters (Hamin et al., 2021). Prior to this, Malaysia had one of the most unpopular pieces of legislation, in the form of the Internal Security Act 1950, which caused citizens to take to the streets to claim that the law violated basic human rights. It was later replaced by the Security Offences (Special Measures) Act (SOSMA) 2012, said to be very similar to the law it replaced (ibid.). SOSMA is a preventive law containing special measures to deal with security-related offences that include terrorism, sabotage and espionage (Dhanapal and Sabaruddin, 2017). The Malaysian Bar Council highlights that the laws in place invoked a low standard of proof and ignored basic safeguards against human rights, leading to numerous civil liberty infringements (ibid.). Despite these controversies, however, the government has set up a Southeast Asian Regional Centre for Counterterrorism, in charge of training, information-sharing and awareness programmes (Hamin et al., 2021).

Similar to the situation in Malaysia, in March 2023 Myanmar published its Anti-Terrorism Bill with the aim of replacing the problematic Prevention of Terrorism Act, which had allegedly led to extensive torture and arbitrary detentions since 1979. The proposed

Bill gives the police, the president and the military more broad powers to detain without evidence, prosecute against vaguely defined criminal offences and ban gatherings and organisations. It also does not fulfil the requirements of the United Nations Special Rapporteur, including the need for an appropriate definition of terrorism, the prevention of arbitrary detention, the prohibition of any type of torture, and guaranteed fair trial and due process (Simpson and Farrelly, 2023).

In the Philippines, terrorism is governed under the Human Security Act of 2007. This has a general and broad definition of terrorism that involves elements of fear and panic among the population that coerce the government to give in to unlawful demands (Rasul, 2023). Thailand has its own National Action Plan on terrorism, finalised in 2022, and has criminalised terrorism within its Internal Security Act 2008 (Rasul, 2023). According to Tan and Nasu (2016), Cambodia has a different approach to counterterrorism, given grave concerns about transnational crimes: intel had revealed that Jemaah Islamiyah leaders were freely travelling through the country. This led Cambodia to enact the Law on Counter Terrorism 2007 and the Law on Anti-Money Laundering and Combatting the Financing of Terrorism 2007, to address counterterrorism financing, which was rampant at the time (ibid.). This move started a regional move to address terrorism financing as part of anti-money laundering policies. Malaysia enacted the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 and Myanmar the Control of Money Laundering Law 2002 (Tan and Nasu, 2016; Ramakrishna, 2017); both laws were later amended to include provisions on terrorist financing.

After the Bali bombing, Indonesia enacted the Anti-Terrorism Law 2003, which gives a broad definition of terrorism and allows a suspect to be detained without trial for a period of up to six months (Ramakrishna, 2017). Indonesia, with the help of the USA and Australia, also created Densus 88 in 2003, which serves as a counterterrorism unit to deal with intelligence and operations to dismantle violent extremist networks (Ramakrishna, 2017; Rasul, 2023). Between 2021 and 2023, there were more than 610 people arrested; 42 per cent of them identified as Jemaah Islamiyah members. This shows that the group is still very active in conducting terrorist activities, especially recruitment, fundraising and regeneration, which have now gone online (Subandi et al., 2023).

The double-edged sword of artificial intelligence in violent extremism

Communication interception has been crucial in preventing and countering violent extremism. However, the evolution and increased availability of communication technologies have resulted in these technologies reaching everyone, including sovereign nations, corporations, individuals... and terrorists. It is now easier for terrorists to evade detection, and accessing critical data to predict terrorist attacks has become increasingly challenging for intelligence agencies. Terrorists are also now implementing more advanced operational security measures in order to evade intelligence collection

operations (Bazarkina, 2023). In essence, terrorists have been early adopters of new technologies that have yet to be effectively governed and regulated (Lakomy, 2023). It has been reported that sections of the ISIS terrorist group within ASEAN have also utilised unmanned aerial vehicles or drones to conduct surveillance and reconnaissance (Liang, 2023).

Terrorists have always found ways to adapt and operate in the shadows to ensure non-detection by enforcement officers. The move from real-life terror operations to the online environment is to be expected, given the borderless and anonymous nature of the internet (Brundage et al., 2018). Governments and companies aim to halt the spread of radicalising content by investing in the creation of technologies to counter and identify extremism through AI solutions (ibid.). The main objectives are to understand the phenomena behind online extremism; to detect extreme users and content in cyberspace; and then to predict the spread of extremist ideologies within the online sphere (Bazarkina, 2023).

Amid these herculean efforts to design and develop effective AI solutions to automatically identify and block radical accounts, extremist organisations are also working hard to adapt their behaviour to avoid being detected. Through technological adaption, such organisations can make use of the latest developments in order to increase their reach undetected (Brundage et al., 2018) and can modify the terms and content they post online to avoid being detected by AI technology (UNICRI and UNCCT, 2021). The ASEAN region has always been a destination for terrorist organisations in procuring funding and recruiting new members; Malaysia and Singapore have highlighted that recruitment and funding are being carried out online and that the use of AI makes it challenging to detect such activities (Tay, 2023).

The use of generative AI has also been seen in violent extremists' exploitation of emerging technology. Media spawning involves the use of a single image or video from which generative AI can then generate thousands of manipulated images or videos capable of circumventing automated detection mechanisms utilised by law enforcers. Fully synthetic propaganda generates artificial content, including speeches, images and other propaganda. Personalised propaganda uses tools to customise messaging and media to a targeted audience with specific demographics. Such technology analyses each demographic and in turn produces personalised propaganda to suit the beliefs and understandings of the audience (Tech Against Terrorism, 2023).

States around the world are using AI to fight extremist content online, and it is seen as a good solution in the fight against online extremism. The mechanics of AI, which allow it to analyse and process enormous amounts of data, facilitate law enforcers to track and identify extremist content and activities. Through content moderation via AI, extremist content is removed and networks are broken (Tech Against Terrorism, 2023). However, any propaganda published is translated into multiple languages via natural language processing software in order to overwhelm moderation. Ultimately, extremist groups have found ways to avoid detection in spreading radicalised content online by subverting

moderation, using AI tools to design multiple variants of propaganda specifically engineered to bypass available techniques put in place by law enforcement (Tech Against Terrorism, 2023).

These new emerging technologies have proven that the current model for detection is obsolete, and the use of generative AI will provide opportunities to stay ahead of the threats (Tech Against Terrorism, 2023). Using AI to circumvent safeguards built into the infrastructure amplifies the distribution and dissemination of terror propaganda (Sabbagh, 2023).

The ASEAN response

The current cyber-climate is challenging, with attacks and threats becoming more sophisticated and volatile. The ASEAN regional response to cyberthreats has always been to fortify high levels of co-operation among member states in the form of computer emergency response teams, which focus on capacity-building and information-sharing in cyber-emergencies. However, the region's response to cyberterrorism is fragmented, owing to the lack of a strategic approach towards cybersecurity. In the second quarter of 2023, ASEAN members agreed to develop an ASEAN Guide on AI Governance and Ethics by 2024, following the focus of other nations in AI governance. However, it must be noted that individual ASEAN member states are very slow to progress on having their own AI governance frameworks.

The emergence of generative AI has changed the landscape of cyberterrorism, and ASEAN countries must be prepared. Tay (2023) highlights that ASEAN's current response to cyberterrorism lacks a regional institutional structure, and the cyber-operation architecture has no clear political authority and is a confusing maze, with various sectoral platforms. The nature of ASEAN itself hinders adequate governance of such crimes; unlike the EU, as a supernational entity, the ASEAN structure is based on intergovernmental organisations and principles of sovereignty, founded in consensus decision-making and non-interference between member states. Apart from this, the uneven development of legal and technological responses to such crimes across ASEAN is seen as a limitation.

Tay (2023) has also contended that the deficiency of the common cyber-lexicon is also a challenge: different states have different measures in defining the impact of a cyber-emergency or an attack on critical national infrastructure. Malaysia, for example defines a Level 5 crisis as having a critical impact on critical infrastructure organisations; however, other countries, such as Cambodia and Indonesia, do not have similar responses to Malaysia in defining a crisis.

Conclusion

There has been unprecedented progress in the use of AI in countering cyberterrorism to predict and detect terrorist attacks. However, significant challenges also arise with the deployment of such technologies. ASEAN should put in place a standard

and agreed terminology to ensure effective communication and information-sharing during a cyber-emergency such as a cyberterrorism attack. The absence of such an agreement will have impacts on the counter-effort to eliminate terrorist threats within the region. Member states within ASEAN should also ensure that the datasets used in countering terrorist attacks are verified and free from the risks of hallucinations and data poisoning. Such risks are aggravated given that the majority of states within ASEAN do not yet have a framework in place to govern AI and are still in the planning stages on addressing the issue. Meanwhile, despite ASEAN's ongoing participation in the effort to ensure global governance in AI, national regulation and regional co-operation are still lacking.

Technology will always evolve and the double-edged impact of AI in cyberterrorism means states must be prepared to face the unpredictable risks associated with it. The constant evolution of extremist behaviours and the numerous ways of avoiding detection in ever-changing narratives call for a serious response within the context of ASEAN. The fight to diffuse the impacts of negative uses of AI technology will continue. Enforcement is the key. Having a clear legal framework to combat terrorism and AI governance is of the utmost importance. Apart from this, digital citizens must be made aware of the subversive nature of the internet and social media, and national action plans and strategies must be put in place to prevent violent extremism.

References

Alcalá, H.E., M.Z. Sharif and G. Samari (2017) 'Social Determinants of Health, Violent Radicalization, and Terrorism: A Public Health Perspective'. *Health Equity* 1(1): 87–95.

Bamsey, O. and R. Montasari (2023) 'The Role of the Internet in Radicalisation to Violent Extremism'. In Montasari, R. (ed.) *Digital Transformation in Policing: The Promise, Perils and Solutions*. Cham: Springer International Publishing, pp. 119–135.

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: Springer International Publishing, pp. 251–272.

Borum, R. (2023) 'Mapping the Terrain: The Current State of Risk and Threat Assessment Practice in the Violent Extremism Field'. In Logan, C., R. Borum and P. Gill (eds) *Violent Extremism: A Handbook of Risk Assessment and Management*. London: UCL Press, pp. 53–78.

Broeders, D., F. Cristiano and D. Weggemans (2023) 'Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy'. *Studies in Conflict & Terrorism* 46(12): 2426–2453.

Brundage, M., S. Avin, J. Clark et al. (2018) 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation'. *arXiv preprint arXiv:1802.07228*.

Commission for Countering Extremism (CCE) (2023) 'Commission for Countering Extremism End of Year Report 2022 to 2023' www.gov.uk/government/publications/commission-for-countering-extremism-end-of-year-report-2022-to-2023/commission-for-countering-extremism-end-of-year-report-2022-to-2023-accessible-version

Dhanapal, S. and J.S. Sabaruddin (2017) 'Prevention of Terrorism: An Initial Exploration of Malaysia's POTA 2015'. *Pertanika Journal of Social Sciences & Humanities* 25(2): 783–804.

Doosje, B. and J.J van Eerten. (2017) '"Counter-Narratives" against Violent Extremism'. In Coleart, L. (ed.) *De-radicalisation*. Brussels: Flemish Peace Institute, pp. 83–100.

El-Muhammady, A. (2023) 'A "Blue Ocean" for Marginalised Radical Voices: Cyberspace, Social Media and Extremist Discourse in Malaysia'. In Loh, B.Y.H. (ed.) *New Media in the Margins: Lived Realities and Experiences from the Malaysian Peripheries*. Singapore: Springer Nature Singapore, pp. 163–192.

Emmerson, B. (2016) 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism'. Human Rights Council Report A/HRC/31/65.

Federal Bureau of Investigation (FBI) (2021). *Strategic Intelligence Assessment and Data on Domestic Terrorism*. Available at: https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report.pdf/view

Fernandez, M. and H. Alani (2021) 'Artificial Intelligence and Online Extremism: Challenges and Opportunities'. In McDaniel, J. and K. Pease (eds) *Predictive Policing and Artificial Intelligence*. Abingdon: Routledge, pp. 132–162.

Garcia, E.V. (2019) 'The Militarization of Artificial Intelligence: A Wake-Up Call for the Global South'. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452323

Gunaratna, R. (2018) 'ASEAN's Greatest Counter-Terrorism Challenge: The Shift from "Need to Know" to Smart to Share'. In KAS and RSIS (eds) *Combatting Violent Extremism and Terrorism in Asia and Europe: From Cooperation to Collaboration*, pp. 111–128.

Gunton, K. (2022) 'The Use of Artificial Intelligence in Content Moderation in Countering Violent Extremism on Social Media Platforms'. In Montasari, R. (ed.) *Artificial Intelligence and National Security*. Cham: Springer International Publishing, pp. 69–79.

Gutiérrez-Castillo, V.L. (2022) 'Big Data and the New Armed Conflicts'. In Fernández-Sánchez, P.A. (eds) *The Limitations of the Law of Armed Conflicts: New Means and Methods of Warfare*. Brill Nijhoff, pp. 284–297.

Home Office (UK) (2013) *HM Government Counter-Terrorism Disruptive Powers report 2022 (accessible version)*. [online]. https://www.gov.uk/government/publications/counter-terrorism-disruptive-powers-report-2022/hm-government-counter-terrorism-disruptive-powers-report-2022-accessible-version

Habulan, A., M. Taufiqurrohman, M.H.B. Jani et al. (2018) 'Southeast Asia: Philippines, Indonesia, Malaysia, Myanmar, Thailand, Singapore, Online Extremism'. *Counter Terrorist Trends and Analyses* 10(1): 7–30.

Hamin, Z., S. Kamaruddin, A.R. Abd Rani and A. Munirah (2021) 'When Violent Extremism Is No Longer a Man's World: Some Evidence from Malaysia'. *International Journal of Academic Research in Business and Social Sciences* 11(9).

Hamzani, A.I. (2020) 'The Trend to Counter Terrorism in ASEAN'. *Journal of Advanced Research in Dynamical and Control Systems* 12(7): 105–113.

Ige, T., A. Kolade and O. Kolade (2022) 'Enhancing Border Security and Countering Terrorism Through Computer Vision: A Field of Artificial Intelligence'. *Proceedings of the Computational Methods in Systems and Software*. Cham: Springer International Publishing, pp. 656–666.

Ilyas, M. (2022) 'Terrorism Industry and Data Coloniality in Southeast Asia'. *Journal of Contemporary Governance and Public Policy* 3(1): 31–46.

Jacobsen, J.T. (2022) 'Cyberterrorism'. *Perspectives on Terrorism* 16(5): 62–72.

Khodzhanovna, S.K. (2023) 'A New Interpretation of Cyberterrorism: Challenges and Prospects'. *Best Journal of Innovation in Science, Research and Development* 2(7): 91–96.

Lakomy, M. (2023) 'Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad'. *Terrorism and Political Violence* 35(6): 1261–1298.

Liang, S.C.. (2023) 'Terrorist digitalis: preventing terrorists from using emerging technologies'. In *Global Terrorism Index 2023*. Institute for Economics and Peace. pp. 72–74. www.visionofhumanity.org/wp-content/uploads/2023/03/GTI-2023-web-170423.pdf

McKendrick, K. (2019) *Artificial Intelligence Prediction and Counterterrorism*. London: The Royal Institute of International Affairs-Chatham House.

Neuman, G.L. (2004) 'Comment, Counter-Terrorist Operations and the Rule of Law'. *European Journal of International Law* 15(5): 1019–1029.

Pressman, D.E. and C. Ivan (2019) 'Internet Use and Violent Extremism: A Cyber-VERA Risk Assessment Protocol'. In IRMA (ed.) *Violent Extremism: Breakthroughs in Research and Practice.* Hershey, PA: IGI Global, pp. 43–61.

Ramakrishna, K. (2017) 'The Growth of ISIS Extremism in Southeast Asia: Its Ideological and Cognitive Features—and Possible Policy Responses. *New England Journal of Public Policy* 29(1): 1–35.

Rasul, A. (2023) 'ASEAN and the Challenge of Democracy'. In Guo, Y. and I. Puja (eds) *Sustaining Peace in ASEAN and the Asia-Pacific: Preventive Diplomacy Measures*. ASEAN-IPR and CFAU, pp. 177–194.

Sabbagh, D. (2023) 'Terrorists Could Try to Exploit Artificial Intelligence, MI5 and FBI Chiefs Warn'. *The Guardian*, 18 October. www.theguardian.com/technology/2023/oct/18/terrorists-exploit-artificial-intelligence-ai-mi5-fbi-chiefs-warn

Salleh, N.M., S.R. Selamat and Z. Saaya (2016) 'A New Taxonomy of Cyber Violent Extremism (Cyber-VE) Attack'. 6th International Conference on Information and Communication Technology for the Muslim World.

Saraiva, R. and A. Erfe (2023) 'Preventing Violent Extremism with Resilience, Adaptive Peacebuilding, and Community-Embedded Approaches'. *Current Opinion in Environmental Sustainability* 61: 101271.

Scrivens, R., P. Gill and M. Conway (2020) 'The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research'. In Holt, T. and A. Bossler (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London: Palgrave, pp. 1417–1435.

Shah, H.A.R., K. Zada, N.M. Ali and M.M. Sahid (2022) 'Peace in ASEAN: Counter-Narrative Strategies against the Ideologies of Radicalism and Extremism (Goal 16)'. In Khalid, R.M. and A.J. Maidin (eds) *Good Governance and the Sustainable Development Goals in Southeast Asia*. Abingdon: Routledge, pp. 194–211.

Simpson, A. and N. Farrelly (2023) *Myanmar: Politics, Economy and Society.* Abingdon: Routledge.

Stankov, L., G. Knežević, G. Saucier et al. (2018) 'Militant Extremist Mindset and the Assessment of Radicalization in the General Population'. *Journal of Individual Differences* 39(2): 88–98.

Stephens, W., S. Sieckelinck and H. Boutellier (2021) 'Preventing Violent Extremism: A Review of the Literature;. *Studies in Conflict & Terrorism* 44(4): 346–361.

Subandi, Y., H.R.T. Sjahputra and M. Subhan (2023) 'Indonesia-ASEAN Partnership to Counter-Terrorism in Indonesia'. *East Asian Journal of Multidisciplinary Research* 2(7): 2857–2874.

Tan, S.S. and H. Nasu (2016) 'ASEAN and the Development of Counter-Terrorism Law and Policy in Southeast Asia'. *The University of New South Wales Law Journal* 39(3): 1219–1238.

Tay, K. (2023) *ASEAN Cyber-Security Cooperation: Towards a Regional Emergency Response Framework*. London: IISS.

Tech Against Terrorism (2023) 'Early Terrorist Experimentation with Generative Artificial Intelligence Services'. Briefing, November.

United Nations Development Programme (UNDC) (2016) *Preventing Violent Extremism Through Promoting Inclusive Development, Tolerance and Respect For Diversity: A Development Response To Addressing Radicalization And Violent Extremism*. https://www.undp.org/sites/g/files/zskgke326/files/publications/Discussion%20Paper%20-%20Preventing%20Violent%20Extremism%20by%20Promoting%20Inclusive%20%20Development.pdf.

United Nations Counter-Terrorism Centre (UNCCT) and the United Nations Interregional Crime and Justice Research Institute (UNICRI) (2021) *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes*. United Nations Office of Counter-Terrorism. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

United Nations Office of Counter-Terrorism (UNOCT) (2015) 'Plan of Action to Prevent Violent Extremism'. www.un.org/counterterrorism/plan-of-action-to-prevent-violent-extremism

United Nations Office on Drugs and Crime (UNODC) (no date) 'Terrorism Prevention'. Regional Office for Southeast Asia and the Pacific. www.unodc.org/roseap/en/what-we-do/terrorism-prevention/index.html.

UNODC (2018) 'E4J University Module Series: Counter-Terrorism: Module 2: Conditions Conducive to the Spread of Terrorism: *"Radicalization" & "Violent Extremism"*'. https://www.unodc.org/e4j/zh/terrorism/module-2/key-issues/radicalization-violent-extremism.html.

Wilujeng, N.F. and H. Risman (2020) 'Examining ASEAN: Our Eyes Dealing with Regional Context in Counter Terrorism, Radicalism, and Violent Extremism'. *International Journal of Social Sciences* 6(1): 267–281.

About the author

Dr Wan Rosalili Wan Rosli is an Assistant Professor at the University of Bradford, United Kingdom. She has secured multiple research grants in subject areas ranging from money laundering to cybercrime, artificial intelligence, prevention/countering of violent extremism-related laws, and cybersecurity issues. She also has more than 30 academic papers published in journals. She was invited to be a subject matter expert in formulating a new anti-stalking law for Malaysia. She developed an application named MyStalk Alert which aims to support the victims of harassment and stalking by assisting them to keep a trail of evidence which is imperative for investigation and prosecution. The app also gives mental health support and useful links that help victims to keep a diary of all incidences. The MyStalk Alert won one gold medal and one silver medal in an international innovation competition. Dr Wan Rosalili has also received several recognitions from her former university, where she won the research and publication award between 2020 and 2022.