Southeast Asia Regional Centre for Counter-Terrorism
Ministry of Foreign Affairs
No 516, Persiaran Tunku Ja’afar, Bukit Persekutuan
50480 Kuala Lumpur, Malaysia

☎ (603) 22802800
✉ info@searcct.gov.my
(603) 22742734
www.searcct.gov.my

9 789671 565643

SEARCCT'S SELECTION OF ARTICLES 2023

SEARCCT’S

Southeast Asia Regional Centre for Counter-Terrorism | Ministry of Foreign Affairs

Selection of Articles

2023

Special Issue: Building Digital Resilience in Preventing and Countering Violent Extremism

SEARCCT'S SELECTION OF ARTICLES 2023 SPECIAL ISSUE: *BUILDING DIGITAL RESILIENCE IN PREVENTING AND COUNTERING VIOLENT EXTREMISM*

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) 2280 2800
Fax: (603) 2274 2734
Email: info@searcct.gov.my

First published in 2023

SEARCCT is dedicated to advocating the understanding of issue pertaining to terrorism and counter-terrorism and contributing ideas for counter-terrorism policy. The Centre accomplishes this mainly by conducting capacity building, research, counter-messaging and public outreach. *All statements of facts opinions and expressions contained in this work are the sole responsibility of the author and do not necessarily reflect those of the Government of Malaysia. The Government of Malaysia assumes no responsibility for any statements of facts or opinions expressed in this work. Articles in this publication were commissioned in November 2023, may not reflect Malaysia's current political environment.*

CONTENTS

FOREWORD

MINISTER OF FOREIGN AFFAIRS, MALAYSIA

This publication of SEARCCT's Selection of Articles (SOA) 2023 Special Issue: "Building Digital Resilience in Preventing and Countering Violent Extremism (PCVE)" aims at providing an all encompassing overview of the inaugural SEARCCT's International Conference 2023 (S.I.C.) 2023 proceedings, which was held from 13 to 15 June 2023 in Kuala Lumpur. The publication also includes articles authored by esteemed speakers and moderators of the conference and other subject-matter experts in the field.

In the dynamic digital environment of the 21st century, it is both remarkable and alarming to observe the swift and widespread dissemination of information, ideas, and ideologies. The advent of the digital era has not only brought about significant progress and enhanced connectivity, but it has also given rise to a novel form of threat: the spreading of violent extremism via digital means.

As we stand at the juncture of technological growth and societal challenges, the SOA 2023 special issue assumes significant importance as it serves as a guide in our shared pursuit of comprehending and addressing the difficulties posed by the digital era. While the digital domain may be a fertile ground for extremist views to flourish, it can also be a platform to promote dialogue and understanding, as well as dissemination of counter-narratives to undermine and dismantle violent extremist beliefs.

We are very honoured to have our speakers shared their experience and knowledge at the conference, which become an important resource of knowledge for PCVE practitioners. Before we delve into the rich tapestry discussions and recommendations that these pages offer, I would like to express my heartfelt gratitude to all the contributors for their insights on this pivotal issue.

Building digital resilience is a continuous endeavour involving various stakeholders. It is my fervent hope that readers, whether they be policymakers, researchers, scholars, or the general public will gain not just a deeper understanding of the challenges at hand, but a sense of optimism for the solutions that lie ahead.

Thank you.

....

DR. ZAMBRY ABD KADIR

MESSAGE

SECRETARY-GENERAL
MINISTRY OF FOREIGN AFFAIRS, MALAYSIA

I would like to congratulate SEARCCT on the publication of the special issue of SEARCCT's Selection of Articles (SOA) 2023. This post-conference publication follows the successful organisation of SEARCCT's International Conference 2023 (S.I.C.) 2023 on 13-15 June 2023. A compilation of articles contributed by experts in the field on the theme of "Building Digital Resilience in Preventing and Countering Violent Extremism (PCVE)" is included in this publication among others.

This publication demonstrates SEARCCT's desire to be one of the leading entities in the exchange of knowledge and the promotion of ideas. The conference proceedings involved the swapping of ideas, the sharing of best practices, and the formulation of recommendations to address challenges posed by online violent extremism. Moreover, the collection of articles in the journal represents an intricate interplay of research, insights, and a deep seated commitment to safeguarding our digital domains. In this dynamic era of digital interconnectivity, digital resilience is a crucial element for ensuring safe and unimpeded societal progress.

I wish to record my sincere appreciation to the contributors for their articles in this issue. These articles are not mere write-up; they are building blocks for change, providing a foundation upon which strategies can be built, policies formulated, and awareness raised.

To the readers, I hope that SOA 2023 will ignite a renewed curiosity awareness about the digital challenges we face, and inspire proactive steps towards resilience.

Thank you.

....

AMRAN MOHAMED ZIN

MESSAGE

DIRECTOR-GENERAL
SOUTHEAST ASIA REGIONAL CENTRE FOR COUNTER-TERRORISM (SEARCCT)
MINISTRY OF FOREIGN AFFAIRS, MALAYSIA

I am delighted to introduce the publication of SEARCCT's Selection of Articles (SOA) 2023 Special Issue: "Building Digital Resilience in Preventing and Countering Violent Extremism (PCVE)." This publication is the culmination of an eventful SEARCCT's International Conference (S.I.C.) 2023, which marked a significant milestone as the Centre celebrates the 20th anniversary of its establishment.

I would also like to express my sincere gratitude to the S.I.C. 2023 organising committee, the speakers, moderators, and all conference attendees, as well as the article contributors, editors, and reviewers of the SOA 2023. The conference and publication have managed to gather policymakers, security practitioners, researchers, scholars, and civil society organisations with a shared vision of constructing a resilient community against the influence of violent extremism in the digital sphere.

Therefore, it is essential to record the discussion presented at the S.I.C. 2023, which outlined current and future challenges as well as recommendations that demanded a coordinated response and effort from various stakeholders. The publication is intended to contribute to the body of knowledge and serve as a resource for the implementation of future actions. Furthermore, this collection of articles authored by subject-matter experts is meant to further expand the discussion that took place at the conference.

The SOA 2023 special issue stands as more than just a compilation – it represents our collective hope and commitment to a digital realm free from the shadows of violent extremism. It is my hope that each article, each insight, reinforces our belief in the power of knowledge as our greatest weapon in this endeavour.

Thank you and enjoy reading!

....

GANESON SIVAGURUNATHAN

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SIC INTERNATIONAL
2023 CONFERENCE
"Building Digital Resilience in Preventing and Countering Violent Extremism - P/CVE"
years of SEARCCT

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SIC INTERNATIONAL
2023 CONFERENCE
Building Digital Resilience in Preventing and Countering Violent Extremism
RCCT

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SIC SEARCCT'S INTERNATIONAL 2023 CONFERENCE
Building Digital Resilience in Preventing and Countering Violent Extremism – P/CVE

SIC SEARCCT'S INTERNATIONAL 2023 CONFERENCE
Building Digital Resilience in Preventing and Countering Violent Extremism – P/CVE

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

SHARING TOGETHER FOR ONLINE RESILIENCE AMONG YOUTH (STORY) REGIONAL WORKSHOP 2023

PART 1

INTRODUCTION TO SEARCCT'S INTERNATIONAL CONFERENCE (S.I.C.) 2023

OVERVIEW OF SEARCCT'S INTERNATIONAL CONFERENCE 2023

"BUILDING DIGITAL RESILIENCE IN PREVENTING AND COUNTERING VIOLENT EXTREMISM (PCVE)"

SEARCCT's International Conference (S.I.C.) 2023 on "*Building Digital Resilience in Preventing and Countering Violent Extremism* (PCVE)" was held from 13 to 15 June 2023 at the Hilton Kuala Lumpur. This inaugural conference was organised to commemorate the 20th Anniversary of SEARCCT.

The conference was preceded by a regional youth workshop entitled "*Sharing Together for Online Resilience among Youth* (STORY)", which took place from 10 to 12 June 2023 at the same location. The STORY workshop featured a total of 28 youth participants from Malaysia and Southeast Asian countries, including Brunei, Cambodia, Indonesia, Philippines, Thailand, and Vietnam. The workshop explored Generative Artificial Intelligence (AI) and the usage of AI tools such as ChatGPT, Image Creator, and more in creating digital resilience-themed contents.

The S.I.C. 2023 was aimed at gathering policymakers, security practitioners, experts, researchers, and civil society organisations to deliberate the current challenges related to online violent extremism as well as ways to prevent/counter them, particularly on the soft approaches in the context of building society's digital resilience. To achieve this objective, there were five panel discussions held throughout the two-and-a-half-day of the conference on the following topics:

(i) Preventing Terrorist Use of the Internet;
(ii) Promoting a Multi-Stakeholder Approach to PCVE;
(iii) Digital Strategic Communication: Counter/Alternative Narratives;
(iv) The Role of Media and Influencers in PCVE; and
(v) Developing Digital Resilience: Strategies and Best Practices.

In terms of programming, aside from the five panel discussions, S.I.C. 2023 comprised of Opening Session and Welcome Dinner held on the first day (13 June 2023); a Luncheon Talk entitled "*Articulating a Madani Framework for Counter-Extremism*", delivered by Prof. Emeritus Datuk Dr. Osman Bakar, the Holder of Al-Ghazali Chair of Epistemology and Civilizational Studies and Renewal at the International Institute of Islamic Thought and Civilisation (ISTAC IIUM); and a Closing Session on the final day (15 June 2023). There was also a showcase of the STORY workshop on 13 June, which featured the outcome of the workshop and the media products created by the participants.

His Excellency Datuk Mohamad Alamin, Deputy Minister of Foreign Affairs of Malaysia graced the Opening Session by delivering the Keynote Address, on behalf of the Minister of Foreign Affairs. The Opening Session also heard the Welcome Address by the Director General of SEARCCT. More than 220 attendees participated in the Opening Session comprised of conference participants and other invited guests including representatives of diplomatic missions based in Kuala Lumpur and members of the media.

The Secretary General of Ministry of Foreign Affairs, Malaysia delivered a Closing Speech highlighting the way forward including on the importance of international collaboration in the fight against violent extremism. The Closing Session also heard a summation by the head of rapporteurs highlighting key takeaways and recommendations discussed at the conference.

Overall, the S.I.C. 2023 was attended by 158 local and international participants, including speakers and moderators, policymakers, enforcement officers, diplomats, academics, researchers, and civil society representatives. There were 24 speakers involved in the conference from prestigious institutions and organisations such as Deakin University, National University of Singapore (NUS), International Institute of Islamic Thought and Civilisation (ISTAC-IIUM), National University of Malaysia (UKM), National Defence University Malaysia (NDUM), Institute of Strategic and International Studies (ISIS) Malaysia, *Yayasan Prasasti Perdamaian*, United Nations Office on Drugs and Crime (UNODC), United Nations Development Programme (UNDP), Mythos Labs, Love Frankie, Moonshot, and Microsoft.

WELCOME ADDRESS
DATO’ GANESON SIVAGURUNATHAN

DIRECTOR-GENERAL
SOUTHEAST ASIA REGIONAL CENTRE FOR COUNTER-TERRORISM (SEARCCT)
MINISTRY OF FOREIGN AFFAIRS, MALAYSIA

His Excellency Datuk Mohamad bin Alamin,
Deputy Minister of Foreign Affairs of Malaysia,

His Excellency Dato’ Norman Muhamad,
Deputy Secretary-General, Bilateral Affairs, Ministry of Foreign Affairs of Malaysia,

Excellencies, Distinguished Ambassadors, Speakers and Moderators,

Participants of the Conference,

Ladies and Gentlemen,

Good morning, *Salam Sejahtera*, *Salam Malaysia Madani* and a very warm welcome to SEARCCT’s International Conference (S.I.C) 2023 on “Building Digital Resilience in Preventing and Countering Violent Extremism or PCVE”.

2. Before I proceed further, allow me to express my sincere appreciation to His Excellency Datuk Mohamad bin Alamin, Deputy Minister of Foreign Affairs of Malaysia, for his time and presence to grace today’s Opening Session despite his busy schedule. We are honoured to have you here, and for that, thank you, Sir.

3. I am also pleased that all of you present here have graciously accepted our invitation to participate in this Conference. Some of you have come all the way from across the globe. Our special thanks to all Speakers and Moderators, which without them, meaningful deliberations of the Conference would not be possible.

4. Our sincere gratitude also goes to our partners including the Delegation of the European Union (EU) to Malaysia, the New Zealand High Commission and the United States Embassy in Kuala Lumpur, who have sponsored their Speakers and flown them to Kuala Lumpur. I am certain they will greatly contribute to the success of this Conference.

Excellencies, Ladies and Gentlemen,

5. The Southeast Asia Regional Centre for Counter Terrorism, or better known as SEARCCT, was established in 2003 and received the recognition of the ASEAN Member States during the 10th Meeting of ASEAN Regional Forum (ARF) in the same year.

6. For the past 20 years, SEARCCT has been involved in the soft approaches to counter-terrorism through various programmes that are based on the five flagships adopted by the Centre, namely: Investigation and Legal Aspects; Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) and Crisis Management; Critical Infrastructure Protection; Terrorism Financing; and Preventing and Countering Violent Extremism (PCVE).

7. These programmes are designed to enhance the knowledge and capacity of the nation's law enforcement, government and security officials, as well as the larger civil society, and the international community. They are conducted through collaboration with local agencies, foreign governments, established think-tanks and international organisations, and serve as a platform that allows inter-agency cooperation and engagement with wider public and civil society.

8. Essentially, SEARCCT envisioned to play a contributing role, so that the community would be prepared, sufficiently robust and resilient to withstand and respond to the threat of terrorism and violent extremism.

Excellencies, Ladies and Gentlemen,

9. Since its inception, SEARCCT has gained much experience and conducted more than 320 programmes. These programmes have benefited more than 13,500 local and international participants from various sectors including government, law enforcement, academia, media, and civil society organisations, among others.

10. At the national level, SEARCCT has reached out to more than 20,000 youth/undergraduates through its various public lecture series and awareness programmes.

11. At the regional level, SEARCCT had organised 32 international and regional levels programmes under various frameworks within the span of eight years from 2015 to 2022. SEARCCT has also worked with ASEAN Dialogue Partners in conducting several regional programmes under the framework of ASEAN Regional Forum (ARF).

12. In addition, SEARCCT also works closely with international organisations, especially United Nations (UN) entities such as the United Nations Office on Drugs and Crime (UNODC), United Nations Counter-Terrorism Committee Executive Directorate (UNCTED) and United Nations Development Programme (UNDP) for its regional programmes and collaborative projects.

13. Recently, SEARCCT has been part of a regional network of Preventing Violent Extremism (PVE) practitioners of Southeast Asia or known as SEAN-PVE, an initiative spearheaded by the United Nations Office on Drugs and Crime (UNODC). The SEAN- PVE network is the first of its kind in the region and has been a promising platform in terms of connecting practitioners with government officials, academicians, and community-based actors around various thematic areas such as youth empowerment, strategic communications, and community resilience. SEARCCT plays an important role in this initiative and is expected to assume the role of administrative office of the network for the next cycle after Indonesia.

Excellencies, Ladies and Gentlemen,

14. What had been highlighted were among the few advances and achievements made by SEARCCT in its 20 years of establishment. The Centre has learned so much and one of it is the realisation of increased emphasis or pivot towards multi-stakeholder approaches in PCVE efforts. This has led to the idea of hosting an International Conference in the field of PCVE to commemorate the 20th Anniversary of SEARCCT.

15. I believe that the theme – Building Digital Resilience in PCVE – is apt, considering the role of the digital space in our lives today. While the internet has been used to communicate and disseminate news and knowledge, there are malicious groups taking advantage of the technology. Terrorists and extremists' ideologies are being disseminated more effectively with a plethora of social media platforms combined with unique social functionality. The threat of increased online exposure to radicalising factors cannot be overstated, which brings us to this Conference agenda.

16. From the PCVE lens, SEARCCT has always emphasised on 'community resilience'. This 'community resilience' needs to be manifested not only in the physical world, but also online. We must ensure that our digital natives are resilient to the challenges of the digital world.

17. On this note, I wish to inform that SEARCCT had organised a pre-event to the S.I.C. 2023 – a Regional Workshop entitled *Sharing Together for Online Resilience Among Youth* (STORY) from 10-12 June 2023. The STORY workshop involved youth from the Southeast Asian region and promotes their partnership in PCVE efforts. This capacity-building workshop culminated with a social media campaign hackathon contest and the outcome would be presented later this evening.

18. Furthermore, improving social cohesion has become a cornerstone of violence prevention and peacebuilding, thus reducing vulnerability to violent extremism. This is also what the Conference aims to achieve: that is to understand digital communities and how they can be more resilient, and exploring coordinated efforts that can be put in place. To achieve this aim, SEARCCT has curated a programme that involves five panels discussion over a two-and-a-half-day Conference.

19. We hope this Conference would serve as a platform for engagement among stakeholders from different sectors. We could compare notes, share experiences, exchange information and nurture new ideas and recommendations in addressing those challenges. I am sure that the Deputy Foreign Minister, His Excellency Datuk Mohamad bin Alamin, will deliberate further in his keynote address.

Excellencies, Ladies and Gentlemen,

20. Before I end my speech, once again, I would like to express our sincere appreciation to all speakers, moderators and participants for lending your time and expertise in ensuring an enriched discussion. To our international delegates and participants, I welcome you to Malaysia. I hope you will be able to take some time to visit the wonderful city of Kuala Lumpur. I can assure you that you will not be disappointed.

21. Excellencies, ladies and gentlemen, on that note, it is my great honour to invite His Excellency, Datuk Mohamad bin Alamin, to deliver the keynote address on behalf Foreign Minister and declare this Conference open.

Thank you.

KEYNOTE ADDRESS
H.E DATO’ SERI DIRAJA DR. ZAMBRY ABD KADIR

MINISTER OF FOREIGN AFFAIRS, MALAYSIA

DELIVERED BY
HIS EXCELLENCY DATUK MOHAMAD ALAMIN

DEPUTY MINISTER OF FOREIGN AFFAIRS, MALAYSIA

CONFERENCE
uilding Digital Resilience in
reventing and Countering Violent
xtremism - PAVE
13 - 15 Ju
Kuala Lu

Assalamualaikumwarahmatullahiwabarakatuh, peace be upon you, *Salam Malaysia Madani* and a very good morning to all.

First and foremost, I would like to convey greetings from His Excellency Dato’ Sri Diraja Dr. Zambry Abdul Kadir, Minister of Foreign Affairs, who is not able to be here this morning due to an unexpected urgent matter that requires him to be with the Prime Minister.

The Foreign Minister wishes all participants a fruitful engagement and successful Conference.

I will be reading the Keynote Address on behalf of the Minister.

(The Keynote Address reads as follows:)

His Excellency Dato’ Norman Muhamad,
Deputy Secretary-General, Bilateral Affairs, Ministry of Foreign Affairs of Malaysia,

His Excellency Dato’ Ganeson Sivagurunathan,
Director-General, Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT),

Excellencies, Distinguished Ambassadors, Eminent Speakers and Moderators,

Senior Officials of the Ministry of Foreign Affairs,

Participants of the Conference,

1. Let me begin by commending SEARCCT for organising this International Conference, or S.I.C. 2023, under the theme of "Building Digital Resilience in Preventing and Countering Violent Extremism or PCVE". It is indeed a privilege for me to stand before you today to open this Conference and say a few words.

2. When I look at the topic and theme of the Conference, my initial thought was it is a complex issue. The term *'violent extremism'* itself lacks clarity and consensus in terms of a universally accepted definition.

3. The same goes to terrorism as what Prof. Alex Schmid and Albert Jongman have said in their book *"Political Terrorism"*.

> *"Authors have spilled almost as much ink – trying to define the concept in terrorism and radicalisation – as the actors of terrorism have spilled blood."*

4. Furthermore, the variance of the causes that lead to violent extremism is unique and, sometimes, specific to certain situations, which in turn, invalidates the *'one-size-fits-all'* solution. This complexity reminds me of the words of Malaysia's founding father – Tunku Abdul Rahman, who once said:

> *"We must remember to be a beacon of light in a disturbed and distracted world."*

5. And here we are – working, deliberating, exchanging ideas, sometimes stumbling even, but always rising again – in our endeavour to find answers to the problem, against the backdrop of a world impacted by technological advances and social transformations.

6. For policy makers, the journey to formulate strategies to address issues begins with defining the terms, understanding the context, comprehending the nuances, and setting in place the necessary terms of reference.

7. Hence,the questions: How far do we really understand the current landscape of violent extremism in the digital realm? and what does digital resilience truly mean?

8. I hope by the end of my speech, I will be able to provoke thoughts, offer some perspectives and suggestions for further deliberation by experts and participants of the Conference.

Excellencies, Ladies and Gentlemen,

9. Notwithstanding the fact that there is yet a clear definition of *'violent extremism'*, the context is generally understood: That is, the use of violent or coercive means to achieve political, social, or ideological objectives. It may involve acts of terrorism, radicalisation of individuals or groups, or support for extremist organisations or beliefs.

10. So, how does this context permeate in the current modern setting?

11. In this ‘digital age’, we have all become interconnected in ways that were inconceivable just a few decades ago. The internet has revolutionised our world by granting unprecedented access to information and real-time global communication. Generally, we often think of its many positive aspects – the ability to connect with others beyond borders, as well as the opportunities for creativity, commerce, and innovation.

12. However, this digital evolution comes with its own obstacles and challenges. While we should *embrace* the opportunities for progress that it provides, we must also *brace* ourselves for the damage it can yield in the wrong hands.

13. By this, I am referring to those who wish and choose to exploit this technology to cause harm, spreading hate, fear, and violence.

14. The same technology that has benefited us can also amplify detrimental ideologies and aid in the spread of terrorism and violent extremism.

15. The internet has been used to disseminate extremists’ propaganda, to recruit and radicalise individuals, to plan and coordinate attacks, and to spread fear and chaos.

Excellencies, Ladies and Gentlemen,

16. We may recall Daesh’s online strategy that has led to thousands becoming foreign terrorist fighters. Their ability to manipulate technology and misuse religious doctrine has been devastating.

17. Despite international efforts to counteract Daesh’s influence with the end of its territorial control in 2019 and the deaths of several of its leaders since then, the group and its affiliates have maintained relevance by expanding their global network, brand, and operations in the digital world.

18. In addition to the threat posed by Daesh, Europol has issued a public warning last year that the threat of violent attacks by right-wing extremists in transnational online communities is growing.

19. The agency discovered more than 800 instances of violent or terrorist content, where many right-wing extremist perpetrators were part of virtual communities.

20. These examples reinforce the urgency in countering violent extremism, and the need to amplify digital literacy and resilience measures in preventing online radicalisation.

Excellencies, Ladies and Gentlemen,

21. We must understand the mechanisms that allow terrorist and extremist groups to endure in the digital world to effectively combat violent extremism. They are attributed to several key factors:

- Digital Savviness: Terrorists and extremists have demonstrated an astute understanding of the power of digital platforms, utilising them to maintain a sense of community and purpose among followers worldwide. The anonymised and decentralised character of the internet provides fertile ground for their digital operations.
- Decentralisation and Anonymity: The internet enables a level of decentralisation and anonymity that is not possible with conventional forms of communication and organisation. Despite crackdowns on their operations, new accounts and platforms continue to emerge, allowing their digital influence to persist.
- Exploitation of Grievances: The rhetoric of terrorists and extremists frequently focuses on exploiting real or perceived grievances, such as political, economic, or social injustices. They exploit divisions, sowing dread, and promoting an *'us-versus-them'* narrative. Such messages resonate with some internet users, thereby aiding radicalisation and recruitment.
- Adaptability: Terrorists and extremists have the capability to adapt to emerging technologies. As older accounts are deactivated, they migrate their activities to new platforms to maintain their digital presence.
- Engaging Strategies: Terrorists and extremists have adapted interactive online strategies, such as the use of video games, online quizzes, and social media challenges, which can be appealing to younger internet users.

Excellencies, Ladies and Gentlemen,

22. To respond to these factors, we must build the capacity of our communities for digital resilience, fortifying our online spaces against the pervasiveness of terrorism and violent extremism.

23. This powerful approach would enable even the most vulnerable members of our communities to be able to tell apart what constitutes extremist propaganda, and to be able to fend off attempts to generate sympathy or even radicalise them into violence.

24. Similarly, our communities can also be better informed on how to report extremist content they find online and contribute to law enforcement efforts in disrupting violent extremist networks.

25. We must remember that digital resilience is not just about countering violent extremism. It is a competency that helps us use digital technologies in a safe and responsible manner. It is about empowering people with skills and knowledge for them to be aware and cognizant of the risks and dangers that exist online.

26. Essentially, digital resilience entrusts us to use technology to promote the positive values towards fostering harmony, peace and mutual understanding that underpin our societies.

Excellencies, Ladies and Gentlemen,

27. We must work together to promote and bolster digital resilience. In this regard, I would like to throw an idea of "Digital Resilience Initiative or DRI," an aspirational framework rooted in the values of *'Malaysia Madani'*.

28. This idea represents a commitment, or rather a call for action, to fostering an online community that is not only safe but also respectful, trustworthy, compassionate and promotes peaceful co-existence, tolerance and healthy multi-religious and multicultural engagements.

29. I would envision that this initiative would be based on four key strategic areas:

A. Firstly; Awareness and Knowledge

- This area involves efforts to promote digital literacy as a core competency, including through the education system. The objective is to cultivate citizens who are discerning information consumers, to be able to distinguish between credible sources and manipulative materials.
- It should focus on the promotion of moral values that call for peaceful co- existence, mutual understanding, respect and compassion, while encouraging inquisitiveness and analytical minds among citizens so that they can separate fact from fiction.
- Developing guiding principles to citizens on how to be safe and responsible online, as well as individualised awareness campaigns about the dangers of online radicalisation that emphasise the significance of reporting suspicious activities must also be considered.

B. Secondly; Support and Empowerment

- This pillar focuses on building the competencies of and empowering credible voices or messengers within the communities. These voices and messengers can provide powerful, authentic alternatives to violent extremist narratives.
- It also involves measures to assist those who have been impacted or targeted by violent extremists' narrative by providing resources for rehabilitation and reintegration.
- This could guide them away from the path of extremism towards embracing inclusivity, tolerance and unity.

C. Thirdly; Regulation and Accountability

- As we navigate the technological advanced age, it is imperative to prevent the potential misuse of tools like generative Artificial Intelligence (AI). Therefore, this area requires regulatory reform, with input and feedback gathered from various relevant stakeholders.
- There must be clear guidelines that encourage the responsible and ethical use of such technologies. At the same time, we must also establish accountability mechanisms for those who maliciously violate these guidelines.
- Any individuals or organisations who abuse these technologies will be held accountable and serve as a deterrent to others that such actions will no longer be tolerated.

D. Fourthly: Cooperation and Collaboration

- We must foster an environment for cooperation, not just between governments, but also across all sectors including tech companies, as well as civil society organisations.
- We should look beyond a Whole-of-Government approach, but also a Whole- of-Society approach in which the various layers and segments of society take ownership of problems and challenges that cut across nations and regions.
- This pillar seeks to improve the sharing of knowledge, information, and best practices among all relevant stakeholders. This could be achieved through creation of platforms such as a global network of practitioners that could facilitate such endeavours.

Excellencies, Ladies and Gentlemen,

30. I believe these four key pillars will enable us to not only fortify our digital spaces against potential threats, but also proactively promote the values of peace, harmony and mutual understanding.

31. I am pleased to note that some of the strategies have been employed by SEARCCT, such as through the hosting of this Conference and a pre-event in the form of a regional workshop entitled *'Sharing Together for Online Resilience among Youth'* (STORY).

32. The regional workshop has provided a platform where young people from the Southeast Asia region come together to brainstorm how they could make their communities more resilient and the online space safer.

Excellencies, Ladies and Gentlemen,

33. Before I conclude, as we embark on this ambitious digital resilience initiative, let us ensure that it is one of resilience, unity, and progress.

34. There is a saying that "*security is not about the absence of danger, but the presence of resilience.*"

35. Therefore, we should strive together towards a future that is free from the scourge of violent extremism, and built on the principles of justice, respect, trust, peaceful co- existence, mutual understanding and compassion.

36. With that, Thank You, and *dengan lafaz Bismillahirrahmanirrahim*, I declare this Conference open.

CLOSING SPEECH
H.E DATO’ SRI AMRAN MOHAMED ZIN

SECRETARY-GENERAL
MINISTRY OF FOREIGN AFFAIRS, MALAYSIA

Assalamualaikum warrahmatullahi wabarakatuh, *Salam Malaysia Madani*, and a very good morning to all.

His Excellency Dato’ Ganeson Sivagurunathan,
Director-General,
The Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT)

Excellencies, Learned Speakers and Moderators,

Distinguished Participants of the Conference,

Ladies and Gentlemen,

Let me begin by extending belated *“Selamat Datang”* to Malaysia to all our International Speakers, Moderators and Participants. I hope you have had a good stay in Kuala Lumpur.

2. I thank SEARCCT for this opportunity to address the closing session of this International Conference, commemorating the 20th anniversary of the Centre’s establishment.

3. The Conference's theme – "Building Digital Resilience in Preventing and Countering Violent Extremism (PCVE)" – has been aptly chosen. Our world is faced with challenges of violent extremism and dangers posed by malicious actors in the digital realm. On this point, I commend SEARCCT for making a meaningful contribution in our common efforts to address these challenges.

4. The Conference is a remarkable milestone for SEARCCT. It is a clear manifestation that the Centre has come a long way since its inception in two thousand and three.It projects the potential of SEARCCT to be one of key global players in countering terrorism and violent extremism.

5. I am happy to learn that you have had extensive deliberations in all panel sessions. We just have heard the summary report from the Head of the Rapporteuring Team, which highlighted many issues that were discussed throughout the Conference. I think all in all, the Conference has managed to provide a platform for exchanges between the brightest minds from across the globe.

6. Policymakers, government officials, security practitioners, experts, researchers, industry players, and civil society organisations – each of you has shared unique perspectives, experiences, and innovative ideas.

7. This rich diversity of knowledge and skillsets have helped shape a more holistic and nuanced understanding of the issues we face in building digital resilience within our communities.

8. Throughout the Conference, you have acknowledged that our battle against violent extremism is not confined to national borders or individual proprietors. Violent extremism permeates every corner of our increasingly interconnected world – the digital world.

9. In moving forward, solid international collaboration is imperative. We should leverage on the strengths, resources, and information possessed by all stakeholders. Nations should not limit capacity to unite against common enemies – violent extremists.

10. Needless to mention, our shared struggle transcends geographical boundaries, political differences, and sectoral divisions. Let us therefore carry this spirit of cooperation and collaboration that prevailed during this conference forward. We should strive for a cohesive and global shield of digital resilience.

11. Within this context, I welcome SEARCCT's plan to publish a full post-Conference report on the proceedings of this Conference, together with a selection of informative articles and presentations contributed by the Speakers and Moderators.

12. This publication will document all ideas, recommendations and best practices presented and deliberated at this Conference. Hopefully it can serve as a reference point for relevant stakeholders in formulating strategies for enhancing digital resilience.

13. As this Conference draws to a close, we are reminded that our common struggle against violent extremism is still far from over. We must remember that our battle is not won in Conference halls.

14. We need to win the hearts and minds of everyday people in navigating the complex digital world. They should be endowed with tools and resources they need in order for them to be resilient when surfing the internet.

15. The insights and knowledge shared during this Conference should be translated into policies and approaches of our respective countries, organisations and communities.

16. On a parting note, I congratulate SEARCCT for reaching this significant milestone, and for the successful convening of the S.I.C. 2023. I commend the organising committee and the secretariat, led by Director General Dato' Ganeson, for planning, curating and executing the programme of the Conference.

17. It would be remiss of me, if I do not record the sincere gratitude of the Ministry of Foreign Affairs of Malaysia to all Speakers, Moderators and Participants for your insightful contributions to the deliberations throughout this Conference.

18. Our heartfelt appreciation also goes to SEARCCT's collaborators and partners – the Delegation of the European Union (EU) to Malaysia, the New Zealand High Commission and the United States Embassy in Kuala Lumpur.

19. Our partners' presence has added great value and richness to the discussions and debates you have had over the past two days.

20. The commitment and unwavering support of all present here to the cause of preventing and countering violent extremism have lent weight and credibility, not only to this Conference, but also to international efforts to fight the menace.

21. To our international Speakers, Moderators and Participants, I hope you would continue to enjoy your stay in Kuala Lumpur. Please bring back with you good memories and have a safe journey home.

Until we meet again, Thank You.

SUMMATION SPEECH
HEAD OF RAPPORTEURS
MOHD HASRIL ABDUL HAMID

DEPUTY DIRECTOR-GENERAL I
SOUTHEAST ASIA REGIONAL CENTRE FOR COUNTER-TERRORISM (SEARCCT)
MINISTRY OF FOREIGN AFFAIRS, MALAYSIA

His Excellency Dato' Sri Amran Mohamed Zin,
Secretary-General, Ministry of Foreign Affairs, Malaysia

His Excellency Dato' Ganeson Sivagurunathan,
Director-General of the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT)

Distinguished Speakers and Moderators, Participants of the Conference,
Ladies and Gentlemen,

Assalamualaikum warrahmatullah hiwabarakatuh, peace be upon you, *Salam Sejahtera* and a very good morning to all.

2. I hope everyone present here is still in a very good spirit as we are approaching the end of SEARCCT's International Conference, (S.I.C.) 2023, "Building Digital Resilience in Preventing and Countering Violent Extremism (PCVE)."

3. It is a great honour for me to deliver a summation that has been carefully prepared by a dedicated team of rapporteurs. The past two days had been hectic – packed with articulations of ideas, enriching debates, insightful discussions as well as sharing of knowledge and experience.

4. Before I proceed further, on behalf of SEARCCT, we would like to put on record our profound appreciation to the rapporteurs for their unwavering commitment and contribution to come up with key takeaways of the Conference, which is imbued in this summation, in a short period of time. Their hard work has been instrumental in ensuring that the gists of the discussion are not lost.

5. I hope this summation would do justice in terms of encapsulating the invaluable insights, recommendations and best practices, or rather some speakers refer to it as exemplary actions, that were highlighted throughout the Conference.

Ladies and Gentlemen,

6. The Conference heard about the idea of Digital Resilience Initiative, or DRI, proposed by the Foreign Minister of Malaysia in his Keynote Address. The DRI is a ‘call for action framework’, consisting of four key strategic pillars to bolster digital resilience. The pillars are: Awareness and Knowledge; Support and Empowerment; Regulation and Accountability, as well as Cooperation and Collaboration. Under these pillars, actionable proposals include the following:

6.1 To promote digital literacy as core competency including through education system;

6.2 To promote moral values that call for peaceful co-existence, mutual understanding, respect and compassion while encouraging inquisitiveness;

6.3 To develop guideline principles on how to be safe and responsible online;

6.4 To come up with individualised awareness campaigns about the dangers of online radicalisation;

6.5 To build and empower credible messengers to counter violent extremists’ narratives;

6.6 To provide resources for rehabilitation and reintegration of those who have been radicalised;

6.7 To develop clear guidelines and accountability mechanism that encourage and ensure the responsible and ethical use of emerging technologies such as generative Artificial Intelligence (AI); and

6.8 To foster an environment for cooperation across sectors including creating a platform such as a global network of practitioners.

7. These proposals were echoed throughout the Conference. There was a general sentiment that they merit further refinement by relevant stakeholders based on the local context, needs and circumstances.

Ladies and Gentlemen,

8. The first panel, Preventing Terrorist Use of the internet, explored the critical challenges posed by online terrorist activities and its implications for global security. Key points and recommendations highlighted were as follows:

8.1 Rapid development of technology has significantly reshaped society, obscuring the line between authentic and deceptive information. This has created opportunities for nefarious activities by violent extremist groups;

8.2 Violent extremist groups have exploited anonymity and the vastness of the digital landscape to disseminate their ideologies, recruit vulnerable individuals, as well as plan and execute acts of violence;

8.3 The process of online radicalisation is influenced by factors that interweave across multiple domains including religious beliefs, political inclination, socio-economic problems, and health-related issues;

8.4 Global crises have the potential to deepen societal divisions, leading to the emergence of vulnerable individuals or groups;

8.5 While there was a decline in terrorism-related arrests, the threat of radicalisation is still prevalent;

8.6 Comprehensive framework that addresses the digital rights and responsibilities of individuals is essential;

8.7 To focus on containing, countering and resilience building efforts rather than preventing terrorist use of the internet;

8.8 To establish and promote credible voices and platforms. The panel heard about "ruangobrol.id" as an example;

8.9 To encourage collaboration between tech giants and relevant stakeholders to ensure the safe use of digital platforms; and

8.10 To consider gender differences in understanding and addressing radicalisation, recognising that men and women may be radicalised in different ways.

Ladies and Gentlemen,

9. The second panel explored the critical importance of Promoting A Multi-Stakeholder Approach to PCVE. It was highlighted that mediums such as sports, culture, and the arts should be explored in PCVE efforts. At the same time, there must be a paradigm shift from national to local level coordination on PCVE approaches. Among the key recommendations emanating from the panel were as follows:

9.1 To incentivise the involvement of local government in PCVE and resilience-building initiatives, as well as strengthen community-based and community-led reintegration efforts;

9.2 To apply effective mentoring initiatives that can be scientifically evaluated, based on the different needs of stakeholders;

9.3 To pursue legal reforms in clarifying the key terminology to tackle hate speech; and

9.4 To implement early-stage interventions against violent radicalisation by different actors through a whole-of- society approach.

10. The third panel emphasised that digital strategic communication is about credible, compelling, and convincing narratives that challenge violent extremist narrative. There was a recognition of the need of blocking terrorists' online contents, while promoting digital resilience and media literacy. A speaker highlighted that counter messaging approaches can be based on the Inoculation Theory and the Frame Alignment Theory. Aside from that, the panel stressed upon a gender-justice narrative to address issues related to female involvement in terrorism.

11. Furthermore, the combined use of edutainment, media and information literacy, and Artificial Intelligence (AI) technology must be considered in counter-messaging strategies as extremist propaganda is influenced by pop culture references. It was also learned that extremists employ "gamification" techniques in spreading their propaganda through the use of in-game chats and gaming adjacent platforms like Discord and Twitch. Additionally, the differences between content-based and communications-based responses in counter messaging were also highlighted at the panel.

Ladies and Gentlemen,

12. The fourth panel understood that media and influencers have significant impact on shaping narratives and influencing public opinion. Key recommendations of the panel include the following:

12.1 There must be greater collaboration among traditional and new media, including social media influencers and citizen journalists;

12.2 Multi-stakeholder collaboration among nations in the region is needed to increase funding and resources for digital influencers. This could assist in enhancing their visibility and creation of impactful content; and

12.3 There is an opportunity to utilise multiplayer gaming and adjacent platforms for positive interventions.

13. The last panel discussion on developing digital resilience highlighted several relevant recommendations. Among others, the UN initiative, known as the Global Digital Compact, could be used as a reference point by practitioners to address challenges posed by the digital revolution. Also highlighted was the need to tackle misinformation or disinformation in line

with the recent Secretary General of the UN Policy Brief on Information Integrity on Digital Platforms.

14. Emphasis was given on repurposing the online gaming space as it helps bridge cultural barriers through direct, private and secure interactions which contribute to digital resilience. For instance, the game ‘Gali Fakta’ was developed by Moonshot to counter misinformation and disinformation. Another example mentioned was Microsoft’s Safety by Design philosophy that facilitates safe and positive online environments for children. Additionally, building digital resilience should also include adding a ‘Dissuade’ pillar to the PCVE framework.

Ladies and Gentlemen,

15. The Conference also had the opportunity to listen to a luncheon talk titled “Articulating a Madani Framework for Counter-Extremism” which delved into the relations between civilisation and extremism. The speaker highlighted the concept of ‘middleness’ as the raison d’etre of civilisation and an effective antidote to extremism.

16. The middle path, as argued, existed across cultures and religions including Islam, Christianity, Buddhism, and Hinduism, making it applicable in a multi-cultural and multi-religious society like Malaysia’s. The speaker called upon scholars and policymakers to continue the discourse on ‘middleness’ and Madani to create a civilised and moderate society, which would serve as a shield against extremism.

Ladies and Gentlemen,

17. This is merely a glimpse of the many ideas and insights that have been shared in the past two days. In going forward, we endeavour in coming up with a post-conference publication in the near future that provides a more detailed and comprehensive takeaway of the Conference.

18. In the meantime, I believe this summation is an immediate outcome that can be used as reference points for contextualising implementable actions in building digital resilience.

19. On that note, thank you for your time and active participation throughout this Conference.

PART 2

RAPPORTEURS REPORT

PANEL 1:

PREVENTING TERRORIST USE OF THE INTERNET

SPEAKERS:
Prof. Greg Barton
Chair in Global Islamic Politics
Deakin University, Australia

Dr. Ahmad El-Muhammady
Assistant Professor
International Institute of Islamic Thought and Civilisation (ISTAC-IIUM), Malaysia

Dr. Noor Huda Ismail
Visiting Fellow
S.Rajaratnam School of International Studies (RSIS), Singapore

MODERATOR:
Ms. Farlina Said
Senior Analyst
Institute of Strategic and International Studies (ISIS), Malaysia

SUMMARY:

The first panel discussion on “Preventing Terrorist Use of the Internet” commenced following the conclusion of the Conference’s Opening Session. The moderator started the session by framing the parameters of discussion which centred around the utilisation of the internet and other digital platforms by terrorists and violent extremists to propagate their narratives or to influence their intended targets for the purpose of recruitment.

DISCUSSION:

1. **Prof. Greg Barton** addressed the challenges of fully preventing terrorist use of the internet and emphasised the importance of containing, countering and building resilience against such activities. In his presentation, Prof. Barton also cautioned that the term “terrorism” should not be applied too broadly or narrowly, as it could be misused to undermine good governance and human rights.

2. Prof. Barton apprised the audience on the common use of the internet by terrorists which includes, among others, propaganda and strategic communications; provocation and manipulation; recruitment and radicalization; as well as fund raising.

3. He noted that certain risks had emerged from rapid technological advancement over the past 15 years. Scams and the potential misuse of artificial intelligence (AI), including Generative AI (GenAI) and ChatGPT, for deceptive purposes have become areas of concern. Prof. Barton highlighted the emergence of trust issues stemming from the misappropriation of digital technology and the rampant spread of conspiracy theories.

4. **Dr. Ahmad El-Muhammady** in his presentation titled “Cyberspace and the Internet: A ‘Blue Ocean’ for Marginalised Radical Voices”, delved into the dynamic process of radicalisation, shedding light on its developmental stages from initial trigger points to extreme cases (peak), and ultimately transitioning into a declining phase (dormant). He described the present state as being dormant.

5. Dr. Ahmad emphasised that radicalisation manifests in both violent and non-violent forms, with non-violent radicalisation persisting even in the absence of terrorism-related arrests. He explained that the origins of radicalisation were multifaceted, encompassing various religious, political, social and health-related factor.

6. It was also highlighted that cyberspace often served as a platform that pushed marginalised individuals into the ‘blue ocean’. Dr. Ahmad further mentioned that global crises have significant personal impacts, leading to societal polarisation and the emergence of vulnerable individuals.

7. **Dr. Noor Huda Ismail** noted the importance of promoting positive narratives among youths as part of their digital rights and responsibilities such as the digital platform *"ruangobrol.id"* which addressed the issues of radicalism and terrorism through credible voices. He also stated that the high number of internet users in Malaysia and Indonesia, particularly among the young population, were considered as both "digital native" and conversely, "digital naïve". Observations of this particular category of young people found that they lacked the inherent skills needed to navigate digital platforms and to filter the authenticity of information presented.

8. Prof. Greg Barton observed that the internet had created a tendency among individuals to question authority and subject matter experts. This phenomenon subsequently breeds a lack of trust, which could significantly contribute to disinformation. Conflicting information also has the potential to confuse and influence vulnerable individuals, rendering them more susceptible to radicalisation.

9. In essence, the speakers underscored the significance of adopting a comprehensive whole-of-government and whole-of-society approach. The session called for governments to support advocacy efforts by civil society organisations (CSOs) and academics in preventing and countering violent extremism (PCVE), while also prioritising digital resilience within society.

10. Recognising the interdependent relationship between online and offline spaces, Dr. Noor Huda stressed that maintaining harmony is of utmost importance. This approach includes engagements with tech giants such as Facebook, TikTok, Google, and Twitter to ensure the safe use of their platforms.

11. Dr. Noor Huda also highlighted that gender differences also need to be further explored, to understand how males and females could be radicalised in distinct ways. He also spoke about the need to ensure safe reintegration of victims of violent extremism and radicalisation into society. Faced with online attacks, these individuals tend to feel alienated, increasing their emotional and ideological vulnerability. The significance of psychological and mental health support was also emphasised.

INTERACTIVE Q&A SESSION

12. During the Q&A session, three questions were raised by the participants regarding the identification of vulnerable groups, the importance of expanding credible voices, and the potential ramifications associated with adopting a rigid, dichotomous definition of extremism and terrorism.

13. Disinformation was defined by Prof. Barton as the spread of inaccurate information. Conspiracy theories are one example, as people often seek these theories to find solutions to problems, leading to confusion and distrust in institutions.

14. Despite being in different parts of the world, some individuals could recruit, persuade and convince others based on shared beliefs and ideologies. The importance of relatability was highlighted, emphasising the need to expand credible voices across all levels, including the direct experiences of victims, to address extremism, terrorism and radicalisation. Dr. Noor Huda also underscored the role of mothers and wives in disengagement from violent extremism.

15. Three key factors, known as the "3N": Need, Narrative, and Network were identified by Dr. Noor Huda in understanding the psychological dimension associated with vulnerability, particularly among youth. Dr. Ahmad described that vulnerabilities may be cognitive, emotional, or ideological while Prof. Barton viewed vulnerable individuals as also those lacking fulfilling human relationships.

PANEL 2:

PROMOTING A MULTI-STAKEHOLDER APPROACH TO PCVE

SPEAKERS:
Mr. Niloy Banerjee
Resident Representative
United Nations Development Programme Malaysia, Singapore and
Brunei Darussalam

Mr. Taufik Andrie
Executive Director
Institute for International Peace Building, Indonesia

Mr. Maarten De Waele
Coordinator Local PVE and Polarisation
Association of Flemish Cities and Municipalities, Belgium

Dr. Murni Wan Mohd Nor
Senior Lecturer
Department of Government and Civilisational Studies
Universiti Putra Malaysia (UPM), Malaysia

MODERATOR:
Prof. Dr. Kamarulnizam Abdullah
Professor and Principal Fellow
Institute for Malaysia and International Studies (IKMAS),
National University of Malaysia (UKM), Malaysia

SUMMARY:

This panel discussion discussed the critical importance of promoting a multi-stakeholder approach to PCVE. The panel called for creative approaches to PCVE which may include the use of mediums such as sports, culture, and the arts. The panel also deliberated on the importance of a paradigm shift from national to local level coordination where panellists shared examples of involvement of diverse institutions and civil society organisations in PCVE. Also discussed were gendered approaches in PCVE initiatives, as well as challenges and recommendations on multi-stakeholder collaboration.

DISCUSSION:

1. **Mr. Niloy Banerjee** highlighted some recommended practical avenues namely
   (i) sports;
   (ii) culture;
   (iii) multi-stakeholder approach; and
   (iv) the media as tools for PCVE.

2. He regarded sports to be an effective platform to unify people across race, culture and religion. The same also goes for cultural elements such as food, film, and theatre, which serve as an effective unifying tool.

3. He further elaborated that the government, as well as civil society, private sector, and academia play significant roles in addressing violent extremism. Additionally, he emphasised the crucial role of the media in influencing how society perceives and responds to violent extremism.

4. **Mr. Taufik Andrie** discussed three models of reintegration for former radicalised individuals in Indonesia, which focused on:
   (i) non-governmental organisations (NGOs);
   (ii) state-based initiatives at national and local levels; and
   (iii) community-based initiatives.

5. He highlighted some of the challenges faced by the Indonesian Government, including:
   (i) the lack of implementation of the National Action Plan (NAP) on PCVE and Local Action Plan at the provincial and municipal level;
   (ii) lack of strong leadership and political will in the provincial and municipal due to security issues; and
   (iii) unsystematic intervention program with no long-term goals.

6. Among the recommendations put forth to overcome these challenges were to enhance push factors such as incentives, resources and support by the federal government in order to galvanise the local government participation, and to strengthen community-led efforts by supporting the reintegration programmes in local communities.

7. He viewed that the implementation of Indonesia’s NAP 2021-2023 should focus on ability and capacity of the local multi-stakeholder actors, underscoring the importance

to strengthen the shifting paradigm from national to local level, as well as from single into multiple implementer actors.

8. **Mr. Maarten De Waele** presented the European experience of the Evaluation and Mentoring of the Multi-Agency (EMMA) project which was aimed at addressing violent radicalisation and terrorism in Germany, the Netherlands and Belgium. The technicalities of the EMMA process are divided into two parts: (i) scientific evaluation; and (ii) mentoring.

9. He further deliberated on the mentoring aspect such as using peer-to-peer network in the process. Also underlined were a few pertinent factors that are significant in contributing towards the success of the EMMA project such as:

(i) strong relationships and networks between partners in multi-agency work (MAW);
(ii) high transparency in each respective role, scope and vision among the multidisciplinary team;
(iii) grasp of up-to-date knowledge and expertise on various forms of radicalisation; and
(iv) standardisation toward a more effective monitoring and evaluation process.

10. **Dr. Murni Wan Mohd Nor** discussed hate speech and extremist discourse in Malaysia from the legal perspective. Dominant themes of hate speech in Malaysia are mostly concentrated on topics concerning race, religion, nationality, and the monarchy. While there is already a framework on the matter, the present intervention mechanisms are focused on measures taken only after an incident has occurred, such as punitive means via existing law. Instead, an early intervention and a comprehensive action plan, including relevant legal reforms, are necessary to address hate speech and extremism.

11. Dr. Murni underscored the importance of a whole-of-society collaboration among various stakeholders including government, media, civil society organisations, and academia. She also stressed the importance of a contextualised approach, whereby local needs and grievances are considered to better counter hate speech and extremism. Also emphasised was the importance of dialogue to encourage open and effective discussions on various issues.

12. She also mentioned that coordination and collaboration at all levels are needed to ensure that action plans and strategies are carried out successfully. The success of the implementation should consider sufficient incentives, resources, and support. Local communities are an integral part of the coordination, whereby they should function as primary actors, and not just supporting roles.

13. Mr. De Waele stressed that Monitoring and Evaluation (M&E) of PCVE programmes would allow practitioners to gather valuable input in measuring desired outcomes. The M&E stage may be multi-disciplinary in nature, calling for strengthened networks between actors involved, so that more knowledge can be gathered in better understanding the complexities of violent radicalisation.

14. Dr. Murni emphasised on the need for specific legislation in combating hate speech. A clear and comprehensive framework is needed with considerations towards defining hate speech and other key terms, categorisation according to nature and gravity of the offence, and issues of intention, among others.

15. Lastly, all speakers emphasised the importance of dialogues between various groups to allow greater understanding of contesting and competing views. Mediums such as sports and culture hold great potential to be leveraged to unify people of different backgrounds.

INTERACTIVE Q&A SESSION:

16. The session featured three questions from the floor. The first question was directed to Mr. Banerjee on the challenges of measuring the effectiveness of sports in countering extremism. In his response, Mr. Banerjee acknowledged the challenges of coming up with scientific measures to measure the use of sports in countering terrorism and extremism. He elaborated that the use of sports as a platform to mediate and rehabilitate might not produce immediate results. However, sporting activities help construct narratives to counter violent extremism.

17. A question from the floor enquired about experiences in applying gender perspectives in the respective speakers' research and/or programmes. In the EMMA project, the gender element could be seen from the mothers and wives of the terrorists that left their family to join terrorist groups in the Middle East. This angle has assisted EMMA in understanding the stories, grievances and frustrations of the family members. Meanwhile, Dr. Murni underscored that hate speech is constructed and exposed to youths and children at home by insensitive parents through the use of stigmatised or derogatory terms. Therefore, it is imperative to educate parents to address the issue of hate speech that is often rooted within communication (or lack thereof) between parents and children at home.

18. Mr. Taufik briefed that a working group was established to mainstream gender perspectives by encouraging discussions about women and children in the Indonesian National and Local Action Plan. Apart from that Mr. Banerjee saw the potential roles of women as mentors and mediators to reconcile conflicting parties.

19. The final question from the floor sought the panellists' opinion on whether there will be more individual or group terrorists in the foreseeable future. Mr. De Waele and Mr.Taufik agreed that both types of terrorism are expected to be seen. Mr. De Waele shared that one of the most prominent terrorist groups in Belgium, *Sharia4Belgium* is expected to continue to expand as a group in Belgium as part of their aim to expand the network of terrorism in the country and region. In addition, Belgium witnessed lone-wolf terrorism cases, where the individuals involved were radicalised through social media. Mr. Taufik also shared that a terrorist group in Indonesia known as *Darul Islam*, which has been around since Indonesia's independence, may have close to two million members, despite recently being less active.

PANEL 3:

DIGITAL STRATEGIC COMMUNICATIONS: COUNTER/ALTERNATIVES NARRATIVES

S.I.C
2023
DIGITAL STRATEGIC COMMUNICATIONS: COUNTER/ ALTERNATIVE NARRATIVES
DR. CÁTIA MOREIRA DE CARVALHO
MS. DWI RUBIYANTI KHOLIFAH
MR. PRIYANK MATHUR

SPEAKERS
Mr. Priyank Marthur
Founder & Chief Executive Officer
Mythos Lab, the United States

Dr. Cátia Moreira de Carvalho
Research Fellow
University of Porto, Portugal

Ms. Dwi Rubiyanti Kholifah
Country Director
Asian Muslim Action Network, Indonesia

Mr. Asrul Daniel Ahmed
Director of Digital Strategic Communications
SEARCCT, Malaysia

MODERATOR:
Mr. Thomas Koruth Samuel
Consultant for UN Agencies, Malaysia

SUMMARY:

The panel discussion emphasised on credible, compelling, and convincing narratives in efforts to challenge violent extremist narratives. Panellists discussed the current usage of the internet globally and how it has changed the approach used by terrorist groups in promoting their messages, the challenges faced by governments and CSOs in formulating counter/alternative narratives, as well as initiatives and programmes that have been implemented by some of the organisations represented in the panel. Some of the initiatives shared were the combined use of edutainment, media and information literacy, and Artificial Intelligence (AI). The panel also shared on how extremists employ "gamification" techniques in spreading their propaganda through the use of in-game chats and gaming adjacent platforms.

DISCUSSION:

1. The first panellist, **Dr. Cátia Moreira de Carvalho**, explained that countering terrorist messages online has become a challenge now that their propaganda has reached previously inaccessible populations. Dr. Carvalho proposed several measures to counter them, including blocking terrorists' content online, promoting digital resilience and media literacy, and using Inoculation Theory and Frame Alignment Theory.

igital counter and alternative
nessages to terr ist content:
Effectiveness and ys forward
Cátia Mo o
14 J

2. Dr. Carvalho cited the lack of evidence on the effects of online content on cognitive and behavioural change, as well as the possibility of exploitation by nefarious actors, including blowback effects, as obstacles to creating online content.To address these obstacles, Dr. Carvalho proposed a number of approaches, such as conducting impact and assessment studies on interventions, investing in evidence-based practices, and pursuing a holistic approach to combating terrorist propaganda.

3. The second panellist, **Ms. Dwi Rubiyanti Kholifah**, centred her presentation on the micro-aspects of providing alternative narratives to violent extremism. Ms. Rubiyanti demonstrated how the three forces of Globalisation, Fundamentalism, and Militarism (GFM) have manifested as patriarchal expressions, which is the belief that males have dominance and control over the lives of women. According to her, GFM intersects with patriarchy to restrict the full manifestation of women's rights in many parts of the globe. She provided a sobering assessment of how terrorist groups manipulate women in multiple ways, including sexual violence, misogyny against women, and the disintegration of protective social networks.

4. Furthermore, Ms. Rubiyanti highlighted the various forms of violence, threats, and discrimination that women face, such as a lack of women representation in human rights issues, a lack of access to justice for women, bullying, social exclusion, and the instrumentalisation of women's bodies, particularly those who are part of the jihad circle. Asian Muslim Action Network Indonesia (AMAN) collaborates with various

parties in Indonesia, including Islamic-based institutions, relevant women's groups, professionals, higher education institutions, Islamic boarding schools (*pesantren*), and *Majlis Ta'lim*, in order to address the aforementioned issues. Positive progress has been made in discussing a variety of issues, including a greater understanding of Islam and Islamic terms. For instance, the term *Ulama* (cleric) can refer to both males and females, and the experiences and knowledge of women can be taken into account when interpreting Islamic law.

5. In addition, Ms. Rubiyanti suggested some key elements in formulating a gender-justice narrative in Preventing Violent Extremism (PVE). Some of these elements are the paradigm in which women are considered in interpreting Islam and policy formulation, and the methodology in formulating a narrative that supports women's rights with reference to the Human Rights Framework and Islamic texts. In this context, AMAN has created a website named *Kupipedia* (www.kupipedia.id) that serves as a communications platform for PVE.

6. The third speaker, **Mr. Priyank Mathur**, described the evolution of extremist narratives since 2012 and drew parallels with contemporary narratives. In 2012, narratives were more religious and sermon-like, multimedia was sombre and of low quality, and communications were significantly more centralised. Meanwhile, extremist narratives at present are more geared towards pop culture references and parodies that appeal to Gen Z audiences.

7. In addition, extremist groups have utilised "gamification" techniques in their propaganda, promoting their messages through in-game conversations and gaming platforms such as Discord and Twitch. Mr. Mathur proposed "edutainment" as a solution to the challenges posed by current extremist content, along with media and information literacy, while embracing Artificial Intelligence (AI) technology for counter-messaging.

8. **Mr. Asrul Daniel Ahmed**, in his presentation, discussed the Zurich London Recommendations that suggest good practices in PCVE online, content and communications-based responses, as well as shaping national conversations with the media. In addition, Mr. Asrul emphasised the importance of both online and offline approaches to mitigate the influence of violent extremism online through education and awareness, building resilient communities, and direct intervention.

9. Mr. Asrul also touched on sports-based PVE interventions, gender-related violent extremism, AI-adjacent platforms, and generative AI, and briefly shared the relevant initiatives and programmes conducted by SEARCCT.

10. Wrapping up the panel presentations, Ms. Rubiyanti stressed that the key elements mentioned need to be taken into consideration when formulating a gender-justice narrative for PCVE. It is important to pay attention to the requirements, narrative, and social networks, as well as the nuances and grey areas when producing effective content.

11. Mr. Mathur viewed that “Edutainment” should be explored as one of the means for counter-messaging, and called for the need to enhance media and information literacy, especially with the rise of technologies such as AI.

12. Mr. Asrul also shared the view that exchanges between local and national levels with a strong emphasis on data protection policies and mechanisms, as well as collaborations between technology developers and regulatory bodies are needed to promote AI literacy.

INTERACTIVE Q&A SESSION:

13. Three questions from the floor were fielded by the moderator for the panellists. A participant noted that there was little discussion regarding the target group, i.e., the general population, vulnerable populations, and those who are already exposed to propaganda, as well as the various tactics or criteria required to target these groups. Dr. Carvalho acknowledged that this was a problem with disseminating counter-narratives online, as it targets the general population, and that the impact of these contents on individuals is uncertain. She added that counter-narratives tend to be more effective with sympathisers of the movement, but not necessarily with radicalised individuals. Through deradicalisation and disengagement, distinct strategies must be employed. Dr. Carvalho concluded that this is also the reason why some programmes fail, as strategies that work for some individuals may not work for others.

14. Mr. Asrul was of the opinion that counter-narratives aimed at a broader audience can be ineffective and that exchanges with CSOs would aid PCVE efforts in gaining a better comprehension of local sentiments. He then proposed exchanges between the local and national levels with a strong emphasis on data protection policies and mechanisms, particularly considering the risks of information leakage and misuse, which could in turn impact existing PCVE efforts.

15. Mr. Mathur emphasised the importance of determining the host of the content and platform based on the targeted audience. He pointed out that agencies or transnational organisations that invest in counter-messaging campaigns must be willing to not take credit for their content by claiming it as their own. Ms. Rubiyanti, citing examples from the Women Ulama with whom she had worked, stated that the age of the audience and the topics of discussion were crucial considerations when developing content, particularly if the topics were relatable to the audience.

16. The form of counter-narratives required to achieve this balance was questioned. Mr. Mathur further elaborated that an underlying emotional need must be addressed when formulating counter-messages. Mr. Asrul stated that efforts must be made to engage the media in order to constructively combat the media’s formulation of the issues surrounding violent extremism and its association with culture and religion.

17. Dr. Carvalho emphasised that the evolution of extremism must be monitored in order to come up with proper strategies, methods, and measures to counter it. She discussed the 3N theory (needs, narrative, and networks) and the need to pay attention to the nuances and ambiguities of individual cases rather than generalise a profile.

18. At the end of the Q&A session, a participant brought up the difficulty of creating an effective counter-narrative, particularly considering the advancement of technology and AI, as well as the UN Secretary General's call for the establishment of a global regulatory body under the UN to govern AI. Mr. Mathur stated that although the establishment of such a body is supported; there is a gap that needs to filled, particularly on AI literacy among policymaker which can be built through capacity-building programmes. Mr. Asrul shared that while many are in favour of such calls, there are also concerns that a lack of comprehension may lead some to opt for a "blanket ban." There is a need for close cooperation between the tech creators and members of this regulatory body.

PANEL 4:

THE ROLE OF MEDIA AND INFLUENCERS IN PCVE

SPEAKERS:
Assoc. Prof. Ts. Dr. Jessica Ong Hai Liaw
Faculty of Defence Studies and Management
National Defence University of Malaysia (NDUM), Malaysia

Mr. Matt Love
Co-Founder & Director
Love Frankie, Thailand

Ms. Tiffany Jane Buena
Information Officer
Department of National Defense of The Philippines

Mr. Muhammad Saiful Alam Shah Sudiman
International Centre for Political Violence and Terrorism
Research (ICPVTR), RSIS, Singapore

MODERATOR:
Dr. Farizal Razalli
Advisor & Director
Strategic Research & Analytics
Ab & Artho, Malaysia

SUMMARY:

The panel discussion highlighted the multidimensional nature of social media and elaborated on its extensive social effects, ranging from promoting mass communications to entrepreneurship. Some of the negative effects, such as cyberbullying and dissemination of false news were also discussed. The need for greater collaboration between traditional and new media illustrated the significant role and impact of media and influencers on shaping narratives and influencing public opinion. The panel emphasised the significance of government and media cooperation for effective information dissemination. Also highlighted was the significance of funding and international partnerships for maintaining the visibility and prominence of religious influencers online.

DISCUSSION:

1. The first speaker, **Dr. Jessica Ong**, began her presentation by describing the various modes of communication, such as in-person and virtual. These modes of communication differ in terms of their effectiveness. In addition to influencing enterprises and making the world more accessible, digital transformation has altered the way people communicate.

2. She then emphasised the significant impact that social media influencers have on youth in today's digital world. This posed an ethical dilemma regarding the methods employed by influencers to gain more followers.

3. The speaker also illustrated the adverse impact of social media such as cyberbullying. Experiences with cyberbullying are also associated with mental health disorders such as depression and anxiety that can lead to family problems, academic difficulties, or even violence.

4. She added that laws such as Anti-Fake News Act (2018), Printing Presses and Publications Act (1984), and the Communications and Multimedia Law (1998) are vital in ensuring a safe digital space and social media environment for everyone. In Malaysia, Safer Internet Day (SID) celebration was first held in 2010 and initiated by CyberSecurity Malaysia, under the CyberSAFE initiative where various programmes and activities are organised together with partners who embrace cyber security and internet safety agenda in Malaysia. SID 2023 Malaysia Edition suggested the theme of a smart community through the "Siber Malaysia Madani" campaign where digital citizens are urged to practice good manners, good ethics, have high educational knowledge, and have wide knowledge in the field of cyber security by cultivating the concept of digital citizenship within the community.

5. The second speaker, **Mr. Matt Love**, illustrated the importance of creating positive narratives that focus on cultivating community's resilience against violent extremism, as well as hate speech on social media. He further stated that understanding the locally-relevant resilience factors against violent extremism is crucial to develop appropriate strategies and steps to counter such threats.

6. The speaker continued by emphasising the importance of engaging with youths on PCVE, especially after findings have shown that younger people (aged 17-25 years old) are most likely to support violent extremism. At the same time, the same age group, however, is also the most "swayable" if they are exposed to positive messaging that is strategically delivered to them.

7. Accordingly, the speaker underscored that creative campaigns by the right messengers, especially influencers, will go a long way in delivering the positive messages to the masses, particularly the youths. The speaker opined that youth leaders, civil society leaders and influencers are the front-liners in the battle of narrative that is shaping up in the social media sphere. This can also be combined with potential youth at grassroot level, who can also be developed into campaigners and activists.

8. The speaker then focused his attention on the nexus between extremism and gaming, the latter being arguably the most profitable entertainment sector worldwide, with more than USD$196.8 billion in revenue for the year 2022 and 2.81 billion active gamers, corresponding to 25% of humanity. He further illustrated that gaming is not only restricted to entertainment per se, as many gamers are increasingly involved in creating nascent gaming communities which work as social spheres by utilising adjacent gaming platforms such as Twitch and Discord.

9. The speaker then proposed several specific steps to be considered in the endeavour against violent extremism, as follows:

(i) Work alongside youth influencers to build messages for their own communities;
(ii) Invite everyday youths into research process of establishing projects fighting against violent extremism, which in turn will inspire them to do more for their own communities;
(iii) Since alternative narratives alone are not enough to sustain a movement, explore the path of also covering peripheral issues in communities in order to build a more equitable and peaceful society;
(iv) Convene strategic supporters to create an ecosystem that will turn youths into life-long advocates; and
(v) Develop partnerships with social media platforms.

10. The third speaker, **Ms. Tiffany Jane Buena**, began her presentation by outlining the PCVE challenges in the Philippines context, which is facing numerous internal conflicts due

to ethnic, political, socio-economic, sectarian, and religious frictions that led to further destabilising threats of terrorism and transnational criminal activities. The Philippines is also facing the menace of misinformation, disinformation and malinformation which created the perilous conditions that make it a relatively challenging country for journalists and media practitioners.

11. The speaker then presented the "communications perspective" in which stories and narratives can be utilised to create a better world. She elaborated on the power of the "fourth estate" which is the traditional media and journalism institutions, in setting and framing the perspective towards PCVE.

12. This traditional influence is being challenged by the "digital third place", online digital spaces in which youth converge. This digital third place relies on social media, citizen journalists and influencers for relatable content and information. As such, governments need to build a modicum of trust with the fourth estate and the digital third place in creating a positive public narrative against violent extremism.

13. She then illustrated the power and influence of media in public life, whereby stories and narratives are framed in such a way that they are successful in capturing the public attention. Highlighting the Philippines' experience in facing the Marawi Siege, she underlined the importance of media in feeding the public with correct information regarding the reality on the ground, albeit within the boundaries and ground rules created by the government.

14. The speaker elucidated the consequent importance for governments to collaborate with and leverage the power of media and influencers. This is due to the fact that these two media components can better deliver positive narratives to the target audience, further necessitating continued cooperation with them moving forward.

15. In leveraging the power of media and influencers, the speaker emphasised several elements that warrant further attention, namely (i) developing high-quality content; (ii) nurturing external champions; (iii) conveying one message but using many voices; (iv) promoting community engagement and empowerment; and (v) tapping into human interests.

16. The fourth speaker, **Mr. Muhammad Saiful Alam Shah** started with a novel perspective on influencers that is rather uncommon in discourses related to social media, namely the significant role played by digital religious influencers as messengers of peace. These include influential preachers and clerics who hold sway over their followers and congregants through effective use of social media platforms.

17. The speaker elaborated his assertion by referencing to the “GUSDURian movement” which strives to espouse former President of Indonesia, Abdurrahman Wahid’s (Gus Dur) principles of justice and inclusivity in order to divert people away from violence and expand their energy to serve mankind. Accordingly, many religious influencers do not create digital contents by themselves; rather, these are created by both their followers and haters.

18. The speaker then identified religious figures as individuals who possess religious knowledge, which endows them with authority in the eyes of their followers.Nevertheless, there are some controversial religious figures who used their stature to propagate hate, motivated by skewed interpretation of their own religions, historical grievances, perceived threats as well as their desire to gain control over the populace.

19. Additionally, the speaker presented an example of Singaporean Muslims’ efforts to create a digital platform for millennial religious teachers to propagate positive religious messages, known as Asatizah Youth Network. This group of Singaporean Muslim millennials aimed to make a positive impact on the lives of Muslim millennials by enhancing community engagements, disseminating positive messages via social media, writing bite-sized articles as well as creating videos and podcasts.

20. The speaker then stressed the possibility of creating an effective platform to prevent and counter violent extremism through collaboration between platform providers and religious influencers. Platform providers’ expertise on technological tools can be shared with religious influencers who can then utilise them to create valuable contents that can be shared with a much wider audience.

21. The speaker then concluded his presentation by enumerating several issues faced by digital religious influencers in trying to impact positive changes to societies. These issues include distrust of funding from other countries due to perceived hidden agendas, the professed secularism of international organisations which makes them reluctant to work with religious figures, as well as the struggle for digital religious influencers to attain visibility and prominence that can eclipse hateful influencers.

22. Concluding the panel presentations, Ms. Tiffany viewed that there must be greater collaboration among traditional and new media, including social media influencers and citizen journalists. She further deliberated that multi-stakeholder collaboration among nations in the region is needed to increase funding and resources for digital influencers. This could assist in enhancing their visibility and creation of impactful content. Mr. Love reiterated the potential use of multiplayer gaming and adjacent platforms for positive interventions.

INTERACTIVE Q&A SESSION:

23. During the Q&A session, three questions were raised, namely on (i) how Singapore measures its level of vulnerability towards PCVE; (ii) how can the authorities better understand the new generation's perspective; and (iii) effectiveness of traditional media collaboration work in this new era.

24. In answering the first question, Mr. Saiful noted that Singapore government does not publicly share any data and statistics on PCVE, thus causing an information vacuum regarding Singaporeans' vulnerability towards violent extremism.

25. Mr. Love stated that we need to develop better understanding of the new generation and their preferred forms of communication. He stressed that experts and authorities need to delve deeper into online behaviours of the new generation and figure out the factors that are driving positive resilient behaviours on online platforms.

26. Responding to the third question, Ms. Tiffany was of view that the traditional media is shifting its modus operandi in which it now naturally gathers its cues from social media to get more compelling news out. Governments need to empower and train citizen journalists and influencers so that these influential individuals can present the truth in a way that will not harm people.

27. The moderator summarised the session by providing key takeaways from the discussion, as follows:

(i) The need to humanise the narrative against violent extremism to get the message across;

(ii) The importance of more high-impact partnerships involving all relevant stakeholders;

(iii) Empowering the masses with the right resources to build resilience against violent extremism; and

(iv) Producing more collaborative contents based on the utilisation of the right resources.

PANEL 5:

DEVELOPING DIGITAL RESILIENCE: STRATEGIES AND BEST PRACTICES

SLC 2023
PANEL 5
DEVELOPING DIGITAL RESILIENCE: STRATEGIES AND BEST PRACTISES

SPEAKERS:
Mr. Hernán Longo
Regional Programme Coordination Officer
United Nations Office of Counter-Terrorism (UNOCT), Thailand

Ms. Rachel Fielden
International Project Manager
Moonshot, United Kingdom

Ms. Adilah Junid
Director, Legal and Government Affairs
Microsoft, Malaysia

Dr. Nicole Matejic
Principal Advisor, Digital Safety, Regulation & Policy
Department of International Affairs, New Zealand

MODERATOR:
Assoc. Prof. Dr Danial Mohd Yusof
Principal Researcher
Extremism Analytical Research Unit, ISTAC-IIUM, Malaysia

SUMMARY:

The session discussed the role of United Nations (UN) frameworks and initiatives, such as the Global Digital Compact and UN Policy Brief on Information Integrity on Digital Platforms, in addressing the global challenges and opportunities arising from the digital revolution. The discussion also cast light on gaming's dual role as a platform for digital resilience and a breeding ground for extremist ideologies. In addition, Microsoft's digital resilience strategies were discussed, with an emphasis on the collective responsibility to reduce online safety risks while maintaining freedom of expression, privacy, and security. There was also an emphasis on the need for partnerships with local administrations and CSOs to combat online threats, as well as advocacy for the inclusion of "Dissuade" in the PCVE framework.

DISCUSSION:

1. **Mr. Hernán Longo** started his presentation by providing a wider context of the current global counter-terrorist threat landscape as captured in the 16th Report of the Secretary-General of the UN on the threat posed by the Islamic State and Daesh.This document stated that terrorism remains a threat globally. Despite changes in leadership and diminishing cash reserves, major groups like Daesh and al-Qaeda have remained resilient and very active in the past couple of years. This is particularly observed in certain parts of the African contintent.

2. Mr. Longo also elucidated the growing impact of extreme right-wing terrorism, which has been designated as a major and rapidly expanding terrorist threat in certain nations. This group uses information and communication technologies extensively. Mr. Longo asserted that the issue of ICT misuse has been a primary concern in all significant anti-terrorism and PCVE initiatives.

3. In relation to Artificial Intelligence (AI), Mr. Longo provided examples of how AI has been used to create fake identities, social media profiles, deep fakes, spread propaganda, and spread false information while concealing the perpetrators' identities. Mr. Longo further explained that "The New Agenda for Peace" demonstrated the UN Secretary-General's awareness of the need for a new agenda for peace to address the numerous challenges that the international community faces today, for which he stated that we must redouble our efforts and identify effective means and significant steps for risk management. The Global Digital Compact will define a shared principle for an open, free, and secure digital world for everyone.

4. **Ms. Rachel Fielden**, in her presentation, highlighted the potential of gaming as a tool for developing resilient strategies. She stated that because of technological advancements, extremist organisations are better able to coordinate attacks, disseminate propaganda, and recruit members. Tapping into the potential use of gaming in PCVE, she emphasised that gaming, whether pursued casually or as a leisure, can contribute to the development of digital resilience.

5. Ms. Fielden also discussed the propagation of extremist ideology on gaming platforms and provided examples of games that have been utilised to combat misinformation and disinformation. She argued that gaming affords a one-of-a-kind opportunity to address physical limitations, linguistic obstacles, and cultural differences that may impede traditional methods of interaction. Gaming facilitates the development of digital resilience by providing a more direct, private, and secure method of engagement.

6. Ms. Fielden also presented on the Moonshot-created game *'Gali Fakta'* as a tool to combat the spread of misinformation and disinformation. The goal of this game is to promote permanent behavioural and attitude changes among participants, illustrating profound effect games can have on human behaviour.

7. She suggested that gaming, especially online gaming, has transformed passive participation into active participation. This transition can be leveraged to educate users effectively about the dangers of radicalisation. Games provide an exceptional opportunity for intervention in a more subtle, familiar, and entertaining manner.

8. Ms. Fielden continued by stating that over the past five years, numerous games have been created to combat online dangers. Some of the examples are 'Bad News Game', 'Harmony Square', and 'Decount'. These games varied in style and design, incorporating scenarios, frictional elements, cartoon graphics, and real-world elements.

9. The third presenter, **Ms. Adilah Junid**, began her presentation on Microsoft's approaches to combating violent extremism online and building digital resilience by quoting the keynote address delivered by the Deputy Foreign Minister, Datuk Mohamad Alamin on the Digital Resilience Initiative which has a lot of resonance with Microsoft's practices.

10. Ms. Adilah provided examples of digital resilience strategies that have been contextualised by referencing how they may apply to a specific community and the collaborative efforts Microsoft has made to achieve this, citing Xbox Ambassador programmes and a safety toolkit that was co-created with stakeholders including the government and civil society.

11. Microsoft's framework for dealing with extremist content consists of four pillars. These pillars should not be regarded separately, as they all contribute to achieving the objective.

(i) platform architecture;
(ii) content moderation;
(iii) having the appropriate culture; and
(iv) collaboration.

12. She further elaborated that the economic model of a platform can have a significant effect on its security. Platforms that adopt an engagement-based business model, for instance, may induce unique user behaviours, necessitating the application of unique risk mitigation strategies.

13. She also provided an example of safety by design, a prominent philosophy in consumer services. The digital community strongly encourages parents to utilise this function to promote a safe environment and a positive gaming experience for their children. It provides family-safety features and additional settings, such as the ability to personalise the experience and build guardrails.

14. Moving on to the next pillar, content moderation plays a crucial role in promoting safety by having clear policies, consistently enforcing those policies, and providing transparency regarding the outcomes of those policies. Content moderation is not limited to the detection of infringing content; it must be an end-to-end process that ensures the content adheres to the specified policies. Microsoft's annual Global Online Safety Survey revealed that 85 percent of respondents expected some form of filtering for detrimental and illegal content.

15. Ms. Adilah further explained that Microsoft uses both automated and human content moderation to prevent some content from appearing on the services. Both proactive and reactive modes of moderation exist. The majority of proactive moderation is automated and is able to flag problematic online conduct that contravenes the terms of service and its code of conduct.

16. To truly empower users to set norms and standards for online behaviour, the culture pillar can only be accomplished through collaboration with other stakeholders, as it reflects diverse digital bases. Culture is often neglected as a safety factor, but as online spaces develop their own cultures and communities, distinct cultural norms emerge.

17. Ms. Adilah provided an example of the Xbox Ambassadors programme, which encourages gamers to cultivate positive engagement within their community by treating other gamers with respect and welcoming newcomers. This is an example of exhibiting the appropriate behaviours and practices that result in positive social environment and experiences.

18. The collaboration pillar demonstrates how establishing digital resilience necessitates cooperation between all stakeholders. One example of this is the development of the toolkit for gaming safety, a collaboration between Microsoft New Zealand, the government and civil society. The collaboration aimed to equip parents with an age appropriate toolkit to help their children develop positive experience as well as provide valuable case studies, such as warning signs to look out for and implementation strategies.

19. **Dr. Nicole Matejic** continued the session by challenging the conventional PCVE framework, where emphasis is put on the types and influences that lead people towards and away from violent extremism. The general understanding of violent extremism has always been that a deep commitment to an extreme ideology is the driving force. In her presentation, Dr. Matejic suggested a shift of focus from ideologies that people generally adopt to roles and influences that underpin and support radicalisation.

20. She also elaborated on how viewing radicalisation through an agnostic lens permits a nuanced understanding of the process and the role that extreme, overvalued beliefs play in justifying or abandoning violence. This perspective considers radicalisation to be on a continuum, in which individuals may progress towards or away from these beliefs. It examines the intricate interplay of personal, social, cultural, and political factors that shape a person's worldview and susceptibility to acquire extreme, overvalued beliefs.

21. Radicalisation can occur in various directions and intensities. She recognised that individuals may go through different phases, such as initial exposure to radical ideas, gradual adoption and intensification of extreme beliefs, and potentially a process of disengagement or deradicalisation. This process also implies a dynamic process in which individuals can be influenced by others, both in radicalising or disengaging directions.

22. Dr. Matejic also emphasised the significance of pre-suasion and pre-bunking as innovative PCVE framework approaches. "Pre-suasion" is described as a process by which a person's experiences and knowledge predispose them to be receptive to particular ideas and beliefs. "Pre-bunking" involves proactively introducing counter-narratives and information that challenge extremist ideologies before individuals come into contact with them. By understanding how individuals can be influenced and using this knowledge to dissuade and immunise against extremist ideologies, an online community that is more informed and critical can be cultivated and promoted.

23. Concluding the panel presentations, Mr. Longo emphasised that relevant stakeholders such as policymakers, tech corporations and the youth should work collaboratively and expansively, resulting in an established multilateralism network.

24. Ms. Fielden elaborated that in order to implement interventions that can effectively combat online harm, the potential of gaming as a means to construct resilient strategies should be looked into through leveraging the interactive nature of games and their influence on behaviour.

25. Ms. Adilah stressed that digital resilience should be promoted as a potent tool for achieving a positive experience in the digital world by providing users with all the necessary knowledge and skills. Each stakeholder's unique contribution to the advancement of digital resilience should be recognised.

26. Dr. Matejic stressed that given that the propagation of extremist ideas or the process of disengagement can occur through human interactions, social networks, or exposure to ideological narratives and propaganda, radicalisation should thereby be countered in its early stages.

INTERACTIVE Q&A SESSION:

27. The session gathered five questions from the audience. The first question was for Dr. Matejic on the good practices of debunking to be implemented by the programming industry players. In response, she said the good practices of debunking involve conducting research to understand the specific misinformation issues, tailoring debunking efforts accordingly, communicating accurate information effectively, and collaborating with relevant

stakeholders. These practices can help programming industry players effectively combat misinformation and contribute to a more informed society.

28. The second question posed was on effective collaboration in the Malaysian context. Ms. Adilah mentioned an example of collaboration between Microsoft and the Malaysian government, where Microsoft pledged to train one million Malaysians within a year. This initiative aimed to prepare both fresh graduates and existing industry players for digital technology adoption in the coming years, ensuring that they are future-ready. The collaborative effort between Microsoft and the Malaysian government is a prime example of how collaboration can drive Malaysia's social and economic benefits, where the initiative contributes to the development of a competent workforce that is equipped to embrace digital technologies and thrive in the evolving job market.

29. The next question was asked to Mr. Longo on the current state or trend of terrorism. He answered that while numbers seemed to be declining, it could be linked to the pandemic. The concern remained on what would happen after the pandemic as people start to travel due to freedom of movement. For the past couple of years, the use of the internet and ICT for terrorism purposes has increased exponentially due to the reliance on technology. However, there were several very successful counter-terrorism operations, particularly in Indonesia and the Philippines. He cautioned that terrorist threats in the region still exist, and the need to stay vigilant is imperative.

30. Another question was directed at Ms. Fielden, inquiring whether she had witnessed any kind of change in the narrative as per Moonshot's research on deradicalisation efforts. Using Indonesia as an example, she and her team saw a growing distrust of government institutions in the online sphere, particularly regarding their handling of the pandemic.

31. The last question inquired on the Player Versus Environment (PVE) space as some were not familiar with the idea of gaming to be the frontline of digital resilience, and how to close the gap between past gamers and the current generation of gamers. In response, Ms. Fielden recommended two initiatives: (i) to collaborate with the actual game practitioners, people who really understand gamification, and (ii) to adapt to the fast-changing gaming world. Ms. Adilah added that it is best to collaborate with people who develop gaming platforms because they are the one who look after the platforms.

LUNCHEON TALK SESSION:

ARTICULATING A MADANI FRAMEWORK FOR COUNTER-EXTREMISM

SPEAKER:

Professor Emeritus Datuk Dr. Osman Bakar
Holder of Al-Ghazali Chair of Epistemology and Civilisational Studies
and Renewal
International Institute of Islamic Thought and Civilisation (ISTAC-IIUM), Malaysia

MODERATOR:

Assoc. Prof. Dr. Danial Mohd Yusof
Principal Researcher
Extremism Analytical Research Unit, ISTAC-IIUM, Malaysia

SUMMARY:

The speaker highlighted the concept of ‘middleness’ as the raison d’etre of civilisation and an effective antidote to extremism. The middle path, as he argued, existed across cultures and religions including Islam, Christianity, Buddhism, and Hinduism, making it applicable in a multi-cultural and multi-religious society like Malaysia. The speaker called upon scholars and policymakers to continue the discourse on ‘middleness’ and “Madani” to create a civilised and moderate society, which would serve as a shield against violent extremism.

DISCUSSION:

1. The luncheon talk started with Dr. Danial explaining that the speaker was intimately familiar with the concept of “Madani”, and has contributed numerous articles to the discourse on the topic. Since Madani is a policy framework introduced by the Prime Minister of Malaysia, it is appropriate to discuss how this concept can be integrated into preventing and countering violent extremism (PCVE) from the Malaysian perspective.

2. In his introduction, Professor Emeritus Osman explained the cultural perspective of the Madani concept in PCVE. According to him, the concept of “Madani”, loosely defined as “civilisation”, appears in both Eastern and Western philosophies. Al-Farabi, a scholar of the philosophy of society and religion who introduced the “science of Madani/civilisation” to humanity, was the originator of this concept from the East. Meanwhile, in the West it was Samuel Huntington who published “The Clash of Civilisations” to explain global politics in the post-Cold War era.

3. He continued by stating that nation-states must adopt a civilised approach to human issues, including extremism. He emphasised that extremism and civilisation are intertwined, and that pursuing civilisation would aid in the fight against extremism. He argued that the conventional approach to combating extremism lacked a qualitative approach; thus, a new and innovative approach from a civilisation perspective was necessary to resolve problems facing humanity.

4. In the context of Malaysia, he mentioned that the Madani framework under the leadership of the Prime Minister Dato’ Seri Anwar Ibrahim can be found in the 2022-published book “SCRIPT: For a Better Malaysia – An Empowering Vision and Policy Framework for Action”. This framework serves as a guide for addressing contemporary issues in the nation, including PCVE. The framework is divided into six pillars, namely, Sustainability, Care and Compassion, Respect, Innovation, Prosperity, and Trust. He emphasised that in addressing the issue of extremism, it is also necessary to examine the six pillars’ underlying principles, such as “unity” and “middleness”.

5. On the topic of unity, he explained the significance of openness, pluralism, and interdependence. He believed that an inclusive strategy is essential for addressing a variety of human issues as it would facilitate the integration of diversity in societies and, ultimately, enhance the quality of life for all individuals.

6. Concluding his presentation, he reminded that the Madani concept is an on-going discourse. Using the framework outlined in the SCRIPT, he urged all academicians and policymakers to continue researching the "Madani" concept, including its application in PCVE.

INTERACTIVE Q&A SESSION:

7. A question was posed to the speaker to elaborate more on the concept of "middleness". Professor Emeritus Osman explained that every religious belief has its own traditions that reflect on 'taking on the middle path'. He argued that people are naturally inclined to avoid extremes. In Islam, for instance, the terms 'wasatiyyah' and 'ummatan wasatan' denote 'middle community'. In addition to Islam, he emphasised that Buddhism, Hinduism, and Christianity each have their own definitions of 'middleness,' which has been fundamental to civilisation and is one method for avoiding extremism in the society. In the Malaysian context, he suggested that a framework for Malaysia's approach to 'middleness' could be established if all religions in Malaysia could come together through dialogue.

8. The moderator in his intervention stated the Madani concept is viewed as a continuance of previous Islamic policies in Malaysia, such as Islam Hadhari. Some individuals did not view Madani as a perpetuation of national policies or frameworks such as '1Malaysia' or 'Keluarga Malaysia'.

9. Professor Emeritus Osman emphasised that Madani is pertinent to all Malaysians, not just the Muslim population. Nonetheless, he acknowledged the challenge in assimilating the Madani concept into Malaysia's multiracial fabric. Furthermore, the similarities and distinctions between Islam Hadhari and Madani are so universal that the concept of Madani could be "globalised" in the future.He concluded that Madani paves the way for additional dialogue, particularly among all religions in Malaysia.

THE RAPPORTEURS COMMITTEE

HEAD OF RAPPORTEURS
MOHD HASRIL ABDUL HAMID

COORDINATOR OF RAPPORTEURS
KENNIMROD SARIBURAJA

MEMBER OF THE RAPPORTEURS COMMITTEE
KHAERIAH ZAEHERA ABD KAYYUM
JASMINE MOHAMED JAWHAR
MOHD ZHAFRIE JOHARI
THANGESWARY PALESWARAN
IZZATI AISYAH ADNAN
NUR ANIS FITHRAH AHMAD RUMAINI
NUR NAZURAH MOHD NASIR
AHMAD SHUKRI AL HILMI AHMAD FARIS
MUHAMMAD IKHWAN FADHLAN MD NAZIMAN SHAH
AMIR HAMZAH MOHD NASIR
AWANG SYAZUAN SHAFIQ AWANG JAYA
SYARAFINA ADILAH AHMAD NASIR
MUHAMMAD AFIQ ISMAIZAM
NURUL HIDAYAH MOHD NOAR

PART 3

ARTICLES BY SPEAKERS AND MODERATORS

DIGITAL COUNTER AND ALTERNATIVE MESSAGES TO EXTREMIST CONTENT: EFFECTIVENESS AND WAY FORWARD

Cátia Moreira de Carvalho

ABSTRACT

This paper examines the potential effect of two different types of online messages to counter and prevent extremist content online. Counter messages aim to challenge extremist content, through the delegitimization and deconstruction of extremist content. This type of message comes with challenges as it is a reaction that might have the opposite effect: cause resistance and have no change on the extremist behaviour at all. On the other hand, alternative messages are positive messages, which aim to tell a different story, without causing resistance or challenging extremist beliefs and ideology. Despite the massive use, a comprehensive study has demonstrated that counter narratives do not work and do not produce the intended effect, which is to prevent extremist behaviour. As such, this paper examines how counter messages and alternative messages might work, through the analysis of two theories: the Inoculation Theory and the Frame Alignment Theory. To conclude, it is offered some recommendations to improve this area of preventing and countering violent extremism (PCVE): investment in evidence-based practices and in impact assessment of interventions, as well as work in an active collaboration with social media and online platforms, governments, civil society organisations, the academia, and the community.

Keywords: counter messages, alternative messages, extremism, terrorism, effectiveness

INTRODUCTION

THE USE OF INTERNET BY EXTREMIST ACTORS

In July 2023 a new milestone was achieved: the internet use reached over 5 billion people, which means that 64.5% of the global population are now online and have access to online platforms (Kemp, 2023). In terms of social media use, the numbers are also impressive: almost 5 billion people have a profile or use social media platforms (Kemp, 2023). This means that more and more people can communicate rapidly around the world without leaving the comfort of their home. However, the benefits of the internet have also been leveraged by extremist actors, to pursue their intentions and disseminate their ideology.

Terrorist organisations, such as the Islamic state, have been using the internet to recruit and radicalise (Zeiger and Gyte, 2021). The use of internet by terrorist actors shows a completely different approach from older, traditional terrorist organisations: they recruit around the world, get in contact with previously unreachable populations, incite people to commit attacks without leaving their home country, and disseminate their seductive messages and ideology in various social media platforms, with attractive, contemporary design (Stern and Berger, 2015). Extremist lone actors have also been keen on using online platforms. For instance, the Christchurch attacks in New Zealand was live-streamed on Facebook by the terrorist at the same time of the attacks, to an international audience composed of his followers (Macklin, 2019). Afterwards, Facebook reported that it removed 1.5 million videos of the attacks (Facebook Newsroom, 2019).

Indeed, extremist actors have been creative and innovative in using social media and online platforms to pursue their goals through very different means. And, although some online platforms have implemented measures to prevent extremist content from going online, many terrorist organisations have been adaptable to circumvent the imposed restrictions.

PREVENTION OF ONLINE EXTREMIST USE: A CHALLENGE

Preventing the spread of online extremist use comes with many challenges. First, it is difficult to impose required measures as social media and online platforms are privately owned and controlled, meaning that they are not always responsive to the legislative and policy requirements of governments and international organisations (Stern and Berger, 2015). Since usually policy makers are not experts on new technologies and the internet, there seems to be a misunderstanding of how these platforms operate, what is possible to implement and how to keep up the pace of new emerging technologies (Zeiger and Gyte, 2021). This results in limited responses and recommendations that are not adequate to the reality. In this vein, a closer collaboration between social media and online platforms and governments is required to produce more effective responses.

A second challenge concerns the amount of extremist content published and shared online. More and more extremists use internet and social media platforms to their own benefit and to leverage their agenda, by disseminating their narratives and propaganda. This is connected to the third challenge: extremist actors use as many platforms as possible to reach previously inaccessible populations, in different languages, all over the world. This makes it virtually impossible to contain and prevent extremist presence online (Zieger and Gyte, 2021).

Although it is very difficult to prevent extremist use of the internet, some attempts have been made to prevent its spread. For instance, blocking online content and barring online access to extremist actors, as well as filtering and removing content have been measures promoted to directly contain extremist content. Nevertheless, these measures also pose some challenges: it is required appropriate resources to remove content. There is a lack of experts on language and cultural issues to deal with nuanced extremist content in different languages, blocking and barring access to social media platforms not only makes it more difficult for extremist actors to use these tools, but also for the general population, and, finally, blocking access will make extremist actors to look for alternative social media platforms (Zieger and Gyte, 2021; Elkin-Koren, 2020; Steckler, 2018; Stern and Berger, 2015).

The extremist use of the internet has made many people perceive this technology as an enemy to the fight against terrorism. However, internet and social media platforms can be seen as viable and reliable partners in preventing and countering violent extremism. In this vein, more positive measures can be promoted, such as the promotion of digital resilience and media literacy, to equip the general population with strategies to be more resilient to extremist content, and the development of counter messages and alternative messages. These last two measures will be analysed in the next sections of this paper.

THE USE OF COUNTER MESSAGES: DO THEY WORK?

The use of counter messages has been widely promoted as a tool to tackle extremist content online and to prevent radicalization and extremism. Counter messages aim to directly or indirectly challenge extremist messages, through online and offline interventions (Briggs and Feve, 2013).

Some recommendations on how counter messages might work are to take into consideration the local context in which the target audience is placed, to make sure to include the specific grievances and needs of said context, tailor the counter message to a specific audience, and include attractive and correct content, to both captivate the target audience's attention and to send the right message (Zieger and Gyte, 2021). According to these authors, this can be achieved through the deconstruction and de-legitimization of extremist content and undermining of its credibility.

Although recent years have seen an increase in the implementation of counter messages, some authors question their potential to prevent individuals from radicalising. For instance, Schlegel (2020) notes that while most of the propagandistic content is produced to be used by extremist groups' followers, exposure to extremist content is not a necessary condition for radicalisation. However, most of the counter narratives programmes are designed with this assumption in mind.

In order to inspect the potential of counter narratives programmes and its effectiveness in preventing violent radicalisation, Carthy et al. (2020) conducted a systematic review. This comprehensive study demonstrates that the impact of counter narrative interventions is very limited or has no impact at all on reducing the risk of violent radicalisation. Moreover, the authors state that an ineffective counter narrative might have exacerbating effects of radicalisation, causing resistance to the counter messages, and amplifying the problem (Bell, 2015; Carthy et al., 2020).

Additional challenges of counter messages are the superficial assessment and impact evaluation of the interventions already implemented, and a blowback effect. In other words, extremist actors might use counter messages to make their arguments more public and divert attention from the counter arguments (Schmid, 2014; Zeiger and Gyte, 2021).

To avoid the challenges mentioned before, one way counter messages might work is to apply the assumptions of the Inoculation Theory (McGuire, 1961). Similar to medical vaccines, this theory posits that preemptively exposing people to a weakened dose of a specific persuasive argument could confer psychological resistance against future exposure to persuasive arguments of the same nature, conferring resistance and protection in the future (McGuire, 1961). Research has demonstrated that Inoculation Theory seems to be a robust framework to counter persuasion, namely in the context of violent radicalisation (Braddock, 2019; Banas and Rains, 2010).

THE PROMOTION OF ALTERNATIVE MESSAGES: HOW THEY MIGHT WORK

Rather than reacting to the messages of extremist groups, as counter narratives do, positive and alternative messages might be promoted. Alternative messages do not aim to directly challenge the extremist content, but to tell a different story (Carthy, 2021). By doing this, alternative messages can build positive identities, while addressing some risk factors conducive to radicalisation (Zeiger and Gyte, 2021). Indeed, some benefits of alternative messages is to build positive and non-violent messages rooted in the context where the target audience is, and tackle personal and structural drivers of radicalization without causing resistance. Thus, alternative messages seem to be a viable way to prevent radicalisation, aligned and congruent with a more positive, non-violent identity.

This can be achieved through the tenets of the Frame Alignment Theory. This theory posits that frames are simple schemas that people mentally define, to help them to both label and ascribe meaning to the world (Snow et al., 1986). Thus, frame alignment is the correspondence of an individual's interpretive schemas to those of a given social movement, aligning key aspects of the individual's ideologies, goals, and activities with that of the social movement (Snow et al., 1986). In this vein, Frame Alignment Theory is very useful to build alternative messages, as people can be persuaded to support the position of a given movement (positive and non-violent), provided the movement's position is aligned with a separate, but compatible position already held by the individual (Williams and Lindsey, 2014). This way, alternative messages can contribute to creating correspondence between one's own frame and a positive, non-violent frame and identity.

CONCLUSION AND WAYS FORWARD

The aim of this paper is to debate how counter messages and alternative messages might work, their challenges and effectiveness. Although these two types of interventions have been widely promoted to prevent radicalisation to extremism, further investment is still needed to take full advantage of these interventions. As the systematic review developed by Carthy et al. (2020) demonstrate counter messages have very limited impact on preventing violent radicalisation. Despite its ineffectiveness, counter messages are still promoted worldwide, and a large amount of public funding has been invested in their implementation. Thus, the impact of these practices should be rigorously assessed. The same applies to alternative messages. A similar study as developed by Carthy et al. (2020) has yet to be conducted for alternative messages, therefore it is not possible to determine the effectiveness of this practice at the moment. However, this paper strongly recommends the development of such research.

Besides the recommendations to produce effectiveness and impact studies, this paper also suggests the development of counter messages and alternative messages based on evidence and empirical research, to increase the chances and maximise the potential of both measures.

Developing counter messages and alternative messages alone will not solve the problem of extremism or prevent radicalisation. This should be done with the engagement of social media and internet companies, as well with multidisciplinary teams and governmental entities, to produce more realistic and impactful interventions. An often forgotten component of any intervention on prevention and countering of violent radicalisation is the active involvement of the community. The community – both online and offline – is very important as it is the context in which people are and where the drivers of radicalisation can be countered and prevented. As such, interventions in this field should also address the role that the community plays in contributing to maximise the effect of these practices.

Finally, as research has also shown, expectations regarding the effect of these interventions should be lowered and adjusted to reality, as counter messages and alternative messages seem to work better for the general population, or people who are at risk of radicalisation, or who are sympathisers (Carthy et al., 2020). Those who are already radicalised will most likely benefit from different strategies, such as strategies implemented in deradicalization and disengagement programmes.

REFERENCES

Banas, J. A., & Rains, S. (2010). A meta-analysis of research on inoculation theory. *Communication Monographs*, 77, 281–331. https://doi.org/10.1080/03637751003758193

Braddock, K. (2019). Vaccinating against hate: Using attitudinal inoculation to confer resistance to persuasion by extremist propaganda. *Terrorism and Political Violence*, 34(2). https://doi.org/10.1080/09546553.2019.1693370

Bell, P. (2015). ISIS and Violent Extremism: Is the West's Counter-Narrative Making the Problem Worse?. *Influence Online*, 25 June 2015. Available at: https://influenceonline.co.uk/2015/06/25/isis-violent-extremism-wests-counter-narrative-making-problem-worse/.

Carthy, S., Doody, C., Cox, K. O'Hora, D, & Sarma, K. (2020). Counter-narratives for the prevention of violent radicalisation: A systematic review of targeted interventions. *Campbell Systematic Reviews*, 16. https://doi.org/10.1002/cl2.1106.

Carthy, S. (2021). Lessons learned from alternative narrative campaigns. *Radicalisation Awareness Network*. Available at: https://home-affairs.ec.europa.eu/system/files/202203/ran_lessons_learned_from_alternative_narrative_campaigns_032022_en_1.pdf

Elkin-Koren, N. (2020). Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence. *Big Data & Society*, 7(2). https://doi.org/10.1177/2053951720932296

Facebook Newsroom (17 March 2019). Available at: https://twitter.com/fbnewsroom/status/1107117981358682112.

Kemp, S. (2023). Digital 2023 July global statshot report. *DataReportal*. Available at: https://datareportal.com/reports/digital-2023-july-global-statshot

Macklin, G. (2019). The Christchurch attacks: Livestream terror in the viral video age. *Combating Terrorism Center Sentinel*, 12(6). Available at: https://ctc.westpoint.edu/christchurch-attacks-livestream-terror-viral-video-age/

McGuire, W. J. (1961). The effectiveness of supportive and refutational defenses in immunizing and restoring beliefs against persuasion. *Sociometry*, 24, 184–197.

Schlegel, L. (2020). The ongoing trouble with counter-narratives: Why evaluation may not be everything. *European Eye on Radicalization*. Available at: https://eeradicalization.com/the-ongoing-trouble-with-counter-narratives-why-evaluation-may-not-be-everything/

Schmid, A. P. (2014). Al-Qaeda's 'Single Narrative' and Attempts to Develop Counter-Narratives: The State of Knowledge. *The International Centre for Counter-Terrorism*. Available at: https://www.researchgate.net/publication/285546585_Al_Qaeda's_Single_Narrative_and_Attempts_to_Develop_Counter-Narratives.

Snow, D. A., Rochford, E. B., Worden, S. K., & Benford, R. D. (1986). Frame alignment processes, micromobilization, and movement participation. *American Sociological Review*, 51, 464-481. https://doi.org/10.2307/2095581

Steckler, S. (2018). Why Facebook is Losing the War on Hate Speech in Myanmar. *Reuters*. Available at: https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/.

Stern, J. & Berger, J. M. (2015). *Estado Islâmico: Estado de terror*. Amadora: Vogais.

Williams, M. & Lindsey, S. (2014). A social psychological critique of the Saudi terrorism risk reduction initiative. *Psychology, Crime and Law*, 20(2). https://doi.org/10.1080/1068316X.2012.749474

Zeiger, S. & Gyte, J. (2021). Prevention of radicalization on social media and the Internet. In *Handbook of Terrorism Prevention and Preparedness* (Ed. Alex Schmid). Available at: https://www.icct.nl/handbook-terrorism-prevention-and preparedness

DIGITAL RESILIENCE, CVE AND EMERGING TECHNOLOGIES

Farlina Said

ABSTRACT

Definitions of resilience has legal and scientific roots. It could mean a restoration of the original legal situation or the elasticity and springiness of solid bodies. There can be an element of disaster and recovery in constructing a resilient framework. For instance, the OECD risk and resilience framework looks at the ability of households, communities and nations to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty (OECD, n.d). However, radicalisation in the digital space can take place in cognitive openings from identity and self-formation. This would mean that a digital resilience framework may have to be closer to the UK Council for Internet Safety's Digital Resilience Framework that defines resilience as 'a process to harness resources to sustain wellbeing' (UK Council for Internet Safety, n.d.). However, the way the internet and technologies shape identity have not been fully explored. Further as technology becomes a part of personal and societal lives, its impact on identity-formation may be significant. On such a landscape, radicalisation efforts could have specific push and pull components exacerbated by identity incoherence vulnerabilities. Thus, this paper aims to (i) examine the way the internet and technologies shape identity, and (ii) identify vulnerabilities in this process that impact radicalisation.

Keywords: digital resilience, violent extremism, OECD, radicalisation, digital space

WHY IDENTITY, RADICALISATION AND THE DIGITAL REALM?

This paper does not aim to do justice to the great breadth of work already completed by psychoanalysts, sociologists and radicalisation scholars in this field. Rather, this piece aims to articulate the shifting dynamics of identity formation ignited by technology and provide some thoughts to how the shape and form of technology have transformed the way individuals think of themselves. An example would be the mobile phones that at the turn of the millennium seem a luxury but today is so interconnected with the average person that to part may feel like the severance of a phantom limb. Technologies have yielded great optimism for development. There is a digital economy worth US$1 trillion by 2030 that serves as a goal for ASEAN (Google, Temasek, Bain and Company, 2022). A 2018, Pew Research Center research saw the positives of a tech-saturated world to be the ability to build connections, enhance commerce and improve the government's delivery of services (Rainie, 2018). This means, humanity will have access to more information, decreased barriers to education and enhancement in scientific progress (Rainie, 2018). However, digital deficits are inclusive of harmful cognitive and emotional consequences (especially with constant intrusive connectedness), greater isolation due to an inability to build strong relationships with others and information overload (Rainie, 2018). Some impacts of technological adoption on the individual have explored by past scholars. For instance, there is the association between screen time and depression (Madhav, Sherchand, and Shercan, 2017), an increase in 'depression' and 'anxiety' article searches in the age of digitalisation (Teepe, Glase, & Reips, 2012), increases in depressive symptoms and suicide-related outcomes (Twenge, Joiner, Rogers, and Martin, 2017) while social media use could lead to emotional problems (Vuorre, Orben, and Przybylski, 2021). Meanwhile, digital transformation saw exacerbations in disinformation (Guardian, 2023), algorithmic bias (Heilweil, 2020), cyberbullying (Ybarra and Mitchell, 2004) and mistrust in institutions (Maati, Edel, Saglam, Schlumberger, and Sirikupt, 2023). Misinformation and disinformation activities could impact social cohesion thus increasing risk for extremism in society ((Maati, Edel, Saglam, Schlumberger, and Sirikupt, 2023); (Colley, Granelli, and Althuis, 2020)). Additionally, policies and studies have explored how those with low self-esteem, discriminated or who may feel judged by their culture or depressed as those at risk to radicalisation thus vulnerable to the acceptance of violence (Devon Children and Families Partnership, n.d.; Wright and Hankins, 2016).

Digital spaces and tools have benefited terrorists and criminals. Widespread internet access, end-to-end encryption and virtual private network (VPN) have allowed for instantaneous communication (Harrison, 2018), increased capacities for recruitment and more logistical awareness to carry out global attacks (UNICRI and UNCCT, 2021). A United Nations Office of Counter-Terrorism and Integrated Crime and Justice Research Institute report stated how digital connectivity were used to recruit, raise and move funds, buy and transfer weapons as well as make tutorials or instruments for members (UNICRI and UNCCT, 2021). Further, Daesh in Syria had experimented with weaponising self-driving cars and drones (UNICRI and UNCCT, 2021). The usage of internet for radicalisation occurs with increasing internet penetration. A report on countering internet radicalisation in Southeast Asia published in 2009 articulated how extremists drew on narratives to attack governance arrangements of regional states (Bergin, Osman, Ungerer, and Yasin, 2009). Taking a look at Southeast Asia, the recorded number of radical and extremist websites in Bahasa and Malay rose from 15 in 2007 to 117 in 2008, whether these are forums, sympathetic blogs and social networking accounts or websites manned by radical groups (Bergin, Osman, Ungerer, and Yasin, 2009). However, it is Daesh's prevalence in recruitment that exemplifies the efficacy of the digital spaces. Daesh's information strategy maximised the digital space to deliver high quality promotional video clips, develop and distribute online magazines and as well as manipulate platforms such as Twitter to enhance dissemination techniques (NATO Strategic Communications Centre of Excellence, 2015). NATO's Strategic Communications Centre of Excellence stated Daesh uses three categories of narratives to achieve appeal: political, religious and social narratives. The first delivers political narratives such as the oppression of Muslims by Western powers or the need to establish a governance system such as a Caliphate. The second are religious narratives aimed at invoking religious duty of Muslims while the last looks at the promise of a better life targeted to young people who feel abandoned or desiring significance (NATO Strategic Communications Centre of Excellence, 2015).

There can be correlation between belonging, identity and radicalisation. Wiktorowicz's analytical model based on British Extremists supports the idea of participants identifying meaning in radical forms of Islam (Torok, 2020) with the socialisation process as the final step of identity construction and value changes (Wiktorowicz, 2013). Borum's Four-Stage Model articulates how grievances eventually turn into distancing and devaluations of specific groups (Torok, 2020). Particularly, a sense of injustice, a search for identity and an individual defining his or her identity through group membership may be motivational and vulnerable factors to radicalisation (Borum, 2004). Further, belonging in a group gives a sense of connectedness and affiliation, which could stabilise and consolidate one's identity

(Borum, 2004). This would prove important with Festinger's experiment with misinformation and conspiracy theories. Meanwhile, Moghaddam's staircase has significant floors for the displacement of aggression and moral engagements (Torok, 2020) which are components to address moral inhibitions. However, such correlations are not absolute. Borum cautioned that general explanations can suffer from critical shortcomings, especially as the process of radicalisation can depend on the individual and ultimately, available social networks. However, studies have shown a correlation between identity as a vital component of radicalisation. Thus, begins this paper to explore how technologies and the digital environment impact identity formation; and what are the trends of vulnerabilities that should be addressed.

IDENTITY, TECHNOLOGY AND THE DIGITAL ENVIRONMENT

The first question to ask, is what is identity? The way individuals think of themselves or identify themselves would have a large influence on their associations with groups. However, examining identity itself can be complex. John Locke's articulation of personal identity that constitutes the continuity of the self and memory, were particularly important to place responsibility for justice because a person would have to be the same to be accountable for past deeds ((Locke, 2004); (Izenberg, 2016); (Gordon-Roth, 2019)). Academic psychology after the 1970s distinguished between 'Self' and 'Identity' where 'Self' is the total person or the experiencing subject while identity is the 'self-concept' or how someone consciously defines himself (Izenberg, 2016). Erik Erikson adds to this where personal identity is based on the "immediate perception of one's selfsameness and continuity in time; and the simultaneous perception of the fact that others recognise one's sameness and continuity" (Erikson, 1980). Further, Erikson articulated stages for the development of ego identity, among which are years in search of identity or identity versus identity confusion (WebMD, 2023). Adolescents develop a philosophy of live to establish a coherent, nuanced sense of career, moral, ethic, religious, political and sexual identity with purpose an enduring personal meaningful commitment that one hope to accomplish or work in life (Bronk, 2011). Snow and Anderson in their research to understand how the homeless generate identity and measure self-worth and dignity articulated identity consists of social identity, personal identity and self-concept (Snow and Anderson, 1987). Social identities are attributed to others to situate them as social objects. Personal identities are the meanings attributed to the self by the actor while the self-concept feature the overarching view or image of themselves (Snow and Anderson, 1987). Cohesion in identity is identified by the idea of identity work, which refer to the range of activities individuals engage to create, present and sustain personal identities (Snow and Anderson, 1987). While Erikson's literature state that identity crisis is normal and is a part of development, there can be the view that identity certainty would help a person reject incongruent self-evaluations (Villines, 2023). Examples given are of people capable of rejecting bullying due to a stronger sense of identity or the propensity of identity confusion and uncertainty leading to mental health issues such as depression and anxiety (Villines, 2023).

Discourse theories that aim to understand identity through cultural and social forces could be useful to examine frameworks shaping the individual (Cover, 2016). Thus, the work of Michel Foucault and Judith Butler would be useful to understand the interaction between external environment and the person. Foucault's Technologies of the self aimed to look at how humans developed knowledge about themselves hence able to take steps to renouncing parts of the self (Foucault,1988). Yet the significance in the body of literature is in describing ways philosophy, religion or even pedagogic texts have become part of rationality constructs (Lemke, 2000) and to undermine the notion of a free, liberal subject (Cover, 2016). Meanwhile, Judith Butler's work on performative identities indicate how identities are performed to certain norms (Cover, 2016). Thus, the individual that could be in search of identity could also be performing such identities via social-networking profiles or choosing experiences online (Cover, 2016). Attributes to determine identity can be categories such as gender, race, ethnicity, sexuality, nationality, citizenship and socioeconomic status (Cover, 2016). Suggested by Foucault are steps for self-care which includes developing perceptions of the self (Foucault, 2001).

TECHNOLOGIES, DIGITAL SPACES AND IDENTITY

The digital space and its related technologies have become a vital realm for identity development. However, digital technologies may challenge traditional approaches to identity formation. Cyberspace can be characterised by the physical, logic, information, and people layer (Clark, 2010); with each bearing different types of influences capable of shaping an individual's identity. For instance, the physical layer which are physical devices or components can determine access or enhance digital divides. Identity and inclusivity can be determined by access to technologies and digital services. The logic layer shapes the internet, thus are the strings of code that combine databases with the Web or could be the protocols programming access. For some examples of influence on identity formations, the logic layer could contain algorithmic contortions that skew search outputs or suggest content on a platform. The logic layer delivers what is needed on the information layer, which is the layer of data, user interface and content. The information consumed can introduce ideologies, symbols and stereotypes that oversaturate individuals with information. Lastly, is the layer of people which define and use cyberspace (Clark, 2010). In some paradigms, the people layer could be explored further between the physical user and online avatars. The people could build networks online, be it physical user or online personas. As such, could shape the development of self and identity.

There has to be a way to view the subject in an environment of interconnected submarine cables, burgeoning content generation and constant communication. In mid-1990s, Thompson following the tradition of hermeneutics, stated that the formation of the self is a symbolic project the individual actively constructs (Thompson, 1995). Viewing each individual as biographers of self-identity indicates the possibility of the individual drawing on various sources to form a sense of self; among which is the media (Thompson, 1995). Thompson's literature stated that individuals will find methods to organise the self, which would include methods to sift through large amounts of information – for instance relying on verified or close networks such as friends and family as sources (Thompson, 1995). Thompson's views on the self in a mediated environment are important to feature subjects as actors communicating in digital spaces rather than being passive receivers. Rob Cover's work in digital communication and identity aim to articulate this further, where an individual's activities online can be seen as identities in performance bound by norms and limits determined by platforms and may be susceptible to surveillance from others (Cover, 2023). However, there are elements of digital spaces that are out of control which may be the impetus for moments of incoherence in identity. For instance, a person scrolling through the "project of selfhood" spanning months or years may reveal aspects of the identity that could have changed or the individual curating their identity performance could reveal an alternative story emerging from relational engagement such as tagging with others (Cover, 2023). The outcome of a rapidly shifting and disruptive environment may be identities in states of incoherence or incongruence. Furthermore, as algorithms are not within the control of users, users are subjected to content delivered by platforms. In such situations, the coherence of a ‘for you page’ reflecting the combination of social identity, personal identity and self-concept may not be possible due to data management access, privacy issues and trade secrets.

This process of identity formation in digital spaces meets the ongoing phenomenon from the digital environment: the information disorder. The internet, social media and algorithms have introduced newer disruptions impacting the individual’s ability to organise information. The information disorder is caused by human inattention, low media literacy, bots and disinformation factories. If such information or news is carried out by verified media without sufficient fact-checking processes, the exposure rates for misinformation is higher (Pennycook and Rand, 2021). Pennycook and Rand state that political identity can skew abilities to discern truth from falsehood. However, they mentioned it is important to note that politics does not trump truth as political affiliations may not indicate the veracity of news (Pennycook and Rand, 2021). Information provided by people viewed as credible along with the strength of elite messaging are contenders as main drivers of misinformation. However, social media related feedback such as ‘likes’ also increases belief in news content (Pennycook and Rand, 2021). However, there can be a correlation between misinformation, disinformation, prevalence of conspiracy theories and community-building. Festinger’s theory on cognitive dissonance observed a cult who believed in the coming for the end of the world. However, when the end of the world did not occur, the cult began proselytising to enlist social support for the cause, thus adding consonant elements to restore consonance (Suls, n.d.). This could mean that in experiencing cognitive dissonance for a specific worldview, people may seek confirmations of their worldview thus building associations to uphold specific viewpoints.

RADICALISATION, DIGITAL SPACES AND DIGITAL RESILIENCE

Identity makes powerful motivations in radicalisation. Thomas Samuel’s observation Daesh’s messaging among an Indonesian audience used religion where Daesh quoted hadiths and ideological affinities (Samuel, 2016). Among the hadiths was a prophecy for Daesh’s birth, stated to be foretold as the final stage in the five stages of Islam (Samuel, 2016). In Malaysia, Thomas Samuel added personal motivations such as ‘thrill-seeking’ ideas, the need for ‘self-redemption’ and obligations to stand up and fight for their Sunni kin as motivating factors to join Daesh (Samuel, 2016). This would result in Daesh’s success in delivering messages drawing 102 Malaysians to travel to Syria between 2013 and 2018 (Yusa and Azmi, 2018). The digital environment introduces new factors shaping identities are formed. Thus, building digital resilience may have to consider shoring resilience and coping mechanisms for identities in flux. Thus, building digital resilience means addressing tensions in identity formation that could equip individuals with the capability the self-assess. The effort of delivering tools for retrospection and building self-perception also needs to be accompanied by constant value systems on ethics and compassion. While digital resilience may address how individuals address external environments, it should also focus on how individuals could arrest the slide down the slippery slope themselves.

REFERENCES

Bergin, A., Osman, S. B., Ungerer, C., & Yasin, N. A. (2009, March). *Countering internet*. From ASPI: https://ad-aspi.s3.ap-southeast-2.amazonaws.com/import/9_22_46_AM_SR22_Countering_internet_radicalisation.pdf?VersionId=gf6cEpmNIYq8IeDBRKdz9o2Idi4FEpEm

Borum, R. (2004). *Psychology of Terrorism*. Tampa: University of South Florida.

Bronk, K. C. (2011). *The role of purpose in life in healthy identity formation: A grounded model*. From CGU Scholar: http://scholar.cgu.edu/wp-content/uploads/2017/03/role-of-purpose-chapter.pdf

Clark, D. (2010, March 12). *Characterising cyberspace: past, present and future*. From MIT: https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf

Colley, T., Granelli, F., & Althuis, J. (2020, Autumn). Disinformation's Societal Impact: Britain, Covid and Beyond. *Defence Strategic Communications, 8*. From ResearchGate: https://www.researchgate.net/publication/342709609_DISINFORMATION'S_SOCIETAL_IMPACT_BRITAIN_COVID_AND_BEYOND

Cover, R. (2016). *Digital Identities: Creating and Communicating the Online Self*. Oxford: Elsevier.

Cover, R. (2023). *Identity and Digital Communication: Concepts, Theories, Practices*. New York: Routledge.

Devon Children and Families Partnership. (n.d.). *Child abuse Radicalisation extremism*. From Devon Children and Families Partnership: https://www.dcfp.org.uk/child-abuse/radicalisation-and-extremism/

Erikson, E. H. (1980). *Identity and the Life Cycle*. New York: W. W. Norton & Company Inc.

Foucault, M. (1988). *Technologies of the Self: A Seminar with Michel Foucault*. (L. H. Martin, H. Gutman, & P. H. Hutton, Eds.) London: Tavistock Publications. From https://monoskop.org/images/0/03/Technologies_of_the_Self_A_Seminar_with_Michel_Foucault.pdf

Foucault, M. (2001). *13 January 1982 Second Hour. The Hermeneutics of the Subject: Lectures at the College De France 1981-1982*. New York: Picador.

Google, Temasek, Bain&Company. (2022). E-Conomy SEA 2022: *Through the waves, towards a sea of opportunity*. From Google: https://services.google.com/fh/files/misc/e_conomy_sea_2022_report.pdf

Gordon-Roth, J. (2019, February 11). *Locke on Personal Identity*. From Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/locke-personal-identity/

Guardian. (2023, February 17). *The Guardian view on disinformation online: a 21st-century growth industry*. From Guardian: https://www.theguardian.com/commentisfree/2023/feb/17/the-guardian-view-on-disinformation-online-a-21st-century-growth-industry

Harrison, S. (2018, March 22). *Evolving Tech, Evolving Terror*. From Center for Strategic and International Studies: https://www.csis.org/analysis/evolving-tech-evolving-terror#:~:text=Technological%20Capabilities,with%20which%20radicalized%20individuals%20mobilize.

Heilweil, R. (2020, February 18). *Why algorithms can be racist and sexist*. From Vox: https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency

Izenberg, G. (2016). *Identity: The Necessity of a Modern Idea*. Philadelphia: University of Pennsylvania Press.

Lemke, T. (2000, September). *Foucault, Governmentality, and Critique*. From Thomas Lemke Web: http://www.thomaslemkeweb.de/publikationen/Foucault,%20Governmentality,%20and%20Critique%20IV-2.pdf

Locke, J. (2004, January 6). *An Essay Concerning Humane Understanding, Volume I*. From Project Gutenberg: https://www.gutenberg.org/cache/epub/10615/pg10615.html

Maati, A., Edel, M., Saglam, K., Schlumberger, O., & Sirikupt, C. (2023, July 6). *Information, doubt, and democracy: how digitization spurs democratic decay*. From Taylor&Francis Online: https://www.ztandfonline.com/doi/full/10.1080/135
10347.2023.2234831

Madhav, K., Sherchand, S. P., & Shercan, a. S. (2017, December). *Association between screen time and depression among US adults*. From National Library of Medicine: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5574844/

NATO Strategic Communications Centre of Excellence. (2015). Daesh Information Campaign and Its Influence: Results of the Study. (M. R. Zgryziewicz, Ed.) Riga, Kalciema iela, Latvia: NATO Strategic Communications Centre of Excellence. From NATO Strategic Communications Centre of Excellence: https://stratcomcoe.org/cuploads/pfiles/daesh_public_use_19-08-2016.pdf

OECD. (n.d). *Risk and resilience*. From OECD: https://www.oecd.org/dac/conflict-fragility-resilience/risk-resilience/

Pennycook, G., & Rand, D. G. (2021, May). The Psychology of Fake News. *Trends in Cognitive Sciences, 25*(5), 388-402.

Rainie, J. A. (2018, April 17). *The Future of Well-Being in a Tech Saturated World*. From Pew Research Center: https://www.pewresearch.org/internet/2018/04/17/the-future-of-well-being-in-a-tech-saturated-world/

Samuel, T. K. (2016). *Radicalisation in Southeast Asia: A Selected Case Study of Daesh in Indonesia, Malaysia and the Philippines*. Kuala Lumpur: The Southeast Asi Regional Centre for Counter-Terrorism.

Snow, D. A., & Anderson, L. (1987). Identity Work Among the Homeless: The Verbal Construction and Avowal of Personal Identities. *The American Journal of Sociology, 92*(6), 1336-1371. From https://www.researchgate.net/publication/249173990_Identity_Work_Among_the_Homeless_The_Verbal_Construction_and_Avowal_of_Personal_Identities

Suls, J. (n.d.). *Cognitive Dissonance of Leon Festinger*. From Britannica: https://www.britannica.com/biography/Leon-Festinger/Cognitive-dissonance

Teepe, G. W., Glase, E. M., & Reips, a. U.-D. (2012, April 7). *Increasing digitalisation is associated with anxiety and depression: A Google Ngram analysis*. (O. E. Santangelo, Ed.) From National Library of Medicine: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10081798/#:~:text=Our%20results%20show%20an%20increase,and%20depression%20words%20(r%20%3D%20.

Thompson, J. (1995). *Self and Experience in a Mediated World. The Media and Modernity: A Social Theory of the Media*. Standord: Stanford University.

Torok, R. (2020). Social Media and the Use of Discursive Markers of Online Extremism and Recruitment. In I. R. Association, *Cyber Warfare and Terrorism: Concept, Methodologies, Tools and Applications* (pp. 478-508). Hershey: IGI Global.

Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, a. G. (2017, November 14). *Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time*. From Sage Journals: https://journals.sagepub.com/doi/10.1177/2167702617723376

UK Council for Internet Safety. (n.d.). *Digital Resilience Framework*. From UK Council for Internet Safety: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831217/UKCIS_Digital_Resilience_Framework.pdf

UNICRI and UNCCT. (2021). *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes*. From UN: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

Villines, Z. (2023, February 14). *What is an identity crisis?* (L. Lawrenz, Editor) From Medical News Today: https://www.medicalnewstoday.com/articles/identity-crisis

Vuorre, M., Orben, A., & Przybylski, a. A. (2021, May 3). *There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased*. From Sage Journals: https://journals.sagepub.com/doi/10.1177/2167702621994549

WebMD. (2023, July 29). *What to Know About Erikson's 8 Stages of Development*. (A. Shroff, Editor) From WebMD: https://www.webmd.com/children/what-to-know-eriksons-8-stages-development

Wiktorowicz, Q. (2013). *Joining the Cause: Al-Muhajiroun and Radical Islam*. From Institute of Security Policy and Law: https://securitypolicylaw.syr.edu/wp-content/uploads/2013/03/Wiktorowicz.Joining-the-Cause.pdf

Wright, N. M., & Hankins, F. M. (2016). Preventing radicalisation and terrorism: is there a GP response? *British Journal of General Practice, 66*(647), 288-289. From British Journal of Heneral Practice: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4871284/

Ybarra, M. L., & Mitchell, K. J. (2004, June). Youth engaging in online harassment: associations with caregiver–child relationships, Internet use, and personal characteristics. *Journal of Adolescence, 27*(3), 319-336. From ScienceDirect:https://www.sciencedirect.com/science/article/abs/pii/S0140197104000399

Yusa, Z., & Azmi, H. (2018, October 25). *Malaysia: Widow of Islamic State Fighter Who Died in Syria Comes Home*. From Benar News: https://www.benarnews.org/english/news/malaysian/family-home-10252018170835.html

DEVELOPING MALAYSIA'S NATIONAL ACTION PLAN ON PCVE THROUGH MULTIPLE STAKEHOLDER APPROACHES

Kamarulnizam Abdullah

ABSTRACT

Amid growing terror threats all over the world, many countries have introduced their National Action Plan in Preventing and Countering Violent Extremism (NAPPCVE) as a strategy to address the phenomenon. The adaptation has been part of the United Nations' proposal for each country to design its own NAPPCVE. Malaysia has shown its commitment to introduce its national action and in the process of developing the plan since 2021. Several factors were considered while developing the proposed plan. First, the action plan would not make any reference to a particular religion or ethnic group. Second, it is recognized that Malaysia, since independence, has faced various aspects of violent extremism – ethno-nationalism, politics, and religion. Henceforth, the plan should encompass various aspects of extremist threats. The proposed action plan also took into cognizance of the influence of external elements in spreading extreme ideas and actions in the country. Multiple stakeholders like government agencies, academicians, civil society organization (CSO), religious and political leaders were engaged in drafting the action plan. Focus Group Discussion (FGD) and town hall meetings were among the main methods to solicit their opinion and ideas. Subject to the cabinet approval, the action plan emphasizes several key strategies. Two strategies – prevention and consolidation are briefly discussed in this article. The engagement also shows how the government has transformed its state-centred approach to a more inclusivity in formulating a security policy.

Keywords: national action plan on PCVE, violent extremism, multiple stakeholders, security policy, Malaysia

INTRODUCTION

Combating contemporary violent extremism is challenging and complicated. The world was initially not prepared for these lethal threats. The traditional military's use of force has indeed accelerated the rising numbers of transnational terror groups with defining political and religious objectives. Even major powers like the United States (US) have to admit that their military might would not be able to mitigate the threat. This has been shown in several military missions against so called terror groups targeted in Afghanistan, Iraq, Somalia, and Syria. Under the pretext of either eliminating violent extremist groups like al-Qaeda dan the Islamic State (IS) or toppling a regime that finances state-sponsored terror activities, the US and its allies embarked upon a concerted series of military crush against them. Although these groups or leaders have been crippled, their ideological belief remains and continues to be subscribed to by other affiliated militant groups. Ironically, the targeted countries like Iraq and Afghanistan have to endure a long political instability, constant terror bombings, and humanity crisis.

It has always been argued that the state cannot work alone either through legal or military means to manage the threats (Kamarulnizam Abdullah, 2022; Wildan, 2022; Hikam, 2016; Gunaratna, 2015). States face multiple levels of violent threats. We need a more holistic and inclusive approach by engaging every level of the state operational system – individual, society, enforcement, and policy makers - to work together as part of united force against violent extremism. Eliminating the threats is almost impossible given the dynamic structure of the global system where technology has made communication easier, and ideas are easily spread from one corner of the world to another. Hence, the task is not to eliminate but to prevent and reduce the possibility of violent extremism.

In January 2016, the United Nations (UN) acknowledged the need for a more comprehensive approach in formulating a national action plan in preventing and countering violent extremism. Member countries were given a mandate by the General Assembly to address the dynamism of violent extremist threats. Several countries thereafter introduce their National Action Plan on Preventing and Countering Violent Extremism (PCVE). Indonesia and the Philippines are among the first Southeast Asian countries that have introduced their action plan strategy. The Philippines, for instance, emphasises on "empowering women's organisations to engage in insider mediation and PCVE policy development", while Indonesia focuses a whole societal approach in its PCVE (United Nations Development Program, 2022: 5).

Malaysia, nonetheless, embarked on the plan much later, when in early 2021, the Home Ministry set up a task force and eventually formed a consultative researc group consisting of experts from various local public universities to design the action plan. Although the PCVE action plan was initially being designed by a different ministry, the Ministry of Home Affairs has been tasked by the Malaysian cabinet to come out with a comprehensive national action plan.

Malaysia's PCVE could have been produced earlier if not because of Covid-19 pandemic. Furthermore, calls by several stakeholders including the United Nations and local Civil Society Organizations (CSOs) compelled the government to initiate the task. This paper, therefore, discusses Malaysia's road to develop its own PCVE by highlighting the historical context of earlier approaches, issues and challenges faced to come out with a more all-embracing plan. The article would also highlight two inter-related strategies – prevention and consolidation. All strategies of the NPCE indeed require the involvement of multiple stakeholders. It is argued that a close involvement between government agencies is crucial to ensure the successful implementation of the country's PCVE.

LIVING WITH LEGAL AND PREVENTIVE MECHANISMS

For years, Malaysia adopted two-pronged state approaches in countering terror or violent extremists. This macro approach focused on two main strategies – preventive laws and economic development plan. The legal preventive approaches have been synonymous with the adaptation of the now defunct Internal Security Act (ISA) as the most effective mechanism for the government to "eliminate" violent threats. Initially used by the British colonial forces to address the communist threats, the laws continued to be used by the independent Malayan/Malaysian government as part of security strategies to ensure political and economic stability.

The Economic Development plan was aimed to win the hearts and minds of the people. Winning "the heart and mind" policies like *Keselamatan dan Pembangunan* (Security and Development) or KESBAN, and *Pertahanan Menyeluruh* (Comprehensive Security) or

HANRUH illustrates government’s attempts to use economic development strategies as one of the main pillars in countering extreme terror ideologies particularly from the communist movement. But, if development strategies are not properly executed, it could lead to political tension. The imbalanced economic approaches arguably contributed to the outbreak of the May 13, 1969, racial riots when the Malay-majority population perceived that they were sidelined in the country’s development programs.

But, as the country progresses into a more developed and democratic nation, and the society becomes prosperous, extreme ideological ideas have taken into a different form and derived from various sources. It has been the external sources of extreme ideology with religious overtones that are of major trepidations. Since the September 11 incidents, state strategies need to adapt to the changing nature of extremism. Legal and oppressive approach could not protect a country from rapid spread of extreme violent ideas that transcend beyond borders.

Hence, it is argued that a national action plan is needed to steer the country into a clear direction of new strategy to not only provide a comprehensive mechanism, but also to improve existing initiatives. It has, furthermore, to focus on non-legal preventive measures aiming at averting radical ideas to proliferate in the society.

MOVING TOWARD NATIONAL ACTION PLAN ON PCVE

For Malaysia, despite having a legal mechanism in combating extremism, the adaptation of an all-inclusive action plan has been deferred by various factors.

For years, the government was used to a state legal approach through various laws like the ISA and Emergency Act as preventive measures in countering terror acts. When ISA was repealed and replaced by several new security laws like Security Offences (Special Measures) Act 2012 or SOSMA and POTA (Prevention of Terrorism Act 2015), the due process of law concept was introduced. Yet, it was then argued that to prevent violent extremist activities, preventive mechanisms are still needed to avoid untoward incidents to happen. (Syafique Shuib, 2014; *Berita Harian*, July 28, 2018)

The delay in introducing Malaysia’s national plan on PCVE is also associated with the fluid changes of the country’s political landscape. Yet finally in 2021, it was then decided by the Malaysian cabinet that the Ministry of Home Affairs would become the contact point since it has all the related security agencies like the police, immigration, and Malaysian Maritime Enforcement Agency (APMM) that could effectively enforce the plan.

The consultative committee appointed by the Ministry of Home Affairs commenced its work amid several other challenges. First, were the high expectations by the Civil Society Organisation (CSO) that the action plan should be as inclusive and comprehensive as they could like it to be. A group called *Komuniti Muslim Universal* (KMU), for instance, initiates a website called *Initiate.my* by issuing a policy briefing paper on the possible national plan on PCVE for Malaysia. The group argues that there is an urgent need to draft national PCVE and to engage CSO as check and balance to ensure transparency and democratic process are adopted (*Initiate.my*, 2022). The organisation claims that the policy paper was based on its engagement with various levels of society and organisations.

Second, was the casual relations between Islam and violent extremism, which inevitably produces a global phenomenon of Islamophobia. These delicate correlations need to be addressed carefully by the consultative group for not depicting Islam as the source of extremism in the country. Since the national document will be submitted and deposited to the UN, Malaysia has to be cognisant about this sensitivity. The country, in fact, experienced multiple sources of threat of violent extremism. Violence also occurred due to extreme ethnonationalism and political ideologies. The manipulation of ethnicity or race, for instance, contributed to the intermittent violent actions in the country. The politicising of religious and ethnic issues by self-centred politicians has sparked further the elements of hatred and violence in the society. This has been shown in many incidents like the 1969 May Riots, the 1985 Memali Incidents, and the 2001 Kampung Medan Riots.

On top of that, Malaysia has also been exposed to external and subversive elements that promote violence. Some extreme violent ideas and activities were orchestrated by foreign based movement like Liberation Tigers of Tamil Eilam (LTTE), Abu Sayaf, and Gerakan Aceh Merdeka (GAM) that operate in the country, while other transnational terror movements like al-Qaeda, Jamaah Islamiyah (JI), and IS have used Malaysia as their launching base for regional funding activities.

MULTIPLE STAKEHOLDER ENGAGEMENTS

The societal engagement has been a common practice in developing PCVE all over the world. It has manifold objectives among others, to strengthen awareness especially among the vulnerable especially women and youth. It is believed that youth are,

> *"... generally, much better positioned to promote a culture of tolerance and peace amongst their peers. They possess a talent for communication and mobilization. Engaging and working together with youth as an effective and positive partner continues to be a key priority in Preventing and Countering Violent Extremism (PCVE) policies, programming and capacity-building efforts. (UN Office for Counter Terrorisms, not dated)"*

Additionally, nurture a sense of common responsibility where every member of the community has a role to play. It is a more bottom-up approach where society not only has a role to play in assisting the government to prevent violent extremism, more importantly is that the violent extremism "... in the future depends to a large extent on the establishment of unity and cooperation amongst the authorities and general public." (Aslam, 2021: 65)

In the case of Malaysia, it was a normal practice previously that the state had the monopoly in formulating security related policies. But the government has become more transparent by engaging multiple stakeholders in developing Malaysia's PCVE. It is a welcoming move and a total transformation from the previous approaches. The process of developing Malaysia's PCVE not only involved various government agencies through consultative session, but also series of public engagement like Focus Gorup Discussion (FGD) and town hall sessions with various interest groups like among others *Angkatan Belia Islam Malaysia* (ABIM); *Majlis Belia Malaysia* (MBM); Malaysian Consultative Council of Buddhism, Christianity, Hinduism, Sikhism and Taoism; Christian Federation of Malaysia; Theravada Buddhist Council of Malaysia; and Malaysian Hindu Sangam. Political parties involved included *Parti Islam SeMalaysia* (PAS), the Malay National Organisation (UMNO), *Parti Keadilan Nasional* (PKR), Democratic Action Party (DAP), *Gerakan*, Malaysian Indian Congress (MIC), and *Parti Bersatu*. In short, there were more than fifty experts, CSOs and research outfits that had been involved in this public engagement process.

In addition to that, a survey through online and face to face was also conducted to solicit opinion from the public regarding their concern on violent extremism and terrorism. The findings were partially used by the consultative research group to design and develop questions for in-depth interviews with security experts and policy makers.

The engagement, in fact, has immensely helped the government to devise an all-inclusive approach to PCVE. During an FGD session, for instance, representatives from CSOs agreed that violent extremism should not be associated exclusively with Islam and Muslim community. There was also concern among the Catholic community over the flooding of foreign evangelists who propagated ideologies that were deemed to be incongruent with local cultures and practices. There were also worries, though not confirmed, that some of these evangelist groups were involved in a small movement to promote the idea of independence from the Malaysia Federation. Among the Hindus, there was also concern with the rising influence of Hindutva radicalism.

Another major concern among the CSOs was the tendency of far right political extremism to promote three major sensitive issues– Race, Royal, and Religion- in the country. The majority blamed the "desperate politicking" by some political parties to gain support and power. Despite that, such a strategy has gained traction and become popular in society. Although it is not widespread, the situation could jeopardise the harmony of Malaysian multi-cultural society if attempts are not made to prevent it.

SELECTED KEY STRATEGIES OF PCVE

What are the key strategies that Malaysia should be included in its PCVE? There are several; strategies that would be adopted by the country. But, this article focuses only on the prevention and consolidation aspects since the involvement of multiple stakeholders from individual, society and enforcement agencies are crucial to these strategies.

The famous and popular proverb – prevention is better than cure- clearly describes that for whatever reason we should prevent major security incidents to happen before it happens. Violent extremism can be prevented if we control the early stage of the development of radical ideas itself. In PCVE, we need collaboration and cooperation between state and society to contain the threats. The objective is to develop early intervention programs and strategies through strategic partnership and cooperation between authorities and the local community.

In the advent of globalisation and internet access, the public, especially the youth has been exposed to various sources of uncontrolled information. Ideas that do not conform to the local norms and culture like hedonism, cult, or heretical religious teaching could produce harmful effects in Malaysia's multireligious and multicultural society. In one typical case in the semi-urban area at the northern part of Peninsular Malaysia, for instance, a young but introverted male was involved in supporting and funding extremist groups. Since his parents were separated, the daily activities focused on social media chat groups. Although he did not realise that he was trapped in the militant chat groups, the situation shows how family should become the first line of defence in preventing their children from unwanted ideas and values.

Extreme ideologies could also be spread through peers. It is, therefore, crucial for parents to be ultra-sensitive to any changing pattern of their child behaviour Grossman (2018: 157) argues that "…the role that families and peers can play in detecting early signs of radicalisation and on the importance of early intervention and diversion for young people who may be at risk." Ellefsen and Sandberg (2022: 3) further add,

> "Family members may function as a valuable link between an official exit program and the potential exiter and parents play a key role in establishing parental or family-based community support networks that might assist persons wishing to leave an extremist milieu"

At the same time, the individuals and local community should also be active in their neighbourhood and work closely with the authorities through sanctioned programs like neighbourhood watch and resident association. It is observed that neighbourhood bonding in urban areas has been in decline due to hectic life and work-related factors. This problem needs to be addressed. A sense of togetherness in the community must be invigorated by the local leaders where a close cooperation with the authorities is essential to provide the first line of preventive mechanism for the government.

Preventing early signs of violent extremism also needs close cooperation and understanding among government agencies and ministries. The tasks should not be a burden on the enforcement agencies like the police. Every agency and ministry has its own role. The Ministry of Women, Family and Community, for instance, has a very important position to play in the PCVE. Its function should not be limited only to protect the welfare of the society, but to provide strategies on how local family values should be fortified as part of PCVE prevention strategy. State religious authorities, for instance, should multiply their effort through various programs like Training of Trainer (ToT), where trainers would then be trained with "credible messenger" techniques to counter theological debates on the concepts of *khilafah*, *jihad* and *hijrah*. These concepts have been widely manipulated by extremist jihadi groups to justify their violent actions.

Another important PCVE strategy is on consolidation. The long term of consolidation strategy is forming a more resilient society with a strong national identity. In the immediate term, consolidation strategy is aimed to produce a more responsible Malaysian citizen who could uphold the sanctity of the Federal Constitution, rules of law, Islam as an official religion, and other religions' good moral values.

State and community are working hand-in-hand in achieving this strategy. At the policy level, our educational system requires some readjustment where the elements of patriotism, etiquette, and cultural intelligence should be introduced. Those elements need to be practised from the early stage of childhood education. The sense of patriotism can be achieved through experiential learning where the younger generation practices it through observation, project, songs, and narratives by respected local leaders and experts. Etiquette, and cultural intelligence like tolerance, respecting cultural and religious differences should be fostered and nurtured as part of everyday activities in the classroom rather than being taught as a subject in school. In addition, parents should also be involved in the process by supporting activities through direct and indirect involvement.

Consolidation strategy is also to promote moderation in the society. According to Ahmad el-Muhammady (2019: 134), the concept of moderation of *Wasaṭīyah* is a response "...to the pervasive extremism manifesting itself… either in politics, economics, culture, religion and others." There must be enough moderation narratives in mainstream and social media. The narrative should not be presented as typical government propaganda but rather in the most innovative, entertaining way that could create interest among the general public.

CONCLUSION

While other countries continue to focus on strict legal instruments, Malaysia continues to emphasise more on the soft approach in its PCVE. As mentioned earlier, one of Malaysia's counter-insurgency strategies in the early period of independence was to win the heart and mind of the people. It is crucial to win support from people to counter terrorism during that period. Furthermore, despite being labelled as draconian laws, the ISA did emphasis on the rehabilitation process in its prevention effort. Current ideological threats that promote violent extremism cannot be tackled with enforcement only. Regressive strategy would be backfired especially when dealing with the current extremist ideologies and violence. It is recognised that the hard approach is not the panacea to violent extremism.

In hindsight, the proposed PCVE, unlike the ISA, is more a process of involving every level of society rather than a state's centric legal enforcement. Although the enforcement element is included in the PCVE strategy, it primarily serve as a last resort for taking action against potential radicals in order to prevent violent actions. Its long-term strategy is in fact to create a more resilient society and state, as highlighted in the consolidation strategy, which could withhold existing and future threats of violent extremism.

REFERENCES

Ahmad el-Muhammady. (2019). Applying Wasaṭīyah within the Malaysian Religio-Political Context. *American Journal of Islam and Society* 32 (3), DOI:10.35632/ajis.v32i3.1000

Aslam, M. M. (2021). The critical role of Civil Society Organizations (CSO) in combating terrorism (pp. 63-78). In R. Gunaratna ve M. & M. Aslam (eds.) *Civil society organizations against terrorism: case studies from Asia*. Routledge.

Berita Harian Online. (July 28, 2018). Ambil iktibar kesan pemansuhan ISA - Musa Hassan. https://www.bharian.com.my/berita/nasional/2018/07/454849/ambil-iktibar-kesan-pemansuhan-isa-musa-hassan

Ellefsen, R. & Sandberg, S. (2022). Everyday prevention of radicalization: The impacts of family, peer, and police intervention. *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2022.2037185

Grossman, M. (2018). "The Role of Families and Civil Society in Detecting Radicalisation and Promoting Disengagement from Violent Extremism (pp. 155–70.). In Christian Echle, Rohan Gunaratna, Patrick Rueppel and Megha Sarmah (eds.) *Combatting Violent Extremism and Terrorism in Asia and Europe—From Cooperation to Collaboration*. Konrad-Adenauer-Stiftung and S. Rajaratnam School of International Studies.

Gunaratna, R. (2015). Combating terrorism and extremism: A shift in US approach? *Counter Terrorist Trends and Analyses*, 7, 2 (March 2015), 4-7

Hikam, M. A. S. (2016). *Deradikalisasi: peran masyarakat sipil indonesia membendung radikalisme. Kompas*. https://www.un.org/sc/ctc/focus-areas/countering-violent-extremism/

Initiate.my. (2022). National action plan on preventing and countering violent extremism: civil society deserves a seat at the table. *Policy Brief Issue 1/2022*. https://initiate.my/wp-content/uploads/2022/02/Policy-Brief-012022-v3.pdf/

Kamarulnizam Abdullah. (2022). Navigating Against Salafi-Wahabi expansion in Malaysia: The Role of State and Society" *Studia Islamika*, 29 (2), 1-29

Sabatier, Paul A., (1986). Top-down and bottom-up approaches to implementation research: A critical analysis and suggested synthesis. *Journal of Public Policy*, 6(1), 21–48.

United Nations Development Program. (2022). *Annual report on prevention of violent extremism 2021*. UNDP Crisis Bureau.

United Nations Office for Counter Terrorism. (Not Dated). *Youth engagement and empowerment*. https://www.un.org/counterterrorism/cct/youth-engagement-and-empowerment/

Wildan, M. (2022). Countering violent extremism in Indonesia: The role of former terrorists and civil society organisations. In: Barton, G., Vergani, M., Wahid, Y. (eds) *Countering violent and hateful extremism in Indonesia. New Security Challenges*. Palgrave Macmillan. https://doi.org/10.1007/978-981-16-2032-4_9

Syafique Shuib. (2014, September 21). 'Pemansuhan ISA satu kesilapan, jangan ulangi dengan Akta Hasutan' - Bekas Hakim. *Astro Awani*. https://www.astroawani.com/berita-malaysia/pemansuhan-isa-satu-kesilapan-jangan-ulangi-dengan-akta-hasutan-bekas-hakim-44360

ALL-OF-SOCIETY APPROACH TO ADDRESS HATE SPEECH

Murni Wan Mohd Nor

ABSTRACT

Incidences of hate speech in Malaysia is on the rise and is often triggered by certain events, such as COVID-19 and General Elections. In addition, hateful rhetoric in political communication and problematic media narratives aggravate racial and religious tensions. There is no denying that hate speech has caused further polarization among society, but the current national framework to address this problem is far from sufficient. This paper introduces the complex situation of hate speech in Malaysia by highlighting the major platforms which it thrives, dominant themes within hate speech, as well as considers strengths and weaknesses within the present national framework. The paper concludes by providing an alternative intervention approach focused on collaboration involving all-of-society.

Keywords: hate speech, racism, extremism, PVE, intervention methods.

INTRODUCTION

The multiracial citizens of Malaysia comprise of 68.8% *Bumiputera*,[1] 23.2% Chinese, 7% Indians, and 1% other ethnicities. Like any country, there have been difficulties in maintaining peaceful coexistence between people of different races and religions. However, Malaysia has generally done well in this regard,[2] with low levels of violent crime that has been motivated by racial or religious reasons.

This may be attributed to Malaysia's longstanding commitment towards establishing peaceful inter-racial and inter-religious relations through the formulation of various national policies and related initiatives such as the most recent "Malaysia Madani" introduced by Dato' Seri Anwar Ibrahim. The government also supports the United Nations' pledge to "Leave no one behind," particularly Sustainable Development Goals (SDGs) no. 10 (reduce inequality within and among countries) and 16 (promote peaceful and inclusive societies)—which help to counter hate speech, extremism, and terrorism.

It is promising for those in the field of Prevention of Violent Extremism (PVE) that the number of Malaysians involved in terrorism has decreased significantly in recent years. Yet, Malaysia is not safe from the threat of extremism from affecting its people.[3] The problem is exacerbated by the ever-evolving modus operandi of extremists that have a virtually limitless support base by incorporating the latest technological advancements, causing significant damage, and escaping detection.

[1] *Bumiputera* refers to Malaysians of indigenous origin, including Malays

[2] Mohd, W. (2016). Hate speech on the rise: lacunae in Malaysian law.

[3] Mustafa, M., & Lee, N. (2021, January 15). Terror Arrests Drop in Malaysia Due to Pandemic, New Policing Approach. *Benar News*. https://www.benarnews.org/english/news/malaysian/my-counter-terror-01152021181945.html

MAIN PLATFORMS WHERE HATE SPEECH THRIVES

There are many reasons that allow extremism to flourish—and hatred is the seed which grows when nurtured. In the Malaysian context, research has identified that respondents observe hate speech more predominantly on: (i) social media, (ii) mass media (news outlets, television, etc.); and (iii) through political communication. These platforms increase the public's exposure to hate speech and hateful ideologies which may insidiously influence our minds towards extremism. A study highlighted 83% of militant detainees charged under anti-terrorism laws in Malaysia used social media platforms to access content and establish camaraderie with individuals on the dark web.[4] Therefore, it is imperative to understand the many ways in which harmful content is being disseminated.

Social Media

96.8% of Malaysians are connected online via the internet, with 26.8 million Malaysians active on various social media platforms,[5] such as Whatsapp, Telegram, Facebook, Twitter, Instagram, and TikTok. The form of our interaction with people has become more direct—which encourages boldness and lack of restraint in online expression, which add to the conflict in the virtual world,[6] and manifested through hate speech, harassment, and aggression.[7]

Online hate groups are easier to establish compared to hate groups in the physical world. The user-friendly interface, algorithms which attract content of similar nature, and other features of tools social media platforms provide a suitable environment which may encourage the youth towards hatred and later, extremism.[8] For example, the "Anti Rohingya Club" on Facebook was previously very active in espousing hateful vitriol against migrants and refugees, with one private group that managed to attract approximately 100,000 members.[9] These sentiments are still dominant amongst netizens, reflected in comments on an article published by and posted on Doctor's Without Border's Facebook page about the gratitude expressed by a Rohingya refugee to Malaysia for granting him asylum.[10] The predominant theme of the 149 comments are mostly negative and xenophobic, with dehumanising language. This indicates that Facebook may have mechanisms to monitor and remove hate groups on their platforms, but the process may take time and some hate groups can operate without detection for a considerable amount of time. Unfortunately, the damage is already done.

[4] El-Muhammady, A. (2023). A "Blue Ocean" for Marginalised Radical Voices: Cyberspace, Social Media and Extremist Discourse in Malaysia. *New Media in the Margins*, 163–192. https://doi.org/10.1007/978-981-19-7141-9_8

[5] Howe, S. (2023, February 1). *Social Media Statistics for Malaysia* [2022]. Meltwater. https://www.meltwater.com/en/blog/social-media-statistics-malaysia

[6] Watanabe, H., Bouazizi, M., & Ohtsuki, T. (2018). Hate Speech on Twitter: A Pragmatic Approach to Collect Hateful and Offensive Expressions and Perform Hate Speech Detection. *IEEE Access, 6*, 13825–13835. https://doi.org/10.1109/access.2018.2806394

[7] Zhou, Y., Yang, Y., Liu, H., Liu, X., & Savage, N. (2020). Deep Learning Based Fusion Approach for Hate Speech Detection. *IEEE Access, 8*, 128923–128929. https://doi.org/10.1109/access.2020.3009244

[8] Gerrand, V. (2020, November 13). *Can social networking platforms prevent polarisation and violent extremism?* OpenDemocracy. https://www.opendemocracy.net/en/global-extremes/can-social-networking-platforms-prevent-polarisation-and-violent-extremism/

[9] Latiff, R., & Ananthalakshmi, A. (2020, October 14). *Anti-migrant sentiment fanned on Facebook in Malaysia*. Reuters. https://www.reuters.com/article/uk-facebook-malaysia-rohingya-idUKKBN26Z0BP

[10] (2023, June 22). Facebook; Doktor Tanpa Sempadan / Médecins Sans Frontières (MSF). https://www.facebook.com/msf.malaysia/posts/pfbid033ahtzskTgYmXujYYwxCWV5jK5ar6vX7pBsUQygQ16V33vbf9yK3i5nnA6SEXNzAql

In addition, terrorists have taken advantage of social media to recruit new followers, and groom "selected" individuals on more private and encrypted platforms such as Telegram.[11] Thomas K. Samuel explained some factors which influence terrorists to use social media such as: (i) ideal platform to disguise their identity and activities; (ii) ease to observe like-minded terrorists; and (iii) ability to continue passing on the "mandate" of terrorist leaders posthumously.[12]

Mass Media

Media practices have evolved in line with technological advancements. News portals depend on data analytics to determine the readership of their content—and the number of clicks, likes, and shares are indicative of that. These practices have caused news portals to publish sensationalised news and clickbait headlines. Overemphasis on these practices can actually threaten social cohesion between the people. For example, an article by The Centre stated that "racially-charged speech against both Malay-Muslims and non-Malays on Twitter rose in tandem with the growing number of COVID-19 cases"[13] – particularly when it comes to issues of ethnicity, religion, and nationality.

Political Communication

Certain political figures leverage on the people's well-known sensitivities to gain support from their targeted audience.[14] Interestingly, 60% of respondents from a study cited politicians as the 3rd highest source of hate speech.[15] News reports often publish about the hateful rhetoric being shared by certain parties and their supporters from different ends of the political spectrum, which is purposely done to garner more support for their respective parties[16] and increase success in the elections.

This is dangerous because the status of politicians carries a bigger circle of influence. This may cause people to view politicians' practice of employing hateful rhetoric as "legitimate," and encourage them to engage in hate speech.[17] At present, Malaysia does not differentiate offenders based on their position or status of influence. This may explain the indifference shown by certain politicians who continue to employ the "politics of hate" as part of their campaign strategy.

[11] Wan Mohd Nor, M., & El-Muhammady, A. (2021). Radicalisation and Paramilitary Culture: The Case of Wanndy's Telegram Groups in Malaysia. *Militarization and the Global Rise of Paramilitary Culture*, 95–122. https://doi.org/10.1007/978-981-16-5588-3_6

[12] Jawhar, J. (2016). *Terrorists' Use of The Internet: The Case of DAESH*. SEARRCT: Kuala Lumpur.

[13] Tham, J. V., & Omar, N. (2020, April 2). Like a Virus: How Racial Hate Speech Looks Like in Malaysia During the Covid-19 Pandemic. *The Centre*. https://www.centre.my/post/how-covid-19-influencing-racial-hate-speech-malaysia

[14] Fee, L. K., & Appudurai, J. (2011). Race, Class and Politics in Peninsular Malaysia: The General Election of 2008. *Asian Studies Review, 35*(1), 63–82. https://doi.org/10.1080/10357823.2011.552706

[15] Tham, J. V., & Omar, N. (2020, November 25). Hateful to Whom, and How? *The Centre*. https://www.centre.my/post/hateful-to-whom-and-how

[16] *Malaysia Racial Discrimination Report 2016*. (2016). Pusat KOMAS. https://komas.org/malaysia-racial-discrimination-report/

[17] Murphy, A. (2022). *How does political rhetoric influence hate speech?* [PhD Thesis]. University of Leicester.

For example, the police have arrested Hew Kuan Yew (DAP activist) for statements made in Cantonese during the campaigning period which allegedly encouraged the Chinese community to 'exploit' the disunity of Malays by giving them a 'death blow' during the elections.[18] On the opposite end of the political spectrum, president of the Malaysian Islamic Party (PAS), Abdul Hadi Awang was reported to have used hate speech when he insinuated that most instances of corruption are done by non-Muslims.[19] Former Prime Minister Muhyiddin Yassin has also been heavily criticised for a speech he made, in which he is alleged to have accused Christians of cooperating with a group of Jews for the Christianisation of Malaysia.[20]

It appears that politicians from different political camps have engaged in political polarisation.[21] Ironically, S. 4 of the Election Offences Act[22] was enacted to prevent the practice of hateful political narratives to woo voters. If a person is found guilty under S. 4, one may be barred from voting, or if he/she was elected as a representative in the legislature, the seat would be vacated. Despite the strict legal measures, the main initiators of disinformation (which includes hate speech) have been identified as political parties and/or campaign managers.[23] The situation is particularly difficult to monitor and during campaigning, whereby politicians conduct talks in different languages, in different towns and provinces. It seems that certain politicians and supporters disregard the negative consequences of this practice and continue to use it for political gain.

DOMINANT THEMES OF HATE SPEECH IN MALAYSIA

In Malaysia, the major themes of hate speech are (i) race; (ii) religion; and (iii) nationality. Data from the Malaysian Communications and Multimedia Commission (MCMC) highlights that 80% of reports received on hateful content in 2019 were racial in nature, whereas 20% concerned religious matters.[24] Despite the high volume of complaints regarding harmful content posted on Facebook particularly on the 3R matters, the company META has not responded timely to removal of such content. This has caused the MCMC to consider taking legal action against META unless the company increases its commitment to take down harmful posts.[25]

[18] (2022, November 23). DAP activist 'Superman Hew' nabbed over GE15 speech. *New Straits Time*. https://www.nst.com.my/news/crime-courts/2022/11/854288/dap-activist-superman-hew-nabbed-over-ge15-speech

[19] Pillai, V. (2022, August 28). Guan Eng: "Deafening silence" from Cabinet on Hadi's "hate speech" troubling. *Focus on Malaysia*. https://focusmalaysia.my/guan-eng-deafening-silence-from-cabinet-on-hadis-hate-speech-troubling/

[20] Muhyiddin's Christianisation agenda claim is dangerous, says CCM. (2022, November 18). *The Star*. Retrieved August 14, 2023, from https://www.thestar.com.my/news/nation/2022/11/18/muhyiddin039s-christianisation-agenda-claim-is-dangerous-says-ccm

[21] Singh, B. (2010). Malaysia in 2009: Confronting Old Challenges through a New Leadership. *Asian Survey, 50*(1), 173–184. https://doi.org/10.1525/as.2010.50.1.173

[22] Election Offences Act 1954 (Act No. 5 of 1954), s. 4A

[23] *Youth and Disinformation in Malaysia: Strengthening Electoral Integrity*. (2022). Asia Centre. https://asiacentre.org/wp-content/uploads/Youth-and-Disinformation-in-Malaysia-Strengthening-Electoral-Integrity-1.pdf

[24] *MCMC: Almost 22,000 reports received about insensitive '3R' social media posts in six weeks*. (2019). Malaysian Communications and Multimedia Commission (MCMC) | Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). https://www.mcmc.gov.my/en/media/press-clippings/mcmc-almost-22-000-reports-received-about-insensit

[25] *MCMC: "Legal action" against Facebook's parent Meta for failing to cooperate, take down harmful post*. (2023). Malaysian Communications and Multimedia Commission (MCMC) | Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). https://www.mcmc.gov.my/ms/media/press-clippings/mcmc-legal-action-against-facebook-

In Malaysia, religion is deemed a sensitive subject, therefore hate speech of this nature is perceived as "very serious" due to it attacking fundamental beliefs of adherents and is very likely to induce fear—thus may upset public order and jeopardise national security.[26] For example, a Facebook user uploaded a cartoon image depicting the Prophet Muhammad SAW with his wife Aisha RA in a derogatory fashion—attracting approximately 500 complaints to the MCMC.[27]

In another case, Danny Antoni was found guilty of insulting the Prophet Muhamad on social media. It is interesting to note that the judge, in this case, was a non-Muslim, and Judge Edmin Paramjothy had explained in his judgement that religion is a matter considered sacred to its adherents. Therefore, the insulting nature of the post is inappropriate, irresponsible, and provocative–which is a clear breach of the limits to free speech as guaranteed under the Federal Constitution.[28]

NATIONAL FRAMEWORK TO ADDRESS HATE SPEECH

Freedom of Expression vs. the Right of Society to be Protected from Harm

A.10(1) of the Federal Constitution has guaranteed fundamental liberties such as freedom of expression, which also reflects the government's commitment to uphold A.19 of the Universal Declaration of Human Rights. Our involvement in the Universal Periodic Review process underscores this obligation because freedom of expression is imperative in maintaining a functioning democracy.[29]

However, the approach to be taken in a multi-racial, multi-religious country like Malaysia is caution about the negative consequences of our actions (including hate speech). For example, the genocide in Rwanda historical were precipitated by hate speech which began at the hands of Belgian colonisers when the emphasized differences between the Hutu and the Tutsi and favoured one group over the other. The situation increased division amongst society which was exacerbated further by hateful media narratives.[30]

Although Malaysia is considered one of the most peaceful countries in the world (improving by four spots in the Global Peace Index 2022),[31] tensions can lead to

s-parent-meta-f

[26] Tham, J. V., & Omar, N. (2020, November 25). Hateful to Whom, and How? *The Centre*. https://www.centre.my/post/hateful-to-whom-and-how

[27] Ying, T. P. (2019, February 24). Cops open 3 investigation papers on blasphemy cases. *New Straits Time*. https://www.nst.com.my/news/crime-courts/2019/02/463260/cops-open-3-investigation-papers-blasphemy-cases

[28] Bernama. (2020, July 17). Man sentenced to over 2 years' jail for insulting Prophet Muhammad, Islam. *New Straits Time*. https://www.nst.com.my/news/crime-courts/2020/07/609390/man-sentenced-over-2-years-jail-insulting-prophet-muhammad-islam

[29] Post, R. C., & Barendt, E. (1988). Freedom of Speech. *The American Journal of Comparative Law, 36*(1), 174. https://doi.org/10.2307/840191

[30] Hefti, A., & Jonas, L. A. From Hate Speech To Incitement To Genocide: The Role Of The Media In The Rwandan Genocide. *Boston University International Law Journal, 38*(1), 4-29.

[31] *Malaysia - Global Peace Index 2022*. (n.d.). countryeconomy.com. https://countryeconomy.com/demography/global-peace-index/malaysia

controversial events which leave damaging effects on society.[32] Thus, the government has a very cautious approach to balance fundamental liberties with the rights of the people to be protected from harm. There are approximately 14 different legislations which can be used to limit freedom of expression—and this applies to hate speech as well.

Today, hate speech continues to occur, although there have been no reports of violence caused like that of May 13, 1969. Hate speech and related incidents considered as threats to national security and have strengthened the government's resolve to regulate freedom of expression to protect society against incitement of racial and religious tensions.

Ambiguity of Laws and Policies

Despite these laws, our legal framework to address hate speech has weaknesses—most glaring is the absence of a definition for hate speech. Many other key terms are used in different laws that can be used to restrict speech according to different contexts, but these terms are either poorly defined, or not defined at all. To illustrate, the protection of "national security" is a legitimate ground for restricting expression which exceeds its statutory limits. However, it is not explained what is meant by acts that are prejudicial to national security. In addition, these problems of definition (or lack thereof) can cause arbitrary restrictions of speech. Therefore, clearly and comprehensively defining hate speech is the first step towards addressing this problem.

However, a specific law on hate speech is not to add draconian restrictions on freedom of expression. Rather, it should aim to provide a higher standard of what falls under hate speech to avoid abuse of process. For example, the media has long been under government scrutiny, and the running of their operations is subject to many different legislations. The governments under different administrations pre and post 2018 General Elections have used the law to manage, restrict and/or block access to the media for different reasons. While restrictions are necessary in certain situations, there must be clear guidelines as to what acts constitute a breach of media freedom, what are the legal requirements to be met before enforcement measures are taken, etc. This is to preserve fundamental liberties no matter which authority comes into power—and only allowing legal intervention when truly necessary.

The lawmaking process must also factor in widespread consultation with experts from various backgrounds, affiliations, and organisations–including victims of hate speech. In addition, hate speech laws should also be enacted with the aim of reconciliation instead of merely punitive measures. This may help prevent future instances of hate speech. But legal reforms take time and political will to succeed. This means important work to prevent hate speech and violent extremism must continue in the meantime.

Identifying Weaknesses and Implementing Reforms

First, we need to identify and address current weaknesses. The lack of clarity in the national and legal framework, impractical goals, emphasis on the form as opposed to the substance,

[32] Goh, C. T., & Goh, C. T. (1989). *Racial Politics in Malaysia*. FEP International.

and the need for results now can be counterproductive in PVE. Good things and lasting change take time and thus PVE initiatives must focus on the long-term goals. As such, utmost care, consideration, and collective deliberation must go into the planning and execution of PVE initiatives to ensure we 1) identify root causes 2) address pre-existing grievances, and 3) identify and adapt to developing challenges.

In addition, PVE initiatives must be designed to increase engagement and positive reception by the public. We must not target a particular group due to perceptions that extremism is a problem specific to them as opposed to others. Usage of terms and language used must be accurate and sensitive to the context. For example, commonly used terms like "Islamic Extremism" or "Extremist Islam" are problematic.

Semantically, it suggests that Islam has elements of extremism or worse yet, Islam is synonymous with extremism. This is wrong because Islam is one and is the middle way; extremists are not accepted by Islam and are rejected by Muslims who hold onto true Islamic teachings.

Thus, continued usage of these terms may cause Muslims to feel discriminated against as "perpetrators of extremism" and lead to a higher chance of them rejecting PVE initiatives due to distrust and suspicion, despite the good intentions in implementing them. For example, research has identified that many Muslim Americans feel that police outreach and community engagement efforts are disguised as surveillance tactics that unfairly target them. This causes further stigmatisation which hampers efforts towards inclusivity and social cohesion.

WAY FORWARD: ALL-OF-SOCIETY TO ADDRESS HATE SPEECH

The United Nations recognises the danger of hate speech which has been a catalyst to more serious crimes such as violence and even genocide. As such, the Strategy and Plan of Action on hate speech was launched to address hate speech at a national and international level.[33] The Council of Europe has adopted the recommendation on combating hate speech respectively to meet similar objectives.[34]

Malaysia also has many notable efforts to prevent hate speech and violent extremism which should be acknowledged, supported, and continued. However, more can be done to come up with early intervention methods. It is imperative to have an all-of-society approach that is well planned and executed to be relevant to the situation on the ground. When this is done, PVE initiatives have a higher chance of being accepted. The diagram below highlights initiatives to address hate speech that involves all-of-society:

[33] Guterres, A. (2019). *United Nations Strategy and Plan of Action on Hate Speech*. https://www.un.org/en/genocideprevention/documents/UN%20Strategy%2and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf

[34] Council of Europe. (2022, May 20). *The Council of Europe adopted the Recommendation on combating hate speech*. Committee of Experts on Combating Hate Speech. https://www.coe.int/en/web/committee-on-combatting-hate-speech/-/the-council-of-europe-adopted-the-recommendation-on-combating-hate-speech

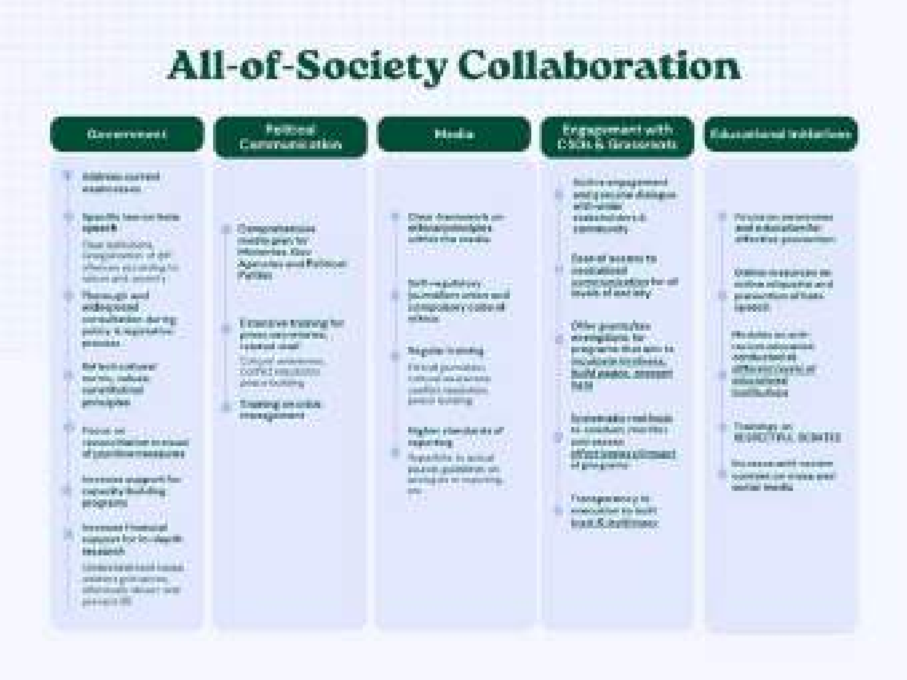

All-of-Society Collaboration
Government
Political Communication
Media
Engagement with CSOs & Grassroots
Educational Initiatives
Address current weaknesses
Specific law on hate speech
Thorough and widespread consultation during policy & legislative process
Focus on reconciliation instead of punitive measures
Increase support for capacity building programs
Increase financial support for in-depth research
Comprehensive media plan for Ministries, Govt Agencies and Political Parties
Extensive training for press secretaries, relevant staff
Training on crisis management
Clear framework on ethical principles within the media
Self-regulatory journalism union and compulsory code of ethics
Regular training
Higher standards of reporting
Active engagement and genuine dialogue with wider stakeholders & community
Ease of access to dedicated communication for all levels of society
Systematic feedback
Transparency in execution to build trust & legitimacy
Focus on awareness and education for effective prevention
Online resources on online etiquette and prevention of hate speech
Increase anti-racism content on mass and social media

Figure 1. Suggested Initiatives to Address Hate Speech

CONCLUSION

Wan Mohd Nor Wan Daud et al. (2021) rightly mentioned that we should avoid enforcing artificial unity through the enforcement of a framework which may not be relatable, relevant, or suitable to the Malaysian people. Doing so may aggravate the problem by causing feelings of frustration, rejection and even radicalism. In contrast, we must emphasise awareness, advocacy and intervention methods that align with local needs which are relevant to our situation. We can overcome hatred with persuasive, positive acts of counterspeech which highlight the shared values of Malaysians. We are all from diverse and different backgrounds, but we MUST come together because a united Malaysia is indeed, worth fighting for.

REFERENCES

Bernama. (2020, July 17). Man sentenced to over 2 years' jail for insulting Prophet Muhammad, Islam. *New Straits Time*. https://www.nst.com.my/news/crime-courts/2020/07/609390/man-sentenced-over-2-years-jail-insulting-prophet-muhammad-islam

adopted the Recommendation on combating hate speech. Committee of Experts on Combating Hate Speech. https://www.coe.int/en/web/committee-on-combatting-hate-speech/-/the-council-of-europe-adopted-the-recommendation-on-combating-hate-speech

Election Offences Act 1954 (Act No. 5 of 1954), s. 4A

El-Muhammady, A. (2023). A "Blue Ocean" for Marginalised Radical Voices:Cyberspace, Social Media and Extremist Discourse in Malaysia. *New Media in the Margins*, 163–192. https://doi.org/10.1007/978-981-19-7141-9_8

Fee, L. K., & Appudurai, J. (2011). Race, Class and Politics in Peninsular Malaysia: The General Election of 2008. *Asian Studies Review, 35*(1), 63–82. https://doi.org/10.1080/10357823.2011.552706

Gerrand, V. (2020, November 13). *Can social networking platforms prevent polarisation and violent extremism?* OpenDemocracy. https://www.opendemocracy.net/en/global-extremes/can-socialnetworking-platforms-prevent-polarisation-and-violent-extremism/

Goh, C. T., & Goh, C. T. (1989). *Racial Politics in Malaysia*. FEP International.

Guterres, A. (2019). *United Nations Strategy and Plan of Action on Hate Speech*. https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf

Hefti, A., & Jonas, L. A. From Hate Speech To Incitement To Genocide: The Role Of The Media In The Rwandan Genocide. *Boston University International Law Journal*, 38(1), 4-29.

Howe, S. (2023, February 1). *Social Media Statistics for Malaysia* [2022]. Meltwater. https://www.meltwater.com/en/blog/social-media-statistics-malaysia

Jawhar, J. (2016). *Terrorists' Use of The Internet: The Case of DAESH*. SEARRCT: Kuala Lumpur.

Latiff, R., & Ananthalakshmi, A. (2020, October 14). *Anti-migrant sentiment fanned on Facebook in Malaysia*. Reuters. https://www.reuters.com/article/uk-facebook-malaysia-rohingya-idUKKBN26Z0BP

Malaysia - Global Peace Index 2022. (n.d.). countryeconomy.com. https://countryeconomy.com/demography/global-peace-index/malaysia

Malaysia Racial Discrimination Report 2016. (2016). Pusat KOMAS. https://komas.org/malaysia-racial-discrimination-report/

MCMC: Almost 22,000 reports received about insensitive ’3R’ social media posts in six weeks. (2019). Malaysian Communications and Multimedia Commission (MCMC) Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM).https://www.mcmc.gov.my/en/media/press-clippings/mcmc-almost-22-000-reports-received-about-insensit

MCMC: “Legal action” against Facebook’s parent Meta for failing to cooperate, take down harmful post. (2023). Malaysian Communications and Multimedia Commission (MCMC) Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). https://www.mcmc.gov.my/ms/media/press-clippings/mcmc-legal-action-against-facebook-s-parent-meta-f

Mohd, W. (2016). Hate speech on the rise: lacunae in Malaysian law.

Muhyiddin’s Christianisation agenda claim is dangerous, says CCM. (2022, November 18). *The Star*. Retrieved August 14, 2023, from https://www.thestar.com.my/news/nation/2022/11/18/muhyiddin039s christianisation-agenda-claim-is-dangerous-says-ccm

Murphy, A. (2022). *How does political rhetoric influence hate speech?* [PhD Thesis]. University of Leicester.

Mustafa, M., & Lee, N. (2021, January 15). Terror Arrests Drop in Malaysia Due to Pandemic, New Policing Approach. *Benar News*. https://www.benarnews.org/english/news/malaysian/my-counter-terror 01152021181945.html

Piazza, J. (2020, September 28). When politicians use hate speech, political violence increases. *The Conversation*. https://theconversation.com/when-politicians-use-hate-speech-political-violence-increases-146640

Pillai, V. (2022, August 28). Guan Eng: “Deafening silence” from Cabinet on Hadi’s “hate speech” troubling. *Focus Malaysia*. https://focusmalaysia.my/guan-eng-deafening-silence-from-cabinet-on-hadis-hate-speech-troubling/

Post, R. C., & Barendt, E. (1988). Freedom of Speech. *The American Journal of Comparative Law, 36*(1), 174. https://doi.org/10.2307/840191

Ram, S. B. (2019, July 12). AG: Cannot rule out applying the Sedition Act until it is repealed. *New Straits Time*. https://www.nst.com.my/news/crime-courts/2019/07/503841/ag-cannot-rule-out-applying-sedition-act-until-it-repealed

Singh, B. (2010). Malaysia in 2009: Confronting Old Challenges through a New Leadership. *Asian Survey*, 50(1), 173–184. https://doi.org/10.1525/as.2010.50.1.173

Tham, J. V., & Omar, N. (2020, April 2). Like a Virus: How Racial Hate Speech Looks Like in Malaysia During the Covid-19 Pandemic. The Centre. https://www.centre.my/post/how-covid-19-influencing-racial-hate-speech-malaysia

Tham, J. V., & Omar, N. (2020, November 25). Hateful to Whom, and How? *The Centre*. https://www.centre.my/post/hateful-to-whom-and-how

Wan Mohd Nor, M., & El-Muhammady, A. (2021). Radicalisation and Paramilitary Culture: The Case of Wanndy's Telegram Groups in Malaysia. *Militarization and the Global Rise of Paramilitary Culture*, 95–122. https://doi.org/10.1007/978-981-16-5588-3_6

Watanabe, H., Bouazizi, M., & Ohtsuki, T. (2018). Hate Speech on Twitter: A Pragmatic Approach to Collect Hateful and Offensive Expressions and Perform Hate Speech Detection. *IEEE Access, 6*, 13825–13835. https://doi.org/10.1109/access.2018.2806394

Ying, T. P. (2019, February 24). Cops open 3 investigation papers on blasphemy cases. *New Straits Time*. https://www.nst.com.my/news/crime-courts/2019/02/463260/cops-open-3-investigation-papers-blasphemy-cases

Youth and Disinformation in Malaysia: Strengthening Electoral Integrity. (2022). Asia Centre.https://asiacentre.org/wp-content/uploads/Youth-and-Disinformation-in-Malaysia-Strengthening-Electoral-Integrity-1.pdf

Zainury, M. A. (2019, November 11). Perselisihan kaum, agama: Ahli politik dan media sosial jadi punca? *Sinar Harian*. https://www.sinarharian.com.my/article/56621/BERITA/Nasional/Perselisihan- kaum-agama-Ahli-politik-dan-media-sosial-jadi-punca

Zhou, Y., Yang, Y., Liu, H., Liu, X., & Savage, N. (2020). Deep Learning Based Fusion Approach for Hate Speech Detection. *IEEE Access, 8*, 128923–128929. https://doi.org/10.1109/access.2020.3009244

(2023, August 7). Now, UtusanTV site blocked as well. *Malaysia Now*. https://www.malaysianow.com/news/2023/08/07/now-utusantv-site-blocked-as-well; (2023, July 28). Online freedom monitor confirms MCMC behind latest site block. MalaysiaNow. https://www.malaysianow.com/news/2023/07/28/online-freedom-monitor-confirms-mcmc-behind-latest-site-block

(2023, June 22). Facebook; Doktor Tanpa Sempadan / Médecins Sans Frontières (MSF).https://www.facebook.com/msf.malaysia/posts/pfbid033ahtzskTgYmXujYYwxCWV5jK5ar6vX7pBsUQygQ16V33vbf9yK3i5nnA6SEXNzAql

(2023, February 16). *Penyata Rasmi Parlimen Dewan Rakyat*. Parlimen Malaysia. https://www.parlimen.gov.my/files/hindex/pdf/DR-16022023.pdf

(2022, November 23). DAP activist 'Superman Hew' nabbed over GE15 speech. *New Straits Time*. https://www.nst.com.my/news/crime-courts/2022/11/854288/dap-activist-superman-hew-nabbed-over-ge15-speech

RETHINKING BUILDING DIGITAL RESILIENCE TO RADICALISATION: REDUCING A PERSON'S SUSCEPTIBILITY TO INFLUENCE THROUGH DISCUSSION

Nicole Matejic

ABSTRACT

In any increasingly mixed landscape of non-violent and violent extremism, the types of influences that lead people towards adopting extreme overvalued beliefs that may lead to terrorism require closer research. This paper contributes to this research by exploring how a susceptibility to influence underpins ideological adoption and offers a new framework for understanding radicalisation: 'The Radicalisation Spectrum'. By viewing radicalisation as a spectrum of commitment towards or away from extreme overvalued beliefs, the full range of motion those radicalising and disengaging can be more closely studied. Further, by expanding the existing PCVE framework of *deter-disengage-prevent-counter* to include a 'dissuade' pillar at the outset; practitioners can consider building resilience initiatives that anticipate and proactively disrupt and degrade the opportunities available to extremists to influence others towards radicalisation. This paper therefore contends that a person's risk of radicalisation should be weighed according to their susceptibility to influence rather than their risk of subscribing to any particular ideology or their belonging to any particular risk community.

Keywords: radicalisation, violent extremism, influence, behavioural economics, counterterrorism, dissuasion, PCVE, disengagement.

INTRODUCTION

The study of violent extremism has often been tethered to the notion that a deep commitment to an extremist ideology is the driving force behind radicalisation But as some scholars and recent violent extremist plots and attacks demonstrate, this is not always the case. With attention turning to an increasingly dynamic extremist landscape, it is clear that a fanaticism towards a particular ideology – or the adoption of or shifting between many beliefs - is not a reliable indicator of violent intent.

This paper therefore argues that a susceptibility to influence is the common precursive marker among those radicalising towards violent extremism in group environments. This paper also proposes that radicalisation should therefore be viewed on a *spectrum* of engagement towards, or disengagement away from, violence. When a susceptibility to influence – rather than particular ideologies – is the primary consideration, the under-explored element of dissuasion presents an opportunity for preventing and countering violent extremism (PCVE) practitioners to better structure disengagement initiatives.

SUSCEPTIBILITY TO INFLUENCE: A MARKER FOR EVALUATING A PERSON'S RISK OF RADICALISATION

To understand how a susceptibility to influence underpins radicalisation, models of radicalisation and disengagement need to begin at a point that pre-supposes any exposure to extreme overvalued beliefs or violent ideation. According to Rahman (2018) an 'extreme overvalued belief' is the adoption of a "rigidly held, non-delusional belief" that can be shared, "relished, amplified and defended by the possessors of the belief" leading to the "belief becoming more dominant over time, more refined and more resistant to challenge" (pp.1-2). People can adopt one or many extreme overvalued beliefs concurrently and they can span many forms of non-violent and violent extremism.

One way people can come to adopt extreme overvalued beliefs, according to psychologist Dr. Robert Cialdini is via Pre-suasion: the way "seemingly insignificant and apparently unimportant details" combine – that leaves people susceptible to influence long before they encounter it. Pre-suasion does this by drawing on the experiences and information a person already has. Cialdini, in his earlier work, identified seven key factors of effective influence: reciprocity, commitment and consistency, social proof, authority, like and scarcity, and unity (Cialdini, 2016, pp.20-63). While Cialdini originally applied pre-suasion to economics, marketing, communication and leadership contexts, the concept can be useful to help explore a variety of situations. In the context of radicalisation, we can apply pre-suasion by exploring an individual's *susceptibility to influence* - rather their susceptibility to ideologies. This is because if someone is unable to be influenced, then the conditions under which radicalisation occurs cannot flourish.

While pre-suasion isn't often articulated as a separately defined segment of radicalisation models, case studies of violent extremists often explore the contributing factors that led them to commit acts of terrorism. Similarly, the radicalisation modelling of notable scholars can be seen to encompass some elements of pre-suasion. In McCauley and Moskalenko's (2017) 'Two Pyramids' model, the Opinion and Action pyramid captures this pre-suasive point in their identification of neutrality and inertness respectively (pp.205-216).

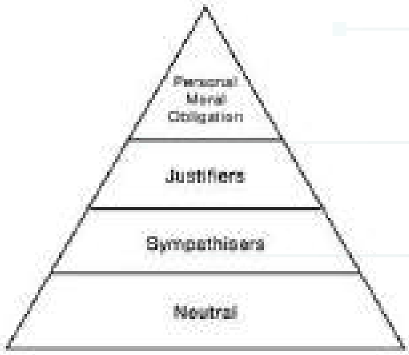


Figure 1: The Opinion Pyramid (McCauley & Moskalenko, 2017).

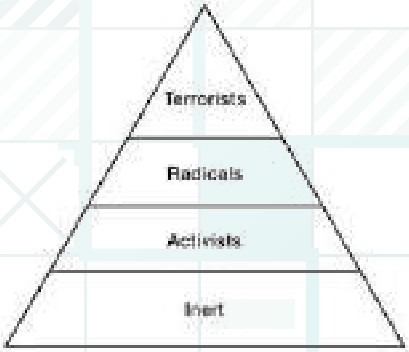


Figure 2: The Action Pyramid (McCauley & Moskalenko, 2017).

In Khalil's (2017) 'The Three Pathways' or 3P model, two of the three pathways could be considered as occurring before a person encounters ideas that justify violence. Pathway once observes that individuals can progress from non-extremism to non-violent extremism to supporters of violence before becoming contributors of violence. Pathway three notes a person's attraction to violence – not the objectives it supports – can influence their decision-making "because they are provided with material incentives, seek adventure, belonging or status (pp.40-48).

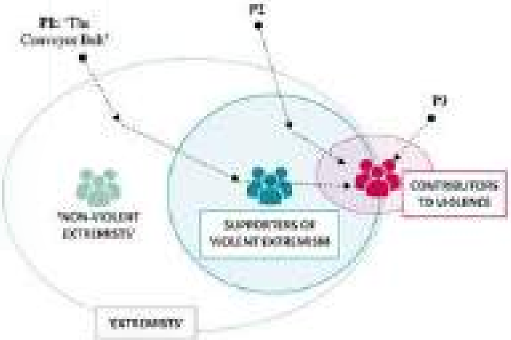


Figure 3: The Three Pathways Model
(Graphic Source: RUSI Journal August/September 2017)

Webber and Kruglanski's (2017) '3N Approach' also captures elements that pre-suppose any interest or exposure to ideas that justify violence. The 3N's – (1) "the needs or motivation of the individual"; (2) "the ideological narratives of the culture in which the individual is embedded"; and (3) "the dynamic interplay of group pressure and social influence that occurs within the individual's social network" (pp.33-43) all speak to the types of influences that may contribute to pre-suasive environments, effectively priming a person for influence. While ideological in nature, the second N can also be seen to encompass environments which are unavoidably influential, accounting for the pre-suasion that occurs, for example, when people are born into extremist families, radicalise in prison or whose choice of friends delivers them into a peer-led misadventure. The idea of influence beginning in a 'pre-radicalisation' period of time has also been observed in Phillips' (2014) economic analysis of lone-wolf terrorism. Explaining that economics is fundamentally "about opportunities and choices," Phillips notes it's utility can be helpful in identifying the choices prospective violent extremists make from the opportunities available to them (pp.159-191).

EXTREME OPPORTUNITIES AND CHOICES

Behavioural economics provides useful frameworks to consider how and why people are influenced towards adopting extreme overvalued beliefs that may lead to violence. Biases and heuristics, for example, can support our understanding of the types of effects influence generates, when and why. Availability Cascades, described by Kuran and Sunstein (1999), where influencers "manipulate the content of public discourse" to "advance their agendas" and cultivate "self reinforcing processes of collective belief formation," are particularly useful in understanding how online environments support radicalisation because the beliefs expressed within an availability cascade deliver "rising plausibility" to extreme narratives.

The result is often that those within an in-group adopt ideas "partly by learning from the apparent beliefs of others and partly by distorting their public response" to maintain social acceptance. Perhaps most applicable to radicalisation is the way extremist influencers can "fix people's attention on a problem, interpreting phenomena in particular ways" to further their agenda. That extremist influencers provide the illusion of certainty on issues that matter to susceptible people at critical moments in their life is worthy of note. Kuran and Sunstein explain that "often people have little information about the magnitude of a risk or the seriousness of an alleged social problem. (So) they stand to gain from tuning into, and letting themselves be guided by, the signals of others" (pp. 683-768). Tversky and Kahneman (1973) observed that a "reliance on the availability heuristic leads to systematic biases" meaning when faced with choices related to judgement, people tend to defer to the information that they can most easily recall, and that fits their existing worldview, inducing confirmation and recency biases (pp.207-232) to achieve cognitive consonance. After all, humans are wired to preference feelings of comfort that give them a sense of control and social acceptance (Festering, 1957, pp.18-21). To compound these influential markers, the onboarding of people into extreme online spaces fosters in-group reciprocity. This in turn leverages the ambiguity effect induced by repetitive narratives, contributing to a rising sense of siege mentality. That susceptible people find the allure of extremist influencers attractive enough to begin adopting extreme overvalued beliefs is therefore a critical point of understanding in a prevention context.

EXTREME OVERVALUED BELIEFS

Kuran and Sunstein's (1999) observation on an influencer's ability to 'fix people's attention' is worthy of further exploration given its role in influencing subsequent decision-making. In the context of non-violent and violent extremism, cults, mass suicides, mass shootings and radicalisation Rahman's (2017) work on extreme overvalued beliefs perhaps best explains ideological pick and mix types of extremism. The parallels between an extreme overvalued belief and how an availability cascade works is also worthy of note because both, in group settings, rely on the participative aspect of belief amplification and defence. In many ways, extreme overvalued beliefs are also like sacred beliefs, which people attach such value to that the belief becomes protected (Ginges and Atran, 2014, pp.275-280). When this happens, challenging or trying to change that belief is interpreted as hostile by the person holding it– causing them to double down on the defence of it. Because of the way contemporary communications leverages emotive decision-making and combined with online algorithms designed to serve users more of the content they engage with, the result is a permissive environment for extremist influencers to build marketplaces for their extreme ideas.

The collision of a pre-suaded person with an extremist influencer however, does not mean persuasion – or radicalisation - is a guaranteed outcome (Kuran & Sunstein, 1999, pp.683-768). In practice, however, once a person has been onboarded into an extremist in-group, disengagement becomes more challenging. That is not to say people cannot or will not disengage of their own volition – they can and do – however it does raise the opportunity costs of PCVE interventions.

WHEN INFLUENCE COLLIDES WITH IDEOLOGY

The point at which ideology becomes an influential part of radicalisation depends on a range of variables. Some grievances will already be wedded to extreme overvalued beliefs

Antisemitism for example, is wedded to far-right and far-left ideologies (for differing reasons). A 'salad-bar' of ideological ideas has been observed in recent years with many borrowing "from numerous at times seemingly contradictory, ideological foundations" (Clarke and Al Aqeedi, 2021; Gartenstein-Ross and Blackman, 2022, pp.555-578; Gartenstein-Ross, Zammit, Chace-Donohue, and Urban, 2023; Comerford and Havlicek, 2021). Conspiracy theories, for example, are an oft recycled patchworked collection of overvalued ideas (some of which are extreme) misinformation and disinformation (Rousis, 2018, pp.16-22; Allington, 2021; Binnendyk and Pennycook, 2022). While more orthodox ideologically aligned extremist influencers deploy a pre-made master narrative often steeped in decades or centuries of historical events and/or mythmaking (Halverson, Goodall, and Corman, 2011, pp.16-31; Ranta, 2017; Knott and Lee, 2020, pp.1-23); 'salad-bar' extremist influencers tend to sell whichever extreme overvalued idea people are currently buying, riding an often manufactured outrage wave (Wallace-Wells, 2021; Thompson Ford, 2019), and pivoting between a few core evergreen extreme grievances to maintain ongoing relevance (Gordon, 2021; Fisher, 2021). Again, the ideology in play is immaterial to the objective: the master narrative must exert sufficient influence to denigrate the decision-making autonomy of each in-group member.

It is for this reason in-group members are encouraged to only seek answers to their questions from within that group; and extremist influencers go to great lengths to discredit out-grouped information sources such as mainstream media, official government information, and academia. This is because it is not enough for the extremist influencer to use their online ecosystem as a self-glorifying soapbox (although plenty of that occurs). To be fully effective they must be able to influence their in-group in ways that take members from extreme overvalued belief to behaviours and action/s inspired by it.

THE RADICALISATION SPECTRUM

By acknowledging that a susceptibility to influence plays a greater role in an individual's nudge towards radicalisation than specific ideologies (in the absence of unavoidable influencing environments) then viewing radicalisation as a spectrum of commitment towards or away from extreme overvalued beliefs can be modelled.

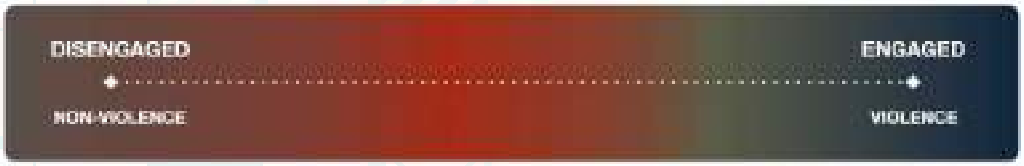


Figure 4: The Radicalisation Spectrum.

In a reflection of the knowledge both scholars and practitioners in the field have observed, a spectrum of overvalued extreme belief accounts more fully for the journey individuals take toward engagement or disengagement (Matejic, 2023). Depicting a full range of radicalising and disengaging motion, a Radicalisation Spectrum also accounts for behaviours such as pivoting back and forth between levels of active engagement or disengagement (Williams, 2019, pp.85-121; Obaidi et al., 2022); stalling and vacillating around levels of pre-violent commitment (Van de Weert, 2021; Knight et al., 2017, pp.230-248); or reaching the peak of their commitment to an extreme overvalued belief at a point that falls short of an act of violent extremism (Halpin and Wilson, 2022, pp.18-33; Lygren and Ravndal, 2023, pp.390-408). These points of pause, vacillation or disengagement within a Radicalisation Spectrum are important because deviant behaviours often manifest over time and the reasons that compel someone to move forward into an actively engaged state, can also resolve to move them backward towards disengagement.

Extremist leaders can also exert sufficient influence on those in their in-groups to moderate violent ideation and actual violence. For example, Wilson and Halpin (2023) observed in a study of a New Zealand based white-nationalist organisation that in-groups themselves may moderate the level of radicalism among members to avoid violent extremes when such outcomes would hinder the group's aspirations and long-term objectives (pp.18-33). This research mirrors that found within decision theory because it indicates both the extant influence the extremist influencer possesses and the presence of anticipated regret (Phillips and Pohl, 2020, pp.1-10) which can also exert significant influence on decision-making. Similarly, strategic decision-making pertaining to the timing of any planned violence speaks to terrorist choice (Phillips and Pohl, 2014, pp.139-160), particularly as it applies to target selection (Phillips and Pohl, 2017, pp.150-164) and propaganda of the deed aspirations (Pohl, 2014, pp.60-76).

Therefore, Cascade-like modelling (Matejic, 2023) can be adopted to depict the full range of motion within the Radicalisation Spectrum. This is depicted at Figure 5, where the coloured line represents motion towards engagement in the cascade and the grey line represents disengagement:

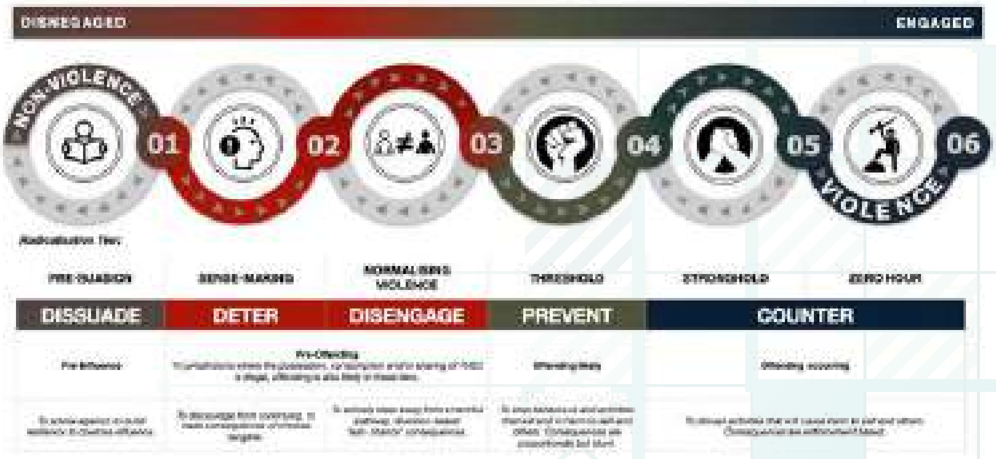


Figure 5: The Radicalisation Spectrum

As the omni-directional nature of the model depicts, those within the spectrum have a range of mobility options. Therefore, the Radicalisation Spectrum also provides a framework for exploring to what degree there is a level of organisation or strategy involved. For example, extremist influencers that are unable to mobilise followers to offline action might never pass tiers 3-4; while those who harbour violent ideation – either for themselves or as a means of incitement – will push up against tier 5 with regularity. That the law in many jurisdictions does not have the legislative means to intervene until tiers 3-6 (when a terrorist plot is detected and enough evidence has been gathered to enable a lawful intervention to disrupt it, or an attack has been committed) leaves the earlier radicalising tiers in the deter, disengage, and prevent realm.

Importantly, the Radicalisation Spectrum model does not presume that people *deradicalise* – only disengage from beliefs that justify violence. As Horgan (2009) notes, "just because one leaves terrorism behind, it rarely implies (or even necessitates) that one becomes deradicalised" (pp.291-298). This is because the notion of divorcing people from their overarching worldview – so long as it is non-violent – is counterproductive to deterrence and disengagement activities. As Wanless (2015) observes: "Want to win hearts and minds? Avoid denigrating them first."

DISSUASION OPPORTUNITIES FOR PCVE

By expanding the *deter-disengage-prevent-counter* paradigm to include a 'Dissuade' pillar at the outset, there is an opportunity to mitigate pre-suasive influence before a person needs deterrence or disengagement. This is important because by the time an individual is detected and assessed to be in the deter or disengage space, a considerable amount of extremist influence has already been exerted on them. That this extremist influence has a proverbial head start makes deterrence moot and disengagement activities more challenging because practitioners must contend with a fledging, yet rising commitment to the adoption of extreme overvalued beliefs and the pull of the rewards an in-group holds out.

The presence of counter-narratives aligned with prevention initiatives may also feed directly into the master narratives and grievances that have already been able to incubate. This makes building a resilience to extremist influence *before the susceptible individual even encounters it* a practical way to disrupt radicalisation. Some scholarship has already considered dissuasive-like interventions. The BRAVE Measure, for example, assists "helping understand young people's resilience to violent extremism" in so far as it explores the socio-cultural factors that underpin known risk factors. Grossman et al. (2020) point out that such efforts are often directed by practitioners and governments that have fixed ideas about which communities are at risk of radicalisation, when in fact the better question to ask is "why the vast majority of people in so called communities of risk do not ever radicalise towards violent extremism" (pp.468-488). In the few short years since the BRAVE Measure was published in 2020, however, the violent extremist landscape has changed significantly. Against a backdrop of COVID19 manifested grievances, conspiracy theories, accelerationist, and salad-bar types of violent extremism, it would be worthwhile re-testing the BRAVE Measure's ability to adapt to this new landscape.

Other avenues worthy of further exploration include ways in which the information environment can be proactively degraded to raise the opportunity costs extremist influencers encounter when trying to establish themselves and maintain their communities. At present, due to an increasingly decentralised online environment, a permissive space exists. However, in the online marketplace of ideas that justifies violence, extremist influencers are considerably more fragile than the communities they create. Online ecosystems have consistently demonstrated a high level of resilience to degradation and disruption, regularly outlasting the extremist influencers that created them. For example, ISIS' cloud caliphate continues to serve as a content library for extreme Islamists (Ayad and Amarasingam, 2021; Macdonald et al., 2022) while other violent extremists producing terrorist and violent extremist content continue to exploit smaller tech platforms, archiving and file sharing services (Tech Against Terrorism, 2023). But, these coordinated content tactics are not universal to all violent extremist groups.

This presents an opportunity to dissuade susceptible people via default because flailing extremist influencers and their fracturing online communities present little value to audiences. What flailing extremist ecosystems do offer, however, are teachable moments at opportune times that can assist to inoculate people against extremist influence. As Braddock (2022) found in research looking at attitudinally inoculating people against hate to build a resilience to persuasion, a dissuasive approach "significantly reduced participants perceptions of the extremist groups credibility." Citing McGuire's work on inoculation theory – that is that resilience to influence can be built by providing people with the knowledge of how to identify and avoid it. Braddock notes that this approach "can persuade not only those affected by violence but also those vulnerable to persuasion to perform violence" (pp.240-262). Inoculation theory should not be confused with counter-narrative or messaging in this context, because the application of the pre-bunking is towards harmful influence, not any particular ideologies; nor does the approach seek to de-bunk any existing narratives.

Such work when combined with organised Strategic Network Disruptions (SNDs) highlight the opportunities for PCVE practitioners to leverage the relative fragility individual extremist influencers have online. Thomas and Wahedi (2023) noted in a recent study of hate-organisations on Facebook that by "removing key actors at the same time" harmful online activity diminished, as did the extremist influencer's ability to rebuild and regroup their audiences. Additionally, the initial backlash observed by core hate-group members dissipated over time which suggests the influence of extremists reduced, resulting in "the hate organisation no longer being able to shape the behaviour of its target audience" (pp.1-9). While a level of user platform migration (Bradely and Shadina, 2022) has been observed after such interventions, and this new research was dependant on a social media network's own willingness to engage in SND's and allowing researcher access to that data; the approach broadly supports the degradation of extremist influencers ability to influence the decision-making of their followers. While the study on SNDs has some limitations – notably their inability to track user migration – the approach could signal a way to for PCVE stakeholders to collaborate in a coordinated, dissuasive context.

CONCLUSION

This paper proposes that models of radicalisation explore the role of pre-suasive influence in more depth; and in building resilience to radicalisation, the addition of a 'dissuade' pillar to the conventional 'deter – disengage – prevent – counter' paradigm would enhance PCVE practitioner understanding of the types of influences that lead people towards adopting extreme overvalued beliefs. By expanding existing modelling and initiatives to include dissuade at the outset, practitioners and scholars can begin to consider resilience building solutions that anticipate and proactively disrupt and degrade the opportunities available to extremists to influence others. This article also proposes that to best model this, radicalisation should be viewed as a spectrum of engagement towards or disengagement away from violent extremism.

If we view radicalisation as a spectrum of extreme overvalued belief based on influences that impact decision-making, the full range of motion those radicalising and disengaging exhibit is more closely captured. Further, an agnostic 'Radicalisation Spectrum' accounts for an increasingly mixed environment that leverages a combination of extreme overvalued beliefs. Therefore, a person's risk of radicalisation should be weighed according to their susceptibility to influence rather than their risk of subscribing to any particular ideology or their belonging to any particular risk community. Dissuasion initiatives therefore present perhaps the most ideal point to build resilience towards extremist influence - before radicalisation can begin.

REFERENCES

Alington, D., (2021) Conspiracy Theories, Radicalisation and Digital Media. Global Network on Extremism and Technology. Retrieveed 1 June 2023, GNET https://gnet-research.org/wp-content/uploads/2021/02/GNET-Conspiracy-Theories-Radicalisation-Digital-Media.pdf

Ayad, M., Amarasingam, A., & Alexander, A. (2021) The Cloud Caliphate: Archiving the Islamic State in Real-Time. Combating Terrorism Center at West Point and the Institute for Strategic Dialogue.

Binnendyk, J. & Pennycook, G. (2022) Intuition, Reason and Conspiracy Beliefs. Current Opinion in Psychology, 47:101387.

Braddock, K. (2022) Vaccinating Against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda. Terrorism and Political Violence, Volume 34(52), pp. 240-262.

Bradely, A., & Shadnia, D. (2022) Examining Online Migration to Terrorist and Violent Extremist-Owned domains. Program of Extremism, George Washington University and Tech Against Terrorism.

Cialdini, R. (2016) Pre-Suasion. pp. 20-63.

Clarke, C. & Al Aqeedi, R. (2021) What Terrorism Will Look Like in The Near Future. New Lines Institute. Accessed 1 June 2023; https://newlinesinstitute.org/nonstate-actors/what-terrorism-will-look-like-in-the-near-future/

Comeford, M. & Havelicek, S. (2021) Mainstreamed Extremism and The Future of Prevention. Institute of Strategic Dialogue. Accessed 1 June 2023; https://www.isdglobal.org/isd-publications/policy-paper-mainstreamed-extremism-and-the-future-of-prevention/

Fisher, M. (2021) From Memes to Race War: How Extremists Use Popular Culture to Lure Recruits. Washington Post. Accessed 1 June 2023; https://www.washingtonpost.com/nation/2021/04/30/extremists-recruiting-culture-community/

Festering, L. (1957) A Theory of Cognitive Dissonance. pp. 18-21.

Gartenstein-Ross, D. & Blackman, M. (2022) Fluidity on the Fringes: Prior Extremist Involvement as a Radicalisation Pathway. Studies in Conflict & Terrorism, 45(7) pp. 555-578.

Gartenstein-Ross, D., Zammit, A., Chace-Donahue, E., & Urban, M. (2023) Composite Violent Extremism: Conceptualising Attackers Who Increasingly Challenge Traditional Categories of Terrorism. Studies in Conflict and Terrorism.

Gordon, J. (2021) No Crisis Left to Waste: Exploring Convergent Themes in Extremist Propaganda. NYPD Intelligence Research Specialist short talk. Accessed 3 June 2023; https://www.chds.us/ed/alumni-short-talks-no-crisis-left-to-waste-exploring-convergent-themes-in-extremist-propaganda/

Grossman, M., Hadfield, K., Jefferies, P., Gerrand, V., & Ungar, M. (2022) Youth Resilience to Violent Extremism: Development and Validation of the BRAVE Measures. Terrorism and Political Violence. Vol 34 (3), pp. 468-488.

Halpin, J. & Wilson, C. (2022) Explaining the Gap Between Online Violent Extremism and Offline Inaction among Far Right Groups: A Study of Action Zealandia from 2019-2021. Behavioural Sciences of Terrorism and Political Aggression. Political Science, Vol 74 (1), pp. 18-33. DOI: https://doi.org/10.1080/00323187.2022.2101493

Halverson, J., Goodall, H., & Corman, S. (2011) Master Narratives of Islamist Extremism. pp. 16-31.

Horgan, J. (2009) Deradicalisation or Disengagement? A Process in Need of Clarity and a Counterterrorism Initiative in Need of Evaluation. Revista de Psicologia Social, 24(2), pp. 291-298.

Khalil, J. (2017) The Three Pathways (3P) Model of Violent Extremism. The RUSI Journal, 162:4, pp. 40-48.

Knight, S., Woodward, K., & Lancaster, G. (2017) Violent Versus Non-Violent Actors: An Empirical Study of Different Types of Extremism. Defence Science and Technology Laboratory, United Kingdom. Journal of Threat Assessment and Management 4(4), pp. 230-248. https://doi.org.10.1037/tam0000086

Knott, K., & Lee, B. (2020) Ideological Transmission in Extremist Contexts: Towards a Framework of How Ideas are Shared. pp. 1-23. DOI: 10.1080/21567689.2020.1732938.

Kuran, T. & Sunstein, C. (1999) Availability Cascades and Risk Regulation. Stanford Law Review, Vol 51(4) pp. 683-768.

Macdonald, S., Rees, C., & Joost, S. (2022) Remove, Impede, Disrupt, Redirect: Understanding and Combatting Pro-Islamic State Use of File Sharing Platforms. Research Resport, April 2022, Resolve Network and Tech Against Terrorism.

Matejic, N. (2023) The Radicalisation Cascade. Using Behavioural Economics as a Framework to Understand How People are Influenced Towards and Away from Violent Extremes. Thesis. Currently under University Embargo until April 2024.

Obaidi, M., Skaar, S., Ozer, S., & Kunst, J. (2022) Measuring Extremist Archetypes: Scale Development and Validation. PLoS ONE, 17(7), DOI: https://doi.org/10.1371/journal.pone.0270225

Phillips. P. (2014) The Economic Analysis of Lone Wolf Terrorism in (Eds) Caruso, R. & Locatelli, A. Understanding Terrorism: A Socio-Economic Perspective. Bingley, United Kingdom. Emerald Group Publishing Limited. pp. 159-191.

Phillips, P., & Pohl, G. (2020) Anticipated Regret, Terrorist Behaviour and the Presentation of Outcomes of Attacks in the Mainstream Media an in Terrorist Group Publications. Aggression and Violent Behaviour, 51:101394, pp.1-10.

Phillips, P., & Pohl, G. (2017) Terrorist Choice: A Stochastic Dominance and Prospect Theory Analysis. Defence and Peace Economics. Vol. 28(2), pp. 150-164.

Phillips, P., & Pohl, G. (2014) Prospect Theory and Terrorist Choice. Journal of Applied Economics. Vol VXII, No. 1, pp.139-160.

Pohl, G. (2014) Media and Terrorist Choice: A Risk-Reward Analysis. Journal of Applied Security Research. Vol 10:1, pp. 60-76.

Rahman, T. (2018) Extreme Overvalued Beliefs: How Violent Extremist Beliefs become "Normalized." Behavioural Sciences. pp.1-2.

Ranta, M. (2017) Master Narratives and the Pictorial Construction of Otherness: Anti-Semitic Imagines in the Third Reich and Beyond. Contemporary Aesthetics. Vol 15, article 25. pp. Accessed online 2 February 2019: https://digitalcommons.risd.edu/liberalarts_contempaesthetics/vol15/iss1/25

Rousis, G. (2018) The Truth is Out There: The Use of Conspiracy Theories by Radical Violent Extremist Organisations. UNF Graduate Theses and Dissertation, pp. 16-22.

Tech Against Terrorism (2023) Report: Patterns of Online Terrorist Exploitation. TCAP Insights, April 2023. Accessed 3 June 2023; https://www.techagainstterrorism.org/2023/04/25/patterns-of-online-terrorist-exploitation/

Thomas, D., & Whaedi, L. (2023) Disrupting Hate: The Effect of Deplatforming Hate Organisations on their Online Audiences. PNAS Research Article, Political

Sciences. pp. 1-9.

Thompson Ford, R. (2019) The Outrage Industrial Complex. Stanford Law Society Blog. Accessed 4 June 2019; https://law.stanford.edu/2019/12/20/the-outrage-industrial-complex/

Tversky, A. & Kahneman, D. (1973) Availability: A Heuristic for Judging Frequency and Probability. Cognitive Psychology (5) pp. 207-232.

Van de Weert, A. (2021) Between Extremism and Freedom of Expression: Dealing with Non-Violent Right-Wing Extremist Actors. European Commission and Radicalisation Awareness Network.

Vergani, M. (2020) Understanding the Full Spectrum of Hate. The Interpreter. Accessed 01 June 2023; https://www.lowyinstitute.org/the-interpreter/understanding-full-spectrum-hate

Wallace-Wells, B. (2021) How a Conservative Activist Invented the Conflict over Critical Race Theory. The New Yorker. Accessed 30 May 2023; https://www.newyorker.com/news/annals-of-inquiry/how-a-conservative-activist-invented-the-conflict-over-critical-race-theory

Wanless, A. (2015) Why the West Can't Win this Propaganda War. Blog – La Generalista. 7 July 2023; https://www.linkedin.com/pulse/why-west-cant-win-propaganda-war-alicia-wanless

Webber, D. & Kruglanski, A. (2017) Chapter 3 – A 3N Approach. The Handbook of Criminology of Terrorism in (Eds) Psychological Factors in Radicalisation, La Free, G. & Freilich, J. First Edition. Wiley, pp. 33-43.

Williams, T. (2019) Ideological and Behavioural Radicalisation into Terrorism – an Alternate Sequencing. Journal for Deradicalisation, Summer 2019, No.19. pp.85-121.

Wilson, C. & Halpin, J. (2023) Action Zealandia, New Zealand's Aspiring Brown Shirts. National Security Journal. DOI: 10.36878/nsj20230319.02

ARTICULATING A MADANI FRAMEWORK FOR COUNTER-EXTREMISM: A MALAYSIAN PERSPECTIVE

Osman Bakar

ABSTRACT

The main aim of this article is to discuss the epistemological role of the Madani philosophy as a source of conceptual and policy framework for counter-extremism responses. The discussion is set against the background of contemporary discourse on terrorism in which there is growing criticism of the lack of objectivity in the approach to terrorism. The article argues that the global search for a universally agreed definition of terrorism would be better served if the issue of terrorism is to be discussed within the framework of a broader discourse on extremism of which it is treated as a special case. The article further argues that the Malaysia Madani concept and philosophy introduced by Anwar Ibrahim, the country's tenth and present Prime Minister, possesses the necessary epistemological characteristics to provide such a framework. The argument is buttressed by philosophical support from al-Farabi's theory of civilisation, the very theory that inspired Malaysia Madani. The most consequential element of epistemological support from the theory is the ethical concept of middleness (wasatiyyah), which is also known in Western thought as the golden mean. The article briefly discusses the sense in which the idea of middleness is consequential on the *madani* framework for counterextremism responses. In the conclusion, the preliminary nature of the discussion in the article is pointed out and the need for a refinement of the framework is emphasised.

INTRODUCTION

Of late, voices are more frequently heard that are critical of the contemporary discourse on extremism, especially of the violent type that is loosely termed terrorism. Critics argue that, in the global context, the term 'terrorism' is often used carelessly and imprecisely. This carelessness and imprecision are not without undesirable practical consequences on the fight against terrorism. These weaknesses in the conceptualisation of terrorism have resulted among other things in injustices against innocent people, not to mention ineffectiveness of many of the counter-terrorism responses itself. It is not uncommon to find individuals and groups being wrongly identified as perpetrators or sympathisers of terrorism only to be found much later that they are in fact innocent. Ending up with mistaken identities, particularly on serious charges related to terrorism that could mean a matter of life and death, is clearly a form of injustice that is intolerable and should be avoided from occurring.

Given the negative implications of vagueness in the definition of terrorism, it is not surprising that some researchers in the field of terrorism studies argue for a universally agreed definition of terrorism that transcends ideological and cultural differences. In their view, the importance of such a definition can hardly be overemphasised.

Anthony Richards, for example, a British academic who has published widely on terrorist related themes, stresses "the importance of conceptualising terrorism, both in the policymaking and academic environments." By 'conceptualising terrorism' he means instilling some analytical quality into the concept of terrorism, not least with the view of preventing the term being manipulated to justify all manner of counter-terrorism responses. Richards argues that the fact that the notion of "terrorism" has continued to be used as a subjective label underlines the need for a more analytical approach in determining what terrorism is and, by the same token, what terrorism is not. He reminds us that the definitional debate has been going on in public policy making institutions for more than a century now going back to the League of Nations' attempts to secure an agreed definition but with no end in sight.

The elusive nature of the definitional quest strongly points to a lack of objectivity in the approach to terrorism. I agree with Richard's critical assessment that analytical quality, which is an epistemological concern, is needed to be injected into the definitional discourse. In emphasising the need for analytical quality and at the same time criticising the prevalence of subjectivity in the discourse on terrorism Richards is, in fact, arguing for a greater appreciation of objectivity among discussants In other words, what he is emphasising is that it is long overdue that subjectivity should give way to objectivity in our contemporary global discourse on terrorism and in our responses to it and more generally to extremism, which is its main causal factor. I could not agree more with this view. As a student of comparative epistemology, I am fully aware of the importance of objectivity of thought in both Western and Islamic intellectual traditions. In Islam, objectivity is viewed as essential to the conception of justice. It is not mere coincidence that the prevalence of subjectivity and the prevalence of injustice in twenty-first century counterterrorism responses have occurred hand in hand. It may be argued that there is a causal relationship between the two phenomena, which lends strong support to Islam's insistence on the linking between objectivity and justice.

A better conceptualisation of terrorism, a better analytical quality input, and a better definition of terrorism, these three interrelated betterments are among those epistemological pursuits that are urgently needed in the present counterterrorism responses. By the way, Islam views the pursuit of these same betterments as being in conformity with its sense of justice as articulated in its Divine Law (Shari'ah). Richards raises another issue that is of relevance to Islamic Law. The issue pertains to what he sees as the failure of the main body of discussants to observe a clear distinction between the goal of terrorism and its method, which he views as a major obstacle to the quest for a more enlightened definition and conception of terrorism. This issue as well is of interest to Islamic law because it touches on the meaning and significance of one of its main principles or legal maxims, namely that goals do not justify means. The observation of this principle in both thought and action can go a long way towards making our world a safer, a more just, and a more peaceful place.

Not withstanding the fact that Islamic epistemology insists on the use of well-defined terms to ensure clarity and avoid confusion in public discourses especially on complex and problematic issues such as extremism and terrorism, Muslim contribution to the contemporary conceptualisation of terrorism debate has not fared any better. Mohammad Hashim Kamali, a world leading authority in Islamic Law, has touched on the definitional issue of terrorism in the context of a broader discourse on the theme of moderation and the middle path in the sense of *wasatiyyah* understood in Islam. From the perspective of Islamic epistemology Kamali adopts the right approach in discussing extremism in the light of the doctrine of *wasatiyyah*, for as he says "extremism is the conceptual opposite of moderation." But his characterisation of terrorism as a form of "practical extremism" (al-tatarruf al-'amaliy) needs further scrutiny. His attempt to identify the essential element of terrorism with "acts of terror and violence…..that kill innocent people and cause destruction" has not resolved the definitional issue since it begs the question of what is meant by "act of terror." From the Islamic perspective itself, a universally agreed definition of terrorism is also yet to be found.

The main purpose of this article is to provide a theoretical framework for counterextremism that may be described as *madani* in spirit and Malaysian in its formal characteristics. The foregoing discussion is aimed at providing justifications for the topic of this article. The first justification is that a more fruitful discourse on terrorism and counterterrorism measures is more likely to emerge from an enlightened discussion of extremism of which terrorism is to be viewed as a special form than from any other approach. It follows from this perspective that there is merit in pursuing a more serious discourse on counterextremism responses to help us better plan counterterrorism strategies. In short, the focus should be on extremism. The second justification is that it is desirable to bring aspects of *madani* philosophy into the discourse on extremism and counterextremism given its special relevance to Malaysia's nation and civilisation building. The special relevance may be viewed in two main respects. First, the philosophy is conceptually related to Malaysia's new national vision under the leadership of Dato Seri Anwar Ibrahim, the present (tenth) Prime Minister. Second, given Malaysia's rich and diverse religious traditions each of which possessing its own conception of moderation and the middle path, it would be a good idea to explore the possibility of formulating a Malaysian perspective on extremism and terrorism that is based on its common spiritual teachings. Moreover, given the fact that one of the core elements of Madani philosophy is its advocacy of moderation and the middle path as a defining element of human civilisation, it would also be meaningful to speak of a *madani* framework for counterextremism approaches. In the light of these considerations, I propose to outline this framework in this article. But for the purpose of clarity, before outlining the framework, it is necessary to make some preliminary remarks on *madani* philosophy.

PRELIMINARY REMARKS ON MADANI PHILOSOPHY

The Arabic word *madani* was first used as a philosophical-scientific concept in the writing of the classical Muslim philosopher al-Farabi (870 CE – 950 CE) who hailed from Farab in present-day Kazakhstan in Central Asia. Al-Farabi used the term to convey the meanings of civilised or civilisational and civilisation. In his celebrated work, Enumeration of the Sciences (Ihsa' al-'ulum), which earned him the honorary title "The Second Teacher," the first being Aristotle, al-Farabi discusses a new universal science, which he calls *al-'ilm al-madani*, meaning "science of civilisation." His discussion of the science contains the fundamental elements of his universal theory of civilisation, which influenced Ibn Khaldun. The term *madani* is etymologically related to the word *madinah*, which means city. The significance of the connection between the two terms is, for al-Farabi, not just etymological but also conceptual and philosophical. His theory of civilisation and civilisation-building was inspired by both ancient Western political thought and the Prophet Muhammad's historic civilisation-building in Medina (al-Madinah), the new name that he gave to the old city of Yathrib, and which simply means "The City." Understandably, this new city-state under the Prophet's rule, which was at once temporal and sacred, soon came to be fondly known as "The City of the Prophet" (al-Madinat al-Nabiy).

Al-Farabi synthesised the political ideas of Plato (428/427 BCE – 348/347 BCE), Aristotle (384 BCE – 322 BCE), and the Prophet (c. 570 CE – 632 CE) within the comprehensive unitary perspective (al-tawhid) of Islam. Within this perspective Plato's idea of philosopher-king became identified with the Abrahamic prophet-lawgiver and Aristotle's ethical virtues with the Prophet's civilisational order in Medina. What may be called al-Farabi's theory of civilisation and civilisation-building in its totality is woven from his philosophical ideas that he discussed not in one single book but in several of his books. The theory is remarkable for its content, universal in its message, and perennial in its significance. Its main ideas include: (1) the ultimate purpose of civilisation-building is the attainment of happiness in this world and in the hereafter; (2) happiness is essentially the possession of rational virtues in the form of knowledge and wisdom, both theoretical (nazariyyah and practical ('amaliyyah), which define the health of the intellect and intelligence ('aql); the possession of spiritual and moral virtues in the form of excellent character; and the possession of artistic virtues in the form of skills, innovativeness, and creativeness; (3) as dictated by political virtues, *madani* polities must put in place mechanisms for counter-degeneration of societal health, that is, prescribing ways of preventing virtuous governments and ways of life from degenerating into corrupt governments and ignorant ways of life; if civilisational degeneration has become a reality, al-Farabi's theory posits the necessity of measures to restore governments and ways of life to their previous virtuous state; and (4) civilisational sustainability depends on enlightened political education, effective political leadership, and well-planned political succession. These ideas define al-Farabi's *madani* philosophy, which we now seek to apply to our search for veritable solutions to the problem of extremism.

THE NEED FOR CIVILISATIONAL APPROACHES TO HUMAN PROBLEMS: THE MADANI APPROACH

Man is a multidimensional living entity with multiple identities and goals in life. As such, a human problem is bound to be multidimensional in nature entailing interdisciplinary approaches to its solution. Given the generally accepted meaning of civilisation as the biggest and all-inclusive cultural unit, there is no other approach that is more multidimensional and more interdisciplinary in its epistemological engagement than the civilisational approach. Al Farabi has shown in his theory of civilisation, especially in his science of civilisation, the truth of this claim. The civilisational approach as articulated by al-Farabi is truly universal in nature. Following al-Farabi, this same approach may be termed the *madani* approach.

As a corollary, it is also true to say that the civilisational approach is the most preferred when it comes to the need to address multi-dimensional human problems, especially those of our times. In affirming this view, we do not mean that the civilisational approach even in its best conception or interpretation renders insignificant the use of other approaches in solving human problems, such as the approaches proposed by some academic disciplines or by specific philosophies and theories. On the contrary, approaches of a specific nature too have their value and significance that could even help enhance the quality of the civilisational approach itself. There is another merit that is unique to the civilisational approach. This universal *madani* approach is empowered with several epistemological features that would enable it to offer a macro, holistic, and inclusive view of things that other approaches of a specific nature could not provide. The latter approaches are only found to be good in displaying a micro-view of things within their respective spheres of methodological competence.

Given the need for civilisational or madani approaches to the solutions of human problems, as we have just shown, we further argue in this article that specific ideas in al-Farabi's *madani* philosophy are of great relevance to issues of extremism. But, before proceeding to this concrete and specific application of *madani* philosophy to extremism, it is deemed desirable to first clarify the conceptual link between al-Farabi's *madani* philosophy and the Malaysia Madani philosophy and vision espoused by Dato Seri Anwar Ibrahim, Malaysia's tenth and present Prime Minister.

Al-Farabi's *madani* philosophy has been circulating in Islam and the West for centuries until modern times, especially in intellectual circles among Jews, Christians, and Muslims. In modern times, there appears to be a revival of interest not only in his madani philosophy but also in other aspects of his thought, which is undeniably comprehensive. But the main interest in his thoughts was mainly academic, at least not until the decade of the 1970s that witnessed what was then popularly known as the Islamic resurgence or revival era. During that decade and beyond youth leaders in Southeast Asia, the most prominent of whom were Anwar Ibrahim and the Indonesian Nurcholis Majid, were instrumental in popularising the term *masyarakat madani*, which was then widely understood as the Malay equivalent of “civil society.” The term became a rallying cry for Anwar and his fellow intellectual-social activists to spearhead the civil society movement, albeit mainly in an Islamic setting. After he joined the Mahathir Administration in 1982, he continued to be committed to advancing the understanding and practices of *masyarakat madani*. During the Mahathir Administration the most visible public event in connection with *madani* issues was perhaps the *Konvensyen Masyarakat Madani* held on 19-21 September 1996 at the National University of Malaysia (UKM) and which Anwar, then Deputy Prime Minister, patronised and officiated.

Anwar earned our profound respect for his steadfast embrace of the *madani* philosophy, first in raising *madani* from being a mere subject of intellectual interest to become a social agenda for the civil society movement, then in securing a government and public space for *madani* in the Mahathir Mohamad Administration when he was part of it (1982-1998), and finally as Prime Minister in declaring the *madani* concept as Malaysia’s new national vision, new national policy framework, and new national slogan. Anwar’s deep knowledge of the *madani* philosophy is unquestionable. But to turn a philosophy that is at once ancient and comprehensive into a source of vision and policy framework for a modern nation like Malaysia requires wisdom and ingenuity. Anwar’s six pillars of Malaysia Madani are a testimony to that ingenuity.

The pillars – sustainability, care and compassion, respect, innovation, prosperity, and trust – which are collectively referred to as Malaysia Madani’s “drivers and policies” may be shown to be conceptually connected to some of the main ideas embodied in al-Farabi’s *madani* philosophy that we have enumerated. More precisely, each of the pillars is related to one or more of the virtues – rational, spiritual-moral, artistic, and political – that are at the core of the *madani* philosophy. These pillars need detailed expositions to help citizens better understand their meanings and significance as social ideals. But, to undertake the expositional task, a familiarity with the *madani* philosophy as conceptualised by al-Farabi would prove to be extremely helpful. To emphasise this point, we may argue that Malaysia Madani offers a policy framework for counterextremism since central to al-Farabi’s *madani* philosophy is ethics of the middle path which runs counter to extremism.

A MADANI FRAMEWORK FOR COUNTER-EXTREMISM: KEY PRINCIPLES

In my view, the most fundamental shaping element of a *madani* framework for counterextremism is the idea of middleness by which is meant the ethical virtue of moderation and the middle path. The *madani* philosophy, which is in harmony with the Islamic teaching on *wasatiyyah* values, affirms the Aristotelian idea of the golden mean. As emphasised by al-Farabi, good actions are “moderate, mean actions between two extremes, both of which are bad, the one excessive and the other defective.” Middleness may then be viewed as the civilisational antidote to extremism and as a preventive social medicine. Indeed, middleness is the raison d’etre of civilisation and a just world order. In accordance with the *madani* philosophy, middleness is the common underlying principle of all the pillars of Malaysia Madani. It is the civilisational spirit and virtue that breathes into each pillar to turn it into a reality. Without middleness, sustainability could not be achieved The idea of sustainability pertains to both the natural and the human social orders. Human greed, which is the opposite of middleness, is the main root cause of the biophysical disorder and the rampant injustices in the world.

The next key principle shaping a *madani* framework for counterextremism is the doctrine of unity. This doctrine is especially necessary for a multiethnic and multireligious country like Malaysia. It is a simple idea to understand, but it is also rich in meaning that is not fully appreciated by many people. For the purposes of this article, I would like to emphasise three conceptual components of the idea of unity that may be viewed as particularly relevant to counterextremism measures. These are the concepts of inclusiveness, shared values, and interdependence. It may be argued that the practice of the six pillars and the three concepts in question may enhance and empower each other that would lead to the greater unity of Malaysia Madani. If that were to be the case, then these practices pursued in an integrated manner would help serve as a potent preventive measure against extremism, be it political, ethnic, or religious.

CONCLUSION

Within the limited scope of this article, my discussion of the topic could only be preliminary in nature. The topic is, without doubt, an important one. The preliminary remarks need to be further expanded and refined. Each of the six pillars of Malaysia Madani that define the *madani* framework needs to be better articulated. A deeper discussion of a more concrete role for middleness perspectives in counterextremism responses is obviously needed.

THE ROLE OF MEDIA AND DIGITAL COMMUNITIES IN PCVE STRATEGIC COMMUNICATIONS: THE PHILIPPINES EXPERIENCE

Tiffany Jane Pery Buena

ABSTRACT

This article describes the internal security situation in the Philippines in recent history, along with the role and responsibility the media plays in portraying the conflicts and reinforcing social cohesion in the regions most affected by these conflicts. It will also explore the different ways threat actors utilise traditional and social media to disseminate their ideologies and initiate radicalization in the youth, their most important target audience. The Philippines experience is further rounded out by the author's personal experience of coordinating crisis communications during the Daesh-inspired attack on Marawi City in 2017, and currently on communications for the Enhanced Comprehensive Local Integration Program (E-CLIP), the government's flagship reintegration program for former local rebels and violent extremists. The role of media—and media relations—in preventing and countering violent extremism is essential not only in communicating the actual situation on the ground, but also to reinforce and employ the role of media as the fourth estate. Media relations serve to strengthen the bond between the state and media practitioners, as they not only advocate not just for the truth, but also for peace. The communications perspective is also paramount in disseminating information to the media and the public, especially in determining the medium by which this information is to be distributed. Moving forward, new media and social media is the new battleground for communicators, creating a new opportunity for communicators to collaborate with media, journalists and influencers to flip the script of radicalisation and violent extremism in the region.

Keywords: Philippines, strategic communication, PCVE, counterterrorism, social media, media relations, reintegration, counterinsurgency

A COMPLEX INFORMATION ENVIRONMENT

The security situation in the Philippines is complex and multilayered, giving rise to a number of risks and incidents in the past decade. Mendoza, Ong, Romano and Torno (2021) have attributed terroristic acts in the Philippines to two strands. The first strand in question are the Islamist-secessionist groups in Mindanao –the Moro National Liberation Front (MNLF); its splinter, the Moro Islamic Liberation Front (MILF), among other modern groups like the Abu Sayyaf. The other strand, the Communist Terrorist Groups (CTGs), namely the Communist Party of the Philippines - New People's Army (CPP-NPA), are one of the oldest communist insurgencies in the world, with the aim of overthrowing the government. These two movements are responsible for the terrorist attacks in the Philippines in recent years, and places the Philippines eighteenth in the 2022 Global Terrorism Index. Radicalization and recruitment are motivated mainly by disgruntlement in their current socioeconomic situations, and the lack of basic government services in the regions where these movements operate. Interviews with beneficiaries of the Enhanced Comprehensive Local Integration Program (E-CLIP), the Philippines' reintegration program for former violent extremists and rebels, point to most recruits believing in promises of housing and financial assistance in exchange for their participation in terrorist activity, all in the name of either radical Communist-Maoist or Islamist ideology.

Another factor that poses an additional risk factor in terms of radicalisation among youth, particularly in Mindanao, is called *rido*, used to pertain to clan feuds or clan conflict. Torres (2014) characterizes this by 'sporadic outbursts of retaliatory violence between families and kinship groups as well as between communities.' This occurs especially in areas where there is a perceived weakness in government or central authority, or lack of justice and security. While the radical Islamist terrorist groups usually dominate the international and local media's attention, *rido*-related incidents are more pertinent in the daily lives of people in Mindanao. Mindanaoans, in fact, are more concerned about *rido* in their communities than the conflict between the government forces and separatist rebels. *Rido* may actually influence decision-making and policy processes in and for Mindanao more than any other issue stated in this paper.

Further complicating this already internecine situation is the involvement of Foreign Terrorist Fighters (FTFs), who often attempt to associate themselves with local groups by offering much-needed financing and radicalisation doctrine. The porous nature of the Philippines' borders, along with the socio-cultural similarities with co-littoral states Indonesia and Malaysia, contribute to the ease by which FTFs move and cooperate with like-minded threat actors in the country.

Cyberspace, particularly new media, is yet another rising theatre in the fight for information dominance. According to Corpus Ong (2018), with a complicated hierarchy of digital workers, whose ability to speak the language of the masses are orchestrated and controlled by advertising and public relations strategists, in an attempt to dominate the information landscape as 'architects of network disinformation.' This interesting mix of anonymity and fame in the cyber sphere serves to blur once-clearly defined lines between fact and fiction. Since the May 2016 Philippine national elections, orchestrated digital campaigns have continued to spread disinformation, and have even managed to exploit the gaps in technological and regulatory features of social media platforms. Facebook executive Katie Harbath even went so far as to say that the Philippines is the "patient zero" of the global information disorder epidemic (Cabañes, Santiago, 2022). This makes the tenuous information landscape of the Philippines a stomping ground for threat actors who wish to use it for radicalisation and recruitment.

The political landscape in the Philippines has not made easy the passage and implementation of key laws on preventing and countering terrorism. However, the passage of the Anti-Terrorism Act in 2020 and the adaptation of a whole-of government approach has helped PCVE efforts, both in policy and on the ground. All these factors are factors contributing to the challenge of implementing counterinsurgency (COIN) strategic communication (STRATCOM) efforts in the Philippines, and yet present opportunities for success, should the right opportunities and messaging emerge.

THE FOURTH ESTATE AND THE THIRD PLACE: THE IMPORTANCE OF MEDIA PRACTITIONERS AND DIGITAL SPACES IN PCVE

The role of journalism and mass media as the fourth estate is long-standing, and crucial to the preservation of Philippine democracy. Its rights to freedom of expression, speech and the press is enshrined in Article III, Section 4 of the Philippine Constitution: *"No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances."* The media's role as the fourth estate, as the agenda-setter and watchdog, is a disruptive counterpoint to the power of the state. Journalism ensures the transparency and accountability of the government to its people. However, and somewhat ironically, the Committee to Protect Journalists (CPJ), an independent nonprofit that promotes press freedom worldwide, ranks the Philippines 7th on the 2022 Global Impunity Index, an annual report wherein countries are ranked according to the number of journalists are murdered in the line ranks it below Somalia, Syria, South Sudan, Afghanistan, Iraq and Mexico and above Myanmar, making it the highest-ranked Asian country on the list (Committee to Protect Journalists, 2022). At this juncture, it is necessary that the state maintain good relations with the media, and view them as partners and fellow advocates in communicating the gains of COIN operations and in maintaining social cohesion.

Another disruptive technology coming into play is the rise of new media—social media, digital communities and influencer culture—that introduced the concept of citizen journalism, defined as the collection and analysis of information from the general public, especially through the internet (Wolbert, 2021). While formally-trained journalists would employ the scientific research method in creating their stories and narratives, citizen journalism, if irresponsibly or deliberately analysed and presented, may result in disinformation and the formation or confirmation of a cognitive bias in the target audience. Furthermore, this new breed of pundits and documenters will often try to form online communities, through which they nurture their purpose and narrative through stakeholder engagement and experience-sharing. These online communities are now the new "third places": social surroundings that are separate from the two usual social environments of home ("first place") and the workplace ("second place"). Urban sociologist Ray Oldenburg (1989) argues that third places are important for civil society, democracy, civic engagement and establishing feelings of a sense of place. Third places allow people the comfort and company of a community, and reinforces the feeling of social acceptance. These shared positive experiences can be easily replicated digitally using Web 3.0 technology, with platforms that now support more forms of media than ever before. These communities lay vulnerable to extremist discourse and radicalization, as extremist narratives change to adapt to current sentiments and language much quicker than government STRATCOM messaging can counter or provide alternative narratives.

THE STRATEGIC COMMUNICATIONS APPROACH

Doody (2023) lists strategic communication as the largest independent variable to ever be published in literature on counterinsurgency, and states that the relationship between the use of propaganda strategies such as radio and media broadcasts, leaflets, and newspaper messaging, and COIN outcomes is a major theme in the study's reviewed literature. Similarly, a series of RAND reports by Paul et al. (2010) analysing the efficacy of strategic communication across a large dataset of insurgencies strongly suggests that STRATCOM may be critical to obtaining successful COIN outcomes. Other research also points to how strategic communication can be used to bolster other COIN operations to obtain successful outcomes. The United Nations Office of Counter-Terrorism (UNOCT) recognizes the importance of strategic communication's vital role in countering and reducing the threat of terrorism, harmful narratives, misinformation and disinformation, and hate speech. The UNOCT even goes so far as making strategic communication the first component in its PCVE Portfolio on the Global Programme on PCVE.

However, Doody also cautions that strategic communication is more likely to succeed when it is implemented "as part of a broader, proactive strategy with relevance to local values and social relations." He posits that in some cases where strategic communication fails, it is because implementing authorities do not enjoy the trust and legitimacy of their target audiences, like the general public. If a government's STRATCOM efforts are in opposition with the culture and values of the target audience, it risks delegitimising its COIN efforts and even perhaps increasing the legitimacy of the insurgents among the populace. In the same vein, when government is put in the position of primarily just reacting to the opposing narrative, then its communication efforts are most likely to fail.

Paul (2010) counts the following factors in ensuring the success of a strategic communication COIN campaign (Paul et al., 2010, pp.56-57):

1) Delivering on promises (COIN force and government actions were consistent with messages);
2) Expectation management (COIN forces maintained credibility with local populations;
3) Messages cohering with the overall COIN approach;
4) Messages and themes were coordinated across all involved government agencies;
5) There was an "earnest information operations, psychological operations, strategic communication, or messaging effort;" and
6) There was unity of effort in mission command.

This underlines the importance of the whole-of-government approach in ensuring successful COIN operations. This also shines a light on the role of media and journalists in ensuring legitimacy, transparency and the subsequent success of COIN operations not only in the Philippines, but also in the region. These factors, while only sporadically apparent in the PCVE STRATCOM experience, contributed to the success of the campaigns where three or more of these were present.

MEDIA RELATIONS THROUGH THE LENS OF DEFENSE

"The press may not be successful much of the time in telling people what to think, but it is stunningly successful in telling its readers what to think about," Bernard S. Cohen's statement in 1963 still rings true today as the agenda-setting theory sets the tone for how the media is an influential part in how issues gain national attention. Whether social or political, it is the media that generates public issues that generates discussion and discourse, whether it be in the halls of government or at the family dinner table. The media may be boon or bane to the PCVE efforts of the government, depending on how it nurtures, if at all, its relationship with the fourth estate. It is an even more crucial question in the context of national defense and security, wherein the concept of media relations usually entails walking the fine line between transparency and accountability, and operational security. The media, and its coverage of conflict throughout history, has showed time and again that it is capable of using words, photographs and video to inadvertently influence public perception of the state's COIN efforts, especially in kinetic operations. Nevertheless, the government's relationship with the media should remain founded on mutual trust, authentic concern and involvement, and a shared vision of a truly, sustainably peaceful society. The media and government should have a mutually beneficial relationship, wherein they recognise each other not just as stakeholders, but as partners in PCVE. Managing communications and relationships all across the spectrum of reporting is one of the factors that must be handled delicately and with mutual respect. Through elevating the level of discourse on preventing violent extremism, the media and government are partner-advocates who work together in telling the story and rallying public support towards the end of all forms of violent conflict and extremism.

LEVERAGING THE POWER OF MEDIA AND DIGITAL COMMUNITIES IN PCVE: THE PHILIPPINES CONTEXT

There are multiple methods to disseminate information on the government's PCVE efforts to media stakeholders, and in this light, the government communicator utilise a wide range of tools and techniques to obtain news coverage and monitor reporting on their organisation over time. Publications, press releases and public affairs guidance issuances are the most commonly used examples, but it is important to constantly research new, innovative options to disseminate information. During the Marawi siege in 2017, communicators throughout the Department of National Defense (DND) found that powerful imagery from the ground, such as videos or photos taken by the soldiers involved, and inspirational anecdotes from the frontline were the ones that gained more traction on both traditional and social media. As these humanized the faces of conflict that were much more impersonally depicted in photos on the nightly news or in publications. These images and stories were so powerful that it inspired netizens to start a community –later dubbed "Support Our Troops: Marawi Heroes"—wherein volunteers extended various forms of support to the soldiers involved in the five-month battle, whether in the form of a child's letter or the distribution of hygiene and care packages in order to cheer on and encourage soldiers on the frontlines. Media featured these stories alongside the regular coverage of the conflict, which served to invalidate the perception of the IS-inspired Maute Group as 'heroes' by juxtaposing the multiple images of Filipino soldiers, who were from similar backgrounds, yet fighting for people of Marawi City.

It is also important to use the most appropriate means of sending messages for the best impact. Operational security, message goal, intended audience, and potential reach are among the factors considered in determining how the information of message is relayed to the media. An example of this is the messaging for *Task Force Balik-Loob* (Task Force Return to Society, also known as TFBL), the strategic communication campaign for E-CLIP, the flagship reintegration program of the Philippine government for former violent extremists. The TFBL was part of a larger messaging campaign of the national government to end local armed conflict that encouraged insurgents to return to the fold of society. Core messaging from the national campaign was cascaded to the local communities—and local media—in the dialects commonly used in their areas. Furthermore, in localities where broadcast news or the internet were intermittent or nonexistent, the Task Force used messages printed on tarpaulins or other physical media, placed in areas with high foot traffic.

Based on interviews with former extremists who availed of the E-CLIP, the most common reason behind their decision to return to society was disillusionment with the ideology behind the insurgency, to which TFBL messaging provided a counter-narrative for them. Their families comprised the second most common reason, as they proved effective in convincing former extremists to reintegrate. Reunion with their families also proved to be one of the stronger themes in the TFBL campaign, as it resonated the most with its intended audience.

CONCLUSION: WAYS FORWARD

In order for a communication strategy to attain its goals, especially in an information environment with multiple actors all angling for legitimacy in the public eye, an important relationship with the media and digital communities should be nurtured and managed in order to supplement COIN operations and PCVE efforts. High-quality content is essential and should always answer the question "Why should I care?" in order for the message to appeal to target audiences. Empowering and engaging communities through stakeholder involvement may also contribute to the success of a communication strategy, as digital third places continue to evolve and exit the realm of social media and into smaller spaces, it is critical that communicators also grasp the proper use of new and disruptive technology. Authentic, quality messaging that resonates with your target audience creates official and unofficial champions, who will also help take the messaging further down the line to the end targets, through tailoring and localisation: the real meaning of the 'one message, many voices' STRATCOM concept. Collaboration with journalists and other media stakeholders, and community leaders on the dissemination of messages ensures that the messaging stays clear and consistent. Fostering a professional, authentic relationship will build trust between the organization and the media, which in turn will augment and sustain PCVE efforts and reinforce social cohesion. This combination of messaging, content creation and management, media relations, stakeholder and community engagement, and the whole-of-government approach have attained considerable gains in the Philippine experience, and the lessons learned here will improve the process of how strategic communication is appreciated and utilised in PCVE practice.

REFERENCES

Cabañes, J., Santiago, F. (2022). *Counter-Disinformation Beyond Fact-Checking: Insights From the Philippines*. Fulcrum ISEAS – Yusof Ishak Institute. https://fulcrum.sg/counter-disinformation-beyond-fact-checking-insights-from-the-philippines/

Committee to Protect Journalists. (2022). *Killing with impunity: Vast majority of journalists' murderers go free. 2022 Global Impunity Index*. Community to Protect Journalists. https://cpj.org/wp-content/uploads/2022/10/CPJ_2022-Global-Impunity-Index.pdf

Corpus Ong, J. & Stewart, D.T. (Hosts). (2018, September 10). Fake news in the Philippines, with Jonathan Corpus Ong [Audio podcast episode]. In Asia Dialogues. Carnegie Council. https://www.carnegiecouncil.org/media/series/asia/20180910-fake-news-philippines-jonathan-corpus-ong

Doody, S. 2023. "Government Responses to Asymmetric Threats: The State of the Literature on Counterinsurgency from 2002 to 2022—The Information Lever of Power." *Global Responses to Asymmetric Threats*. College Park, MD: START (July).

Mendoza, R. U., Ong, R. J. G., Romano, D. L. L., & Torno, B. C. P. (2021). *Counterterrorism in the Philippines: Review of key issues. Perspectives on Terrorism*, 15(1), 246–261. https://www.universiteitleiden.nl/perspectives-on-terrorism/archives/2021#volume-xv-issue-1

Oldenburg, R. (1999.) *The Great Good Place* (Part I). Da Capo Press. (Original work published 1989)

Torres, W. M. (2014). Introduction. In *Rido: Clan feuding and Conflict Management in Mindanao* (pp. 3–5). introduction, Ateneo de Manila University Press.

Vision of Humanity. (2023, June 14). *Global terrorism index: Countries most impacted by terrorism*. Global Terrorism Index. https://www.visionofhumanity.org/maps/global-terrorism-index

Wolbert, M. (2021). *Citizen Journalism: What's the deal?* Reporter Magazine. Rochester Institute of Technology. https://reporter.rit.edu/features/citizen-journalism-whats-deal

PART 4

ARTICLES BY OTHER SUBJECT-MATTER EXPERTS

BUILDING DIGITAL RESILIENCE IN PREVENTING AND COUNTERING VIOLENT EXTREMISM

Ho Kian Wei

ABSTRACT

Recognising that violent extremist and terrorist groups have adeptly harnessed technology to advance their agendas, a Digital Resilience Initiative (DRI) framework that aims to prevent and counter violent extremism in the digital realm has been introduced by the Malaysian government. Nonetheless, this paper discusses the challenges and opportunities to build digital resilience in preventing and countering violent extremism in Malaysia. By focusing on four pivotal areas, namely awareness and knowledge, support and empowerment, regulation and accountability, and cooperation and collaboration, the author argues that the path toward building digital resilience to counter violent extremism in Malaysia requires a multi-stakeholder, inclusive, and data-informed approach, transcending gender, age, and traditional boundaries to safeguard society against the evolving threat of online radicalisation.

Keywords: digital resilience, PCVE, DRI framework, multi-stakeholder approach, data-informed approach

INTRODUCTION

In an increasingly interconnected world, violent extremist and terrorist groups have demonstrated a high level of adaptability when exploiting technology to advance their agendas. In fact, numerous extremist groups with various ideological orientations were initial adopters of social media, as they recognised their potential for recruitment and the dissemination of propaganda (Conway et al., 2019).

In Southeast Asia, the threat of online self-radicalisation is a very real phenomenon. Research has shown that increased use of social media by individuals has abbreviated the radicalisation period to months rather than years (The Soufan Center, 2021). Additionally, the presence of established terrorist and violent extremist groups in Southeast Asia has put local law enforcement and counter-terrorism agencies under pressure to adapt to shifts in terrorist activities, as well as changes in the approaches used for investigating these activities (UNICRI and UNCCT, 2021). Against this backdrop, the Malaysian Minister of Foreign Affairs, Zambry Abdul Kadir mooted the idea of a Digital Resilience Initiative (DRI) framework that aims to prevent and counter violent extremism in the digital realm (The Star, 2023).

The DRI framework consists of four key strategic areas that are interrelated and complementing with each other. The opportunities and challenges of respective strategies will be outlined in the following sections. The author argues that a multi-stakeholder approach is at the core of an effective PCVE policy, particularly in the domain of building digital resilience.

AWARENESS AND KNOWLEDGE

Educational initiatives, including public awareness campaigns led by different institutions, such as the Malaysian Special Branch, the Department of Islamic Development of Malaysia (JAKIM), and other civil organisations have been one of the primary approaches to counter violent extremism. With a significant portion of social media users in Malaysia comprised of young people, the imperative lies in fostering digital and media literacy skills within this demographic. While counter-narratives and content removal represent prevalent methods to mitigate the threat of violent extremism, these methods are inherently reactive, short-term in nature, and fail to address root causes of concern (Rosand and Winterbotham, 2019).

To ensure the advancement of educational initiatives, a proactive stance must be adopted within educational institutions. The Malaysian government should cooperate with schools and universities to introduce accessible and compulsory media literacy programmes targeting students spanning from primary to tertiary education levels. A strategic starting point involves aligning these programmes with the framework dedicated to strengthening digital competencies, encompassing aspects like information and data literacy, communication and collaboration, digital content creation, safety, and problem solving under SDG 4 Quality Education (Law et al., 2018).

Subsequently, the National Unity Action Plan 2021-2030 should be integrated with the framework to draft the programmes in order to fit the Malaysian context - a country that promotes peaceful co-existence, tolerance, and positive multi-religious and multicultural engagements. This initiative, as a long-term solution in the fight against violent extremism, necessitates regular training for educators, given the ever-changing landscape of the online realm. Additionally, it is also the responsibility of involved actors, such as the Ministry of Education and the executive committee of educational institutions to continuously ensure the proper delivery of the programmes by educators and a sufficient level of awareness on the subject matter among students.

Beyond passively receiving information by students on the PCVE topic, a more proactive approach that schools and universities can adopt is to inform students where can they find extra accurate information, such as *mycveguide.com* and *initiate.my*.

SUPPORT AND EMPOWERMENT

The growing online presence of potentially vulnerable youths, coupled with the established violent extremist presence in the region, has pressed the Malaysian government to accelerate the progress in building digital resilience (UNICRI and UNCCT, 2021). On the other hand, the situation of gender equality in Malaysia emerges as a profound concern. As highlighted in the Global Gender Gap Report by the World Economic Forum (2023), Malaysia ranks 102nd out of 146 countries. This indicates that women in Malaysia (especially from rural areas) have more grievances than men, which leads them to be more vulnerable when encountering violent extremist content. In response to these challenges, the ASEAN Plan of Action to Prevent and Counter the Rise of Radicalisation and Violent Extremism (2018-2025) was established as a direct outcome of the Manila Declaration 2017. The Plan of Action urges the member states to empower youth and women to enhance their capacity to prevent the rise of radicalisation and violent extremism. Furthermore, it underscores the importance of involving women in the PCVE efforts (ASEAN, 2018). Indeed, the role of women in terrorism has been largely addressed, as violent extremist groups have become more resilient in their strategies using women in recruitment, providing financial support, and conducting domestic attacks.

In line with the Plan of Action, JAKIM assumes an important role in encouraging women to participate in leadership positions in order to promote moderation and tolerance as part of the PCVE programme. To further bolster these efforts, JAKIM should collaborate closely with the Ministry of Women, Family, and Community Development to establish programmes building digital resilience among women from rural areas, considering the fact that women there are often more vulnerable and have less autonomy to make informed decisions.

REGULATION AND ACCOUNTABILITY

Currently, Malaysia relies on the Prevention of Terrorism Act 2015 (POTA) and the Special Measures Against Terrorism in Foreign Countries Act 2015 (SMATA), as well as the Penal Code to counter violent extremist and terrorist acts (Aziz, 2021). In the digital realm, the Malaysian Communications and Multimedia Commission (MCMC) is at the forefront of countering violent extremist narratives. However, a limitation arises from the absence of a specific monitoring & evaluation framework within the current National Action Plan on Preventing and Countering Violent Extremism (NAPPCVE), thus, undermining the promotion of transparency and accountability in the PCVE area (Shamsuddin, 2022).

Concurrently, Malaysia has resorted to the Sedition Act of 1948 and the Communications and Multimedia Act of 1998 to address hate speech issues. Nevertheless, these laws and regulations are increasingly viewed as inadequate for cultivating digital resilience, particularly as they do not include discriminatory or hate speech directed at minority groups, such as LGBTQ+ and refugees (Elumalai, 2023). Consequently, navigating the delicate balance between preserving national values and upholding human rights assumes significance in the Malaysian context.

The author posits that community engagement and reporting mechanisms are interdependent in building digital resilience. Policymakers should regularly engage with religious leaders, as the latter are accountable for ensuring their followers have the ability to critically identify extremist information. Simultaneously, the government must forge collaborative bonds with local communities to grasp the nuances of their grievances and anticipate potential technical issues they may encounter. In light of these considerations, an accessible, anonymous, clear, and transparent reporting mechanism for citizens to report extremist content needs to be established.

COOPERATION AND COLLABORATION

Cooperation and collaboration among diverse stakeholders are undeniably vital for building digital resilience in preventing and countering violent extremism in Malaysia. The Malaysian government should embrace a multi-stakeholder approach, involving non-governmental organisations, tech companies, think tanks, and even influencers. A prominent example is the Tech Against Terrorism initiative where collaboration among tech companies, counter-terrorism experts, and developers takes place. Establishing a public-private partnership in PCVE is an effective approach, as "the companies feel a business incentive to create a digital environment where their users feel safe" (Hadley et al. 2016). Indeed, major private companies normally may possess better technology or ICT capabilities than the government in detecting violent extremist content. Thus, having a healthy and mutually beneficial partnership between the government and the private sector is complementary to enhancing the national digital capability.

In parallel, think tanks play a crucial role in the PCVE landscape, entrusted with conducting data-informed research and presenting the government with effective and evidence-based policies. However, the barrier of data inaccessibility potentially hinders researchers' ability to create discursive discourse on PCVE and inhibits innovative solutions to build digital resilience (Shamsuddin, 2022). The open-source intelligence (OSINT) is an alternative way to gather data from publicly available information. The advantages of this technique are that it can often be less complicated and easier to share (Cross, 2023). Nonetheless, this technique requires people with certain skills and knowledge to perform. Therefore, the Malaysian government should allocate the necessary resources and foster collaborations with universities to train people in this domain to compensate for the reality of data inaccessibility.

Considering the impacts influencers have on Malaysian society, the Ministry of Communications and Multimedia (MCM) can leverage this phenomenon at their disposal. The government should cooperate with influencers to disseminate the correct information pertaining to diversity, peace, and respect to counter violent extremist narratives. This strategy enables the government to establish a more direct line of communication with the public, particularly the young demography undergoing crucial cognitive development.

CONCLUSION

In conclusion, the high accessibility of the internet has become a breeding ground for violent extremist groups. Therefore, digital resilience stands as a formidable and collective barrier against the spread of extremist ideologies. By equipping individuals with the tools to discern fact from fiction, digital resilience contributes to informed decision-making. Moreover, fostering digital resilience promotes more discerning and vigilant digital citizenship, creating a collective defence against online radicalisation. Thus, building digital resilience must be a priority in the Malaysian PCVE policies. By looking at four key strategic areas outlined in the DRI framework, it is clear that a multi-stakeholder approach is crucial for the effectiveness of building digital resilience from the governmental level to the individual level. Furthermore, it should be noted that PCVE policies need not only to include the conventional male perspective but also females and children. Last but not least, a data-informed approach is also important to advance the current PCVE policies.

REFERENCES

Aziz, W. (2021). The role and initiatives of Malaysian government agencies in countering violent extremism and terrorism. Journal of Public Security and Safety. Edisi Khas, 1-19. https://www.moha.gov.my/images/maklumat_bahagian/ipsom/jurnal/volume11/edisi_khas_num_1.pdf

Conway, M., Scrivens, R. & Macnair, L. (2019). Right-wing extremists' persistent online presence: History and contemporary trends. International Centre for Counter-Terrorism - ICCT. Policy Brief. https://www.icct.nl/sites/default/files/import/publication/Right-Wing-Extremists-Persistent-Online-Presence.pdf

Cross, M. (2023). Counter-terrorism & the intelligence network in Europe. International Journal of Law Crime and Justice. 72, 1-9. https://doi.org/10.1016/j.ijlcj.2019.100368

Elumalai, N. (2023, June 16).Malaysia: An inclusive policy measure is needed to end hate speech and discrimination. Article 19. https://www.article19.org/resources/malaysia-inclusive-policy-measure-needed-to-end-hate-speech/

Hadley, A., Khan, S., Ruiz, D., Sestito, M. & Wilson, K. (2016, June 30). Private sector engagement in responding to the use of the internet and ICT for terrorist purposes: Strengthening dialogue and building trust. ICT4Peace & UNCTED. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/private-sector-engagement-in-responding-to-the-use-of-the-internet-and-ict-for-terrorist-purposes.pdf

Law, N., Woo, D., de la Torre, J. & Wong, G. (2018). A global framework of reference on digital literacy skills for indicator 4.4.2. UNESCO Institute for Statistics. http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf

Rosand, E. & Winterbotham, E. (2019, March 20). Do counter-narratives actually reduce violent extremism?. Brookings. https://www.brookings.edu/articles/do-counter-narratives-actually-reduce-violent-extremism/

Shamsuddin, A. (2022). National Action Plan on Preventing and Countering Violent Extremism (NAPPCVE): A brief report of the Malaysian CSO recommendations. https://initiate.my/wp-content/uploads/2022/02/NAPPCVE-CSO-Report.pdf

Shamsuddin, A. (2022). National Action Plan on Preventing and Countering Violent Extremism: Civil society deserves a seat at the table. INITIATE.MY. Policy Brief. https://initiate.my/download/policy-brief-issue-1-2022/#

The Soufan Center (2021, June 3). Terrorism and counterterrorism in Southeast Asia: Emerging trends and dynamics. https://thesoufancenter.org/wp-content/uploads/2021/06/TSC-Report_Terrorism-and-Counterterrorism-in-Southeast-Asia_June-2021.pdf

The Star (2023, June 13). Zambry suggests digital resilience initiative to prevent, counter violent extremism. The Star. https://www.thestar.com.my/news/nation/2023/06/13/zambry-suggests-digital-resilience-initiative-to-prevent-counter-violent-extremism

UNICRI & UNCCT (2021). Countering terrorism online with artificial intelligence: An overview for law enforcement and counter-terrorism agencies in South Asia and South-East Asia. https://unicri.it/sites/default/files/2021-06/Countering%20Terrorism%20Online%20with%20AI%20-%20UNCCT-UNICRI%20Report.pdf

World Economic Forum (2023, June 20). Global gender gap report 2023. https://www3.weforum.org/docs/WEF_GGGR_2023.pdf?_gl=1*7yjtrw*_up*MQ..&gclid=Cj0KCQjwgNanBhDUARIsAAeIcAt3SQHmLj2MumpIG1ywDtccuriT8h6ohC9LlNI48-l75uKtyJOKWiAaAln9EALw_wcB

DIGITAL DANGERS: EXTREMISM RISKS IN ONLINE GAMING ENVIRONMENTS

Kennimrod Sariburaja

ABSTRACT

The emergence of online gaming platforms as a cornerstone of digital entertainment has attracted millions of gamers worldwide. Beyond conventional cyberthreats, their extensive popularity among youth has raised concerns about potential risks. This paper looks into the susceptibility of online gaming environments to extremist influences and analyses how these platforms may serve as potential hubs for radicalisation. Overall, the gamification and immersive nature of online games, along with a sense of belonging and anonymity, make them fertile grounds for the propagation of extremist ideologies. Some extremists use in-game messaging functions, thematic content, and specialised gaming communities to spread divisive narratives, recruit new members, and even coordinate offline activities. To resolve these challenges, the paper provides enforcement agencies, gaming companies, and the general public with recommendations to ensure that online gaming remains a safe and welcoming environment for all players.

Keywords: Online gaming, extremism, gamification, communal, anonymity, enforcement, empowerment, public education

THE LINK BETWEEN GAMING AND EXTREMISM

The popularity of online gaming platforms has surged in recent decades. These platforms, which boast a substantial global user base, offer individuals an opportunity to actively participate, entertain themselves, and cultivate social connections. Nevertheless, the increasing popularity of these platforms has raised concern regarding their potential misuse, particularly as recruitment sites for extremists. This essay aims to examine the degree to which online gaming platforms serve as a conducive environment for extremist ideas to target young individuals, as well as provide some recommendations.

There has been a growing trend among extremist groups to use online gaming platforms as a means to radicalise and enlist vulnerable young people. Online games, particularly those with multiplayer functionality, facilitate the convergence of individuals from all origins and cultures. Digital platforms such as Discord, Xbox Live, and PlayStation Network offer many communication features, including chat rooms, audio channels, and private messaging, which might potentially be misused for malicious intents (Myers and Browning, 2023). The susceptibility of gamers, particularly among younger individuals, can be attributed to factors such as age, impressionability, and the need for social inclusion (Surette, 2014).

The exploitation of gaming and game-related content by extremist groups is a well-established occurrence. There has been a notable rise in the development of video games by extremist and terrorist groups, which are specifically designed to propagate their ideological beliefs. During the early 2000s, the Hezbollah developed a video game called "Special Force," in which players assumed the role of a Hezbollah warrior engaged in conflict against the Israel Defence Forces (IDF) (Thomson, 2008). In 2003, Al-Qaida made alterations to a video game known as "Quest for Saddam," transforming it into their own version named "Quest of Bush" (Ambareesh and Kuniyillam, 2023). This modified version of the game saw players being instructed to eliminate virtual soldiers who looked like the then President of the United States, George W. Bush (Ambareesh and Kuniyillam, 2023).

Subsequently, following their declaration of a caliphate in Iraq and Syria in 2014, Daesh has since produced multiple video games. The organisation unveiled a proprietary video game called "Salil al-Sawarem" (The Clanging of the Swords), drawing inspiration from the widely acclaimed American video game "Grand Theft Auto" (Al-Rawi, 2016). In 2016, Daesh launched the *Huroof* application, designed to facilitate the learning of the Arabic alphabet among children, which included jihadist-themed songs and cartoons using weaponry (Criezis, 2022). The publication of Heimat Defender: Rebellion in 2020 by the Identitarian Movement from Germany serves as an example of how the aforementioned pattern continues to be present among right-wing extremist groups (Schlegel 2020). A contemporary illustration of this phenomenon may be observed inside the online gaming platform Roblox, where certain gamers with extremist inclinations have established virtual recreations of the Nazi Third Reich (Australian, 2022).

Extremist groups have effectively exploited gaming platforms as a means to engage a broader demographic, particularly the younger population. These groups use such platforms to persuade young people to imitate the game and take up arms, as many youngsters, particularly boys, are drawn to shooting and action-oriented video games. The Federal Bureau of Investigation (FBI) issued a warning in 2019 regarding the possibility of violent extremist organisations, such as Daesh or its associated groups, utilising online platforms as avenues for recruiting individuals (FBI, 2019). In a similar vein, it has been observed that right-wing extremist organisations employ online gaming platforms as a means to disseminate their beliefs and identify potential recruits (UN CTED, 2020).

GAMING SITES AS HIDDEN ARENAS FOR EXTREMIST RECRUITMENT

In a broader sense, gaming systems do not inherently present a significant level of danger. Although some studies suggest that gaming could potentially be a platform for the expression of aggression, it is important to note that there is currently no definitive evidence establishing a causal link between video games and incidences of physical violence. However, certain characteristics of these platforms possess the capacity to facilitate the process of radicalisation. The intersection of gaming and popular culture has become a prominent subject of discourse, with increasing attention being paid to the involvement of online gaming in the propagation of propaganda and the facilitation of radicalisation.

As such, there has been a growing concern regarding the use of online gaming as a potential platform for extremist recruitment. This digital medium has been observed to facilitate the identification of potential recruits, the establishment of initial contact, the cultivation of rapport, and subsequent indoctrination processes. In the Southeast Asian region, a pair of young individuals from Singapore, aged 15 and 16, underwent a process of self-radicalisation facilitated by online gaming platforms (Lim, 2023). The aforementioned transformation occurred due to their engagement with the online gaming platform Roblox and the instant messaging social channel Discord, both of which enjoy extensive usage within the gaming community (Iau, 2023). Additionally, they engaged in active participation in discussions pertaining to the struggles of Daesh and were recruited by an 18-year-old Muhammad Irfan Danyal Mohamad Nor (Iau, 2023). In fact, one of the youths contemplated engaging in knife assaults with the intention of beheading non-Muslims in well-frequented tourist areas in the country (Lim, 2023).

While in Australia, the Australian Federal Police (AFP) has observed a concerning pattern in which extremist groups are actively seeking to radicalise and enlist youth by utilising online gaming platforms. In 2022, the AFP discovered a young individual who allegedly shared extremist content portraying a replay of the 2019 Christchurch attack from a widely played online game on social media platforms (AFP, 2022).

In other cases, gaming platforms serve as not only a means of recruiting, but also as a virtual training ground for extremists. For example, Andres Behring Breivik, the perpetrator responsible for the tragic loss of 77 lives in Norway in 2011, recounted during his trial the manner in which he purportedly prepared for the assaults through engagement with the computer game Call of Duty: Modern Warfare (Eiser, 2021). He confirmed that he used a "holographic aiming device" for the purpose of honing his shooting skills within a war simulation game, which he said is used for training by armies around the world (Pidd, 2020).

HOW DOES IT APPEAL TO THE YOUTH?

The integration of game elements into non-gaming contexts, known as gamification, has garnered significant acclaim due to its capacity to motivate, engage, and instruct. This technology is utilised in multiple areas, ranging from education to marketing. Nevertheless, a concerning pattern emerges when examining the intersection of gamification and violent extremism. Multiple instances of intersectionality have been seen, encompassing a diverse range of groups, movements, and ideologies. These include jihadists, right-wing violent extremists, and ethnonationalist factions (Lakhani, 2021). The use of imaginary and cultural aspects such as memes derived from the well-recognised video game series Call of Duty can be seen in the propaganda disseminated by Daesh (Dauber et al., 2019).

The Christchurch attack that occurred in 2019 is one of the more commonly referred-to examples of the gamification of violent extremism. The incident exhibited several notable manifestations of gamification (Schlegel, 2021). For example, the use of a GoPro camera elicited a sensation akin to that of a first-person shooter (FPS), a prevalent genre in gaming wherein the player immerses themselves in the game through the perspective of the character, as shown by well-known game franchises such as Call of Duty or Halo (Andrews, 2023).

The Halle 2019 attack serves as a further example of "gamified" attacks. The individual identified as Stephan Balliet employed a smartphone affixed to a helmet for FPS purposes (Ebner, 2020). He then published a link to the Twitch livestream on the social media platform Meguca, where he uploaded his manifesto. The video was located and removed by the site administrators within a span of 30 minutes (Wong, 2019). At that point, the viewership of the content had reached an estimated count of 2,200 individuals (Wong, 2019).

In a similar vein, Daesh has devised and circulated a mobile application with the objective of propagating its ideology to children by incorporating seemingly innocuous gaming elements. In 2021, a recently established media station known as al-Mahdi Media, linked with the extremist group Daesh, released a propaganda movie characterised by its animated visuals and high-definition quality (Schlegel, 2021). The video had jihadi-themed music serving as the background score and portrayed a guerrilla-style ambush executed by Daesh fighters against a platoon of United States Army personnel. The visual content had striking similarities to gameplay sequences included in two widely recognised video games, Grand Theft Auto (GTA) and Call of Duty (Dauber et al., n.d.).

Gamification's appeal lies in its ability to tap into human psychology, offering rewards, competition, and progression. Extremist groups acknowledge these components as effective instruments for recruiting. Young individuals, in particular, may first be attracted to the excitement of the 'game,' but they can swiftly become entangled in a network of extremist views (Berger and Morgan, 2015). In addition to this, these groups frequently construct narratives that revolve around themes of heroism, resistance, or reclamation. Coupled with gamified components, these tales provide an engaging encounter in which recruits assume real-life roles like those of game characters, hence intensifying the convergence of ideology and gameplay (Conway et al., 2017).

Furthermore, online gaming platforms possess the capacity to foster a sense of communal belonging among socially isolated youth who mostly partake in solitary activities. The allure of these platforms for terrorist and violent extremist groups and individuals can be attributed to characteristics such as the presence of privacy and anonymity capabilities, secure connections in most situations, and the availability of encryption.

Frequently, those who engage in gaming activities assume the use of avatars and pseudonyms, affording themselves, as well as others who interact with them, a certain level of anonymity. The online gaming industry provides a unique environment where individuals can engage in remote and anonymous communication. The primary purpose of online gaming is to foster a sense of camaraderie among individuals and teams, often characterised by the concealment of their genuine identities. According to Foxman and Wolf (2013), the use of anonymity provides a protective barrier for recruiters, enabling them to discuss difficult subjects or radical views without facing immediate criticism or public scrutiny. Video game platforms inherently possess a lower degree of suspicion compared to other types of communication, hence enabling the gradual socialisation of propaganda among gamers without raising significant concerns. Therefore, the provision of anonymity allows prospective members the opportunity to delve into radical ideologies without facing tangible consequences in the physical realm. The absence of accountability also often resulted in a heightened level of receptiveness among the audience, creating an environment conducive for extreme narratives to gain traction (Conway et al., 2017).

Moreover, these platforms provide the capability to foster a sense of communal belonging among young people who frequently experience social isolation and exhibit a preference for solitary activities. Oftentimes, these individuals replace engagement in their immediate communities with social interaction on the gaming platform. As extremists establish relationships with online recruits, they can gradually introduce progressively radical ideologies to assess and appraise their potential adherents. In the absence of external intervention, those who are alone and susceptible to radicalisation tend to affirm the extremist narratives they encounter since they have fewer opportunities to challenge the rhetoric they hear or read. This isolation contributes to the gradual normalisation of extremist ideology and hate speech on gaming platforms.

According to a study conducted by the Anti-Defamation League (ADL) in 2021, it was discovered that approximately 10% of gamers aged 13 to 17 in the United States had encountered white supremacist ideology and themes while participating in online multiplayer games (Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021, ADL, 2023).

According to the survey, it was indicated that a rough estimate of 2.3 million teens encountered white supremacist ideology within online gaming platforms such as Roblox, World of Warcraft, Fortnite, Apex Legends, League of Legends, Madden NFL, Overwatch, and Call of Duty (Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021, ADL, 2023). The findings of the report indicate that extremist groups have directed their efforts towards various gaming platforms, leveraging the inherent sense of belonging and community that these platforms offer. They have achieved this by either establishing their own gaming communities or by infiltrating existing ones, thereby presenting their ideology as an alternative form of affiliation for gamers (Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021, ADL, 2023).

The nexus of gamification and violent extremism raises concerns, as online gaming platforms provide gamers with opportunities for adventure, social bonding, and escapism. This phenomenon represents a sophisticated evolution in recruitment strategies, wherein extremist groups exploit the human psyche's vulnerabilities.

CONCLUSION AND THE WAY FORWARD

While it is acknowledged that propaganda alone does not solely radicalise individuals, it is important to recognise that extremist groups have effectively utilised new media platforms in creative and innovative manners. This utilisation has the potential to attract disenfranchised young individuals, stimulate and expedite their process of radicalisation, and convert their pre-existing sympathies into more extreme inclinations. In the contemporary era characterised by instances of lone-actor terrorism, the phenomenon of online radicalisation in gaming spaces emerges as a great concern, not only for security services but also for the general public.

Intelligence and counter-terrorism agencies must continue to monitor the digital footprint of extremist groups, especially in the gaming world. The act of removing and censoring content from online sites and gaming platforms may provide temporary results, although it presents persistent challenges and occasional ineffectiveness in the long run due to potential limitations in the capacity of security agencies to monitor online spaces. One potential suggestion would be for the security agencies empowers the gamers themselves, as they are in a much better position to identify and address extremism (Hartgers and Leidig, 2023). This can be achieved by leveraging in-game reporting mechanisms, enabling gamers to report instances of extremist behaviour inside gaming communities to relevant authorities.

An additional proposal involves addressing in-game radicalisation through the implementation of public education initiatives and raising awareness among parents regarding methods for detecting self-radicalisation in youth. This includes identifying indicators such as the withdrawal from regular social circles, the adoption of increasingly extremist ideologies and behaviours, and the manifestation of intense reactions towards specific news or political events by children or family members (Ali, 2023). The general public has a significant role to fulfil in terms of being educated and aware of the perils associated with extremist ideologies and abstaining from consuming or spreading extremist material, regardless of the platform.

Furthermore, gaming companies have a role in preventing and disrupting extremist use of their platforms and services. Nonetheless, the dynamic and instantaneous nature of video games presents a significant challenge in effectively monitoring and regulating instances of illicit or inappropriate conduct. Gaming companies have shown proactive efforts in addressing harmful content by implementing measures such as blocking extremist material and retaining audio recordings of in-game chats for potential future investigations (Myers and Browning, 2023). Given the vast global player base of three billion individuals, effectively monitoring real-time activities becomes an exceedingly challenging task. As such, the gaming industry, players, and general public must remain vigilant and aware of these covert tactics to ensure that these realms of escapism remain untainted by radical ideologies.

In conclusion, the significance of multi-stakeholder methods, which involve the involvement of law enforcement, the general public, the gaming industry, and gaming-adjacent platforms, cannot be overstated. An enhanced approach to mitigating and addressing extremism within the gaming sphere can be attained through the active engagement and empowerment of gamers, public education initiatives, and the collaboration of gaming corporations in the establishment and enforcement of community norms.

REFERENCES

AFP (2022). Extremist recruitment reaching young Australian gamers. Australian Federal Police. https://www.afp.gov.au/news-centre/media-release/extremist-recruitment-reaching-young-australian-gamers

Ali, N. H. M. (2023, February 21). Online gaming platforms easy ground for extremists to target youth, parents should be more vigilant: Experts. TODAY. https://www.todayonline.com/singapore/online-gaming-platforms-extremists-target-youth-parents-terrorism-2113431

Andrews, S. (2023). The ‘First Person Shooter’ perspective: a different view on first person shooters, gamification, and first person terrorist propaganda. Games and Culture, 155541202311537. https://doi.org/10.1177/15554120231153789

Australian, W. (2022, October 24). Roblox: Nazi Germany re-creation discovered in online gaming platform by young Jewish girl from Melbourne. The West Australian. https://thewest.com.au/technology/gaming/roblox-nazi-germany-re-creation-discovered-in-online-gaming-platform-by-young-jewish-girl-from-melbourne-c-8637499

Al-Rawi, A. (2016). Video games, terrorism, and ISIS’s Jihad 3.0. Terrorism and Political Violence, 30(4), 740–760. https://doi.org/10.1080/09546553.2016.1207633

AMBAREESH, S., & KUNIYILLAM, A. (2023, July 11). Countering terrorism in today’s world. Observer Research Foundation. https://www.orfonline.org/expert-speak/countering-terrorism-in-todays-world/

Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2018). Disrupting Daesh: Measuring takedown of online terrorist material and its impacts. Studies in Conflict & Terrorism, 42(1–2), 141–160. https://doi.org/10.1080/1057610x.2018.1513984

Criezis, M. (2022). Create, Connect, and Deceive: Islamic State Supporters’ Maintenance of the Virtual Caliphate Through Adaptation and Innovation. THE GEORGE WASHINGTON UNIVERSITY. https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Criezis_CreateConnectDeceive_09222022_0.pdf

Dauber, C. E., Robinson, M. D., Baslious, J. J., & Blair, A. G. (2019). Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. Perspectives on Terrorism, 13(3), 17–31. https://www.jstor.org/stable/26681906

Ebner, J. (2020, February 14). Dark ops: Isis, the far-right and the gamification of terror. Financial Times. https://www.ft.com/content/bf7b158e-4cc0-11ea-95a0-43d18ec715f5

Eiser, A. R. (2021). Preserving brain health in a toxic age: New Insights from Neuroscience, Integrative Medicine, and Public Health. Rowman & Littlefield.

Foxman, A. H., & Wolf, C. (2013). Viral hate: Containing Its Spread on the Internet. St. Martin's Press.

Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021, ADL. (2023). Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021 | ADL. ADL. https://www.adl.org/resources/report/hate-no-game-harassment-and-positive-social-experiences-online-games-2021

Iau, J. (2023, February 22). 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

Lakhani, S. (2021). Video gaming and (violent) extremism: an exploration of the current landscape, trends and threats. European Commission. https://home-affairs.ec.europa.eu/system/files/202202/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

Lim, K. (2023, February 21). Singapore warns of radicalisation via gaming as 2 teens issued orders under ISA law. South China Morning Post. https://www.scmp.com/week-asia/article/3210987/singapore-warns-radicalisation-gaming-2-teens-hit-controversial-isa-law

Myers, S. L., & Browning, K. (2023, May 18). Extremism finds fertile ground in chat rooms for gamers. The New York Times. https://www.nytimes.com/2023/05/18/technology/video-games-extremism.html

Pidd, H. (2020, April 16). Anders Breivik "trained" for shooting attacks by playing Call of Duty. The Guardian. https://www.theguardian.com/world/2012/apr/19/anders-breivik-call-of-duty

Schlegel, L. (2020, September 17). No Child's Play: The Identitarian Movement's 'Patriotic' video game. GNET. https://gnet-research.org/2020/09/17/no-childs-play-the-identitarian-movements-patriotic-video-game/

Schlegel, L. (2021). Connecting, Competing, and Trolling: "User Types" in Digital Gamified Radicalization Processes. Perspectives on Terrorism, 15(4), 54–64. https://www.jstor.org/stable/27044235

Schlegel, L. (2021). Extremists' use of gaming (adjacent) platforms Insights regarding primary and secondary prevention measures. European Commission. https://home-affairs.ec.europa.eu/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf

Surette, R. (2014). Performance Crime and Justice. Current Issues in Criminal Justice, 26(1), 65-81.

The Federal Bureau of Investigations (FBI). (2019). The challenge of online radicalization. Retrieved from Federal Bureau of Investigation website.

Thomson, M. (2008). Military Computer Games and the New American Militarism [PhD Dissertation]. University of Nottingham.

United Nations Counter-Terrorism Committee Executive Directorate (CTED). (2020). The use of the internet for terrorist purposes. Retrieved from the United Nations website.

Wong, J. C. (2019, October 17). Germany shooting suspect livestreamed attempted attack on synagogue. The Guardian. https://www.theguardian.com/world/2019/oct/09/germany-shooting-synagogue-halle-livestreamed

TECH TERROR: GLOBAL NETWORKS TO GLOBALISATION OF TERRORISM IN THE DIGITAL SPACE

Mohd Mizan Mohammad Aslam
Sinduja Umandi Wickramasinghe Jayaratne

ABSTRACT

In an interview to Press Trust of India (PTI) on 3rd September 2023, Prime Minister Narendra Modi emphasised the social fabric of nations may be affected by terrorists exploiting the dark web, the metaverse, and cryptocurrencies to further their evil intentions. During his interview he urged the need of global cooperation and governance to counter such threats. This showcases the influence of rapidly expanding technology on changing dynamics of terrorism not only in India, but also around the world. The Prime Minister Modi's call for global cooperation to counter such threats, emphasise that states alone cannot face such challenges due to the nature of global connectivity of terror activities in the digital space. Therefore, this research is conducted to identify the changing dynamics of terrorism from global networks to globalisation of terrorism in the digital space. It is also intended to elaborate the challengers and limitations in global cooperation and governance to counter prevent such threats, and how to improve the cooperation and governance among nations to face such challenges. This research is conducted using primary and secondary data collected from case studies, journal articles, interviews, statements, and websites.

Keywords: terrorist networks and organisations, digital space, global cooperation and governance

INTRODUCTION

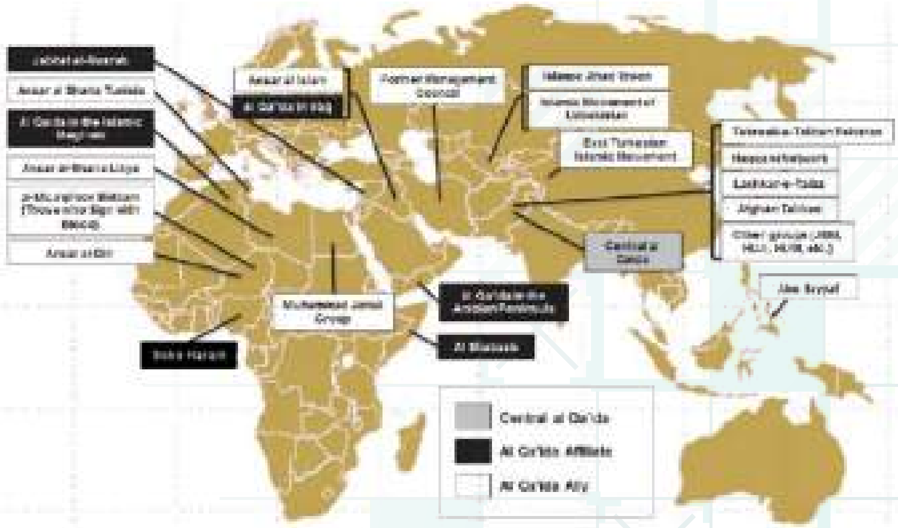
The actions of terrorists have advanced from ground to the digital space which is described as what appears on the screen of a digital device, such as websites, apps, social media, movies and other media (Cesare et al., 2016). This further complicates the definition of terrorism since the action of violence can be a sub result of the use of the digital space by the terrorists, leading the individual to commit a terror attack. The use of the digital space by terrorists has become a significant concern for governments, law enforcement agencies, and technology companies worldwide. On 31st October 2017, a permanent US resident from Uzbekistan called Sayfullo Saipov, drove a rented truck over the civilians in a bike lane in Manhattan, USA. Islamic state of Iraq and Syria (ISIS), claimed the attack, but the authorities failed to establish a direct link between ISIS and Saipov. Instead, they found out more 90 videos related to ISIS and nearly 4000 images in at least two of his cell phones (Semati and Szpunar, 2018). It has also been revealed that Saipov was explicitly motivated by the 3rd issue of 'Rumiyah', which is an online magazine of ISIS. This showcases that, it is not necessary for an individual to physically become a part of a terror organization to commit terror activities. Instead, the like-minded individuals are now been motivated by the online propaganda of terror outfits such as ISIS to commit the attacks from the host countries, without physically being engaged with the organisation. It is now been experienced that, individuals exploit digital platforms and technologies for various purposes of terrorism, including communication, recruitment, fundraising, propaganda dissemination, and also for planning attacks.

Therefore, this research is conducted to understand how the dynamics of terrorism have changed from global networks to globalisation of terrorism, especially analysing how the digital space is used by terrorists for propagation and financial activities. Besides, this research also elaborates on challenges in global cooperation and governance to counter/prevent such threats. Finally, this research recommends how to minimise the gaps in global cooperation and governance to counter/prevent the use of digital space by the terrorists.

GLOBAL TERROR NETWORKS TO GLOBALISATION OF TERRORISM

Global terror networks are made up of interrelated and frequently loosely affiliated groups, people, and organisations who adhere to extreme ideologies and commit acts of terrorism or other forms of violence on a global scale. These networks transcend national borders and collaborate across regions, making them challenging for governments and law enforcement agencies to counter effectively (Boer and Monar, 2002). Global terror networks are typically united by a common extremist ideology, such as radical interpretations of Islam such as Al Qaeda and ISIS or white supreme and neo-Nazism. These ideologies often provide a framework for justifying violence against perceived enemies. United Nations Special Rapporteur Tendayi Achiume has stated that, Jews and many other racial, ethnic, and religious groups are hated to the core by neo-Nazis individuals (United Nations Office for the Coordination of Humanitarian Affairs, 2018). These ideas also threaten women, people with disabilities, lesbians, gay men, bisexuals, transgender individuals, and intersex people. This was evident when Robert D. Bowers, an individual with anti-sematic ideologies, killed 11 people in Pittsburgh in USA on 27th October 2018 (Robertson et al., 2018).

Global terror networks operate across multiple countries and regions, allowing them to recruit, plan, and execute attacks on an international scale. They may have cells or affiliates in various countries, making it easier to carry out attacks and evade law enforcement. Following diagram depicts the affiliates and allies of Al- Qaeda (AQ) around the world.



Map 1.1 – Affiliates and Allies of Al Qaeda (Ligon et al., 2014)

Global terror networks such as ISIS use modern communication technologies to coordinate activities and share information among their members and sympathisers. This includes encrypted messaging apps, social media platforms, and the dark web. During its prime years, ISIS developed its own chat app called 'Alrawi'(Constine, 2016). The motivation to develop such chat app was due to the insecurity of information protection in common chat apps such as WhatsApp. Apart from that global terror networks such as ISIS often recommends its members and supporters to utilise VeraCrypt and TrueCrypt for encrypting files (Regional Cooperation Council, 2018).

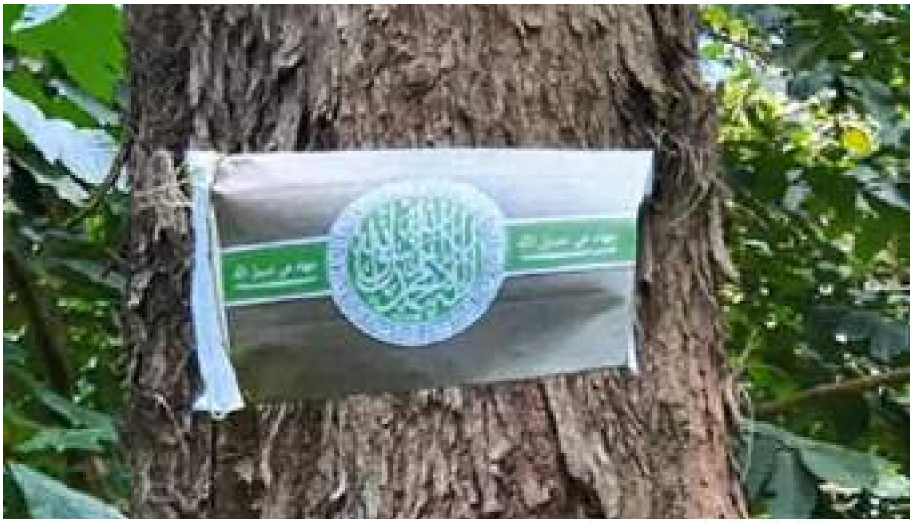
However, current trends of terrorism go beyond global terror networks to globalisation of terrorism. Academics in social sciences often define the term 'globalisation' as, all the methods used to unite the world's population into a one global society (Albrow and King, 1990). One such method of connecting the world together is the advancement of technology and the expansion of the digital space. It has not only brought different societies together, but also it has made different types of terrorists and like-minded individuals to utilise one another's tactics and methods in financing, propagation, planning, communication and others for their own advantage.

Hamas military wing known as Izz el-Deen al-Qassam Brigades was one of the initial terror organisations to utilise cryptocyrrency such as Bitcoin for their fund raising activities. The organisation recently denounced receiving funds through its cryptocurrency wallets due to security reasons (Al-Mughrabi, 2023). However, following the footsteps of Izz el-Deen al-Qassam Brigades, ISIS and AQ have opened up its fund-raising campaigns through crypto wallets (Dion-Schwarz et al., 2019).

A cryptocurrency motoring organisation called the TRM Labs has recently released a report which stated that, "pro-ISIS networks in Tajikistan, Indonesia, Pakistan and Afghanistan have used cryptocurrencies to help conduct their activities" (TRM Labs, 2023). The report further mentioned that over USD 517,000 was sent to ISIS in 2022 by the pro-ISIS supporters in Indonesia through cryptocurrency. This showcases utility of digital space for fund raising activities by terrorists.

The abuse of the digital space by members of terror organisations for illicit activities, such as fundraising, drug trafficking, or extortion, to finance their operations, is not a new phenomenon in terrorism. However, globalisation of terrorism is such that terror activities being replicated or imitated by criminal outfits due to its effectiveness. Due to freely available videos in the digital space by terror organisations such as ISIS, drug cartels in Mexico are currently utilising 'beheading' as a tactic to terrorise the population and the rivalries (Mcnulty, 2023).

The inspiration which is provided by different type of terror groups through propagation of their tactics and the ideology in the digital space have intensified the activities of lone actors without any physical affiliation to any of the global terror networks. The current trends depict that young individuals are motivated simultaneously by both ISIS and AQ ideology which is propagated and freely available in online platforms. Muhammad Irfan Danyal Mohamad Nor (18 years old) was arrested and detained under the Internal Security Act (ISA) in December 2022 (South China Morning Post, 2023). The individual was self-radicalised by ISIS online propaganda and has planned three attacks in Singapore. However, the young individual has also created his own flag which resembles the flag of Hayat Tahirir al-Sham, which was previously known as the AQ Syrian Affiliate.



Picture 1.2 - The flag which was made by Muhammad Irfan Danyal Mohamad Nor (South China Morning Post, 2023)

This incident highlights the following concerns in current trends of terrorism:

1. The online magazines of ISIS such as Voice of Khorasan, Al Naba and Wolves of Manhattan by AQ cater to the like-minded individuals who are in the edge of becoming radicalised.

2. Due to the continuous propagation in the digital space, these individuals are exposed to radicalisation through online indoctrination and ultimately end up in performing a terror attack.

3. However, the globalisation of terrorism is such that, these individuals are not physically or financially engaged with the core-organisation. In fact, it is been portrayed the merger between ideologies of ISIS and AQ making it complicated for the law enforcement authorities to understand the radicalisation process and the motivation of the individual.

4. However, the ultimate goal of the kind of individuals is to perform an attack in the host countries due to the inspiration provided by the propagation in the digital space making the individual a lone actor.

CHALLENGERS AND LIMITATIONS IN GLOBAL COOPERATION AND GOVERNANCE

Terrorism is often visualised as a concept without a universally agreed definition (Hoffman, 2006). It is always been highlighted as a subjective term because "one man's terrorist is another man's freedom fighter" (Beydoun, 2022). Therefore, the term 'terrorism' has been defined by multiple sources with similar meaning. For an example, during the launch of the Global Strategy against Terrorism on 10th March 2005, United Nations Organisation (UNO) described terrorism as an act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organisation to do or abstain from doing any act" (United Nations, 2005). On the other hand academics such as Louise Richardson, who was a former Vice-Chancellor in Oxford University, considers that terrorists intentionally utilise violence against civilians to archive political purposes (Ward, 2018). After close reflection on both the definitions, one can argue that terrorism often entangle and implement violence on civilians as a mechanism to achieve their political goals by intimidating the governing authorities.

Osama Bin Laden, the leader of Al Qaeda (AQ), declared war against the United States of America (USA), especially stating to chase away the USA soldiers from Saudi Arabia (U.S. Department of State, 2001). This was one of the prime goals of AQ during the establishment of the organisation (Senate Hearing 107-390, 2001). Therefore, the goals of AQ are certainly political in nature since it is focusing on establishing an Islamic state while cleansing the infidels from the holy land (Sedgwick, 2004; The Federal Bureau of Investigation (FBI), 2001). However, the ultimate goals of AQ are defined religiously while complicating the situation to make a demarcation whether the organisation has political or religious objectives to achieve. This also complicates the categorisation of the organisation as a terror outfit, especially considering the objectives of the organisation, since terrorism is defined as implementation of violence against civilians to achieve a political goal. Nevertheless, countries such as United States, United Kingdom, Israel, India, Pakistan, Saudi Arabia, Japan, Malaysia along with many other countries have designated AQ as a terror organisation, especially after the 9/11 attack in USA. On the other hand, countries such as Somalia, Afghanistan, Sudan, Yemen are still in the line to designate AQ as a terror organisation, reminding that "one man's terrorist is another man's freedom fighter" (Beydoun, 2022). This showcases the complexity of categorisation of terror organisations such as AQ since there is no common definition agreed by the international community to define the term due to its subjective nature. This ambiguity can hinder efforts to coordinate global counterterrorism actions especially in the digital space.

The principle of state sovereignty often hinders international efforts to combat terrorism. States may be unwilling to cooperate fully if they perceive it as an infringement on their autonomy. This can lead to diplomatic tensions and hinder international cooperation. On the other hand, intelligence sharing on terrorist threats across borders can be challenging due to apprehensions about securing sources and methods of intelligence collection. Even when it could help prevent terrorist attacks, countries may be reluctant to share critical information with other nations due to lack of trust and due to security dilemmas in the in the international system.

Many nations, particularly those in developing regions, lack the capacity and resources which are vital to effectively tackling terrorism. Expansion of terrorism in the African region is a critical example of lack of dedicated resources for the implementation of counter-terrorism strategies in the region (Akanji, 2019). This may result in gaps in international counterterrorism initiatives, allowing terrorist groups to flourish in regions with inadequate governmental control. Countries such as Afghanistan, Mali, and Burkina Faso are couple of examples which have become breading grounds of terrorism due to lack of governmental authority.

On the other hand, emergence and expansion of new technologies such as the 'metaverse' will be a unique challenge to the international community. UNO anticipate terror outfits utilising digital platforms such as the 'metaverse' for recruitment, radicalisation of like-minded individuals, fundraising activities, communication, planning of attacks and for the implementation of propaganda activities (United Nations Office of Counter-Terrorism, 2022). As the 'metaverse' continues to develop, governments, law enforcement agencies, tech companies, and international organisations need to closely monitor and address potential security threats and vulnerabilities. Balancing the open and innovative nature of the 'metaverse' with the need for security and counterterrorism measures will be an ongoing challenge for the law enforcement authorities and the tech companies. Therefore, it is essential to adapt strategies and regulations to mitigate potential risks as the technology evolves. International law and treaties related to terrorism may not be comprehensive or up-to-date enough to address emerging threats adequately. Updating and strengthening these legal frameworks is an ongoing challenge due to the evolving nature of the digital space.

RECOMMENDATIONS TO OVERCOME THE LIMITATIONS

In order to overcome the limitations of countering/preventing the use of digital space by the terrorists, countries need to strengthen international cooperation and diplomacy. Information and intelligence concerning terrorist threats, funding, and operations can be shared across nations. This can aid in the detection and destruction of terrorist networks, the advertence of terrorist attacks, and the capture of terrorist suspects. Since the digital space does not possess any boundaries, terrorist activities in the digital space also become borderless. Therefore, countries need to adapt to this situation which calls for multinational task forces to target and dismantle terrorist organisations operating across borders. One such example is the establishment of the Global Coalition to Defeat ISIS which encompasses eighty six countries (US Department of States, n.d.)

Coordination of counterterrorism operations among member states is greatly aided by international organisations like the United Nations, Interpol, and regional organisations like the European Union. They have the ability to promote exchange of knowledge, capacity development, and the creation of global counterterrorism policies.The international community must also commit to resolving the underlying factors that contribute to terrorism, such as political unrest, economic disparity, and ideological extremism. Furthermore, improving international terrorist governance and lessening its effects globally depend on fostering trust and consensus among governments.

To show their dedication to battling terrorism on a global scale, nations might ratify and abide by international counterterrorism conventions and treaties, such as the International Convention for the Suppression of Terrorist Bombings (1997), International Convention for the Suppression of the Financing of Terrorism (1999), and International Convention for the Suppression of Acts of Nuclear Terrorism (2005). At the same time, international community needs to cooperate and encourage countries to enact adequate laws to fight against the terrorism in the digital space. Furthermore, the fight against extremist and terrorist propaganda involves international cooperation. Nations can cooperate to create and spread counter-narratives in the digital space that oppose the ideas that support terrorism. However, trust, same objectives, and a dedication to maintaining the rule of law and human rights are key for effective international collaboration in the fight against terrorism in the digital space.

CONCLUSION

This research has elaborated on the evolution of terrorism from global terror networks to globalisation of terrorism through its activities in the digital space. This research further emphasise that terrorist utilise digital space for various reasons, especially for fundraising, propagation, planning terror activities, and communication. It is evident that terrorism in the digital space is becoming complex due to the consumption of online propaganda which belongs to multiple terror organisations or networks, by one single individual. At the same time, this research asserts that terror tactics of one organisation is now been imitated by different other organisations due to the effectiveness, making the tactics and strategies of terrorism globalised.Within such context, counterterrorism mechanisms and strategies lack in articulating a universally agreed definition for terrorism, which can be applicable in defining the terror activities in the digital space. Moreover, sovereignty and state autonomy, resource constraints, lack of Intelligence sharing and inadequacy in formulating International Legal Frameworks are highlighted as some of the gaps in global governance and cooperation in countering preventing digital terrorism. Finally, this research assert that, improvement of information sharing among states, establishment of Joint Operations and Task Forces, role of Multilateral Organisations and capacity building of developing states are vital to avoids the gaps in global governance and cooperation in countering/preventing digital terrorism.

REFERENCES

Akanji, O. O. (2019). Sub-regional Security Challenge: ECOWAS and the War on Terrorism in West Africa. Insight on Africa, 11(1), 94–112. https://doi.org/10.1177/0975087818805842

Al-Mughrabi, N. (2023). Hamas armed wing announces suspension of bitcoin fundraising. REUTERS. https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/

Albrow, M., & King, E. (Eds.). (1990). Globalization, Knowledge and Society. SAGE.

Beydoun, K. A. (2022). On Terrorists And Freedom Fighters. Harvard Law Review, 136(1), 1–36.

Boer, M. den, & Monar, J. (2002). Keynote Article: 11 September and the Challenge of Global Terrorism to the EU as a Security Actor. Journal of Common Market Studies, 40(s1), 11–28.

Cesare, D. M. Di, Harwood, D., & Rowsell, J. (2016). It Is Real Colouring?: Mapping Children's Im/Material Thinking in a Digital World. In Handbook of Research on the Societal Impact of Digital Media (p. 25). IGI Global.

Constine, J. (2016). ISIS Has Its Own Encrypted Chat App. Tech Crunch. https://techcrunch.com/2016/01/16/isis-app/

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist Use of Cryptocurrencies. RAND Corporation.

Hoffman, B. (2006). Inside Terrorism (2nd Edition). Columbia University Press.

Ligon, G. S., Harms, M., Crowe, J., & Lundmark, L. (2014). ISIL : Branding , Leadership Culture and Lethal Attraction The Islamic State of Iraq and the Levant : Branding, Leadership Culture and Lethal Attraction Report to the Office of University Programs, Department of Homeland Security (Issue January).

Mcnulty, T. (2023). ISIS-inspired video shows five drug cartel killers being beheaded in mass execution. Express. https://www.express.co.uk/news/world/1734657/ISIS-Mexico-drug-cartel-killers-beheaded

Regional Cooperation Council. (2018). Cyber Caliphate: What Apps Are the Islamic State Using? News. https://www.rcc.int/swp/news/38/cyber-caliphate-what-apps-are-the-islamic-state-using

Robertson, C., Mele, C., & Tavernise, S. (2018, October 27). 11 Killed in Synagogue Massacre; Suspect Charged With 29 Counts. The New York Times. https://www.nytimes.com/2018/10/27/us/active-shooter-pittsburgh-synagogue-shooting.html

Sedgwick, M. (2004). Al-qaeda and the nature of religious terrorism. Terrorism and Political Violence, 16(4), 795–814. https://doi.org/10.1080/09546550590906098

Semati, M., & Szpunar, P. M. (2018). ISIS beyond the spectacle: communication media, networked publics, terrorism. Critical Studies in Media Communication, 35(1), 1–7. https://www.tandfonline.com/doi/full/10.1080/15295036.2018.1414751?scroll=top&needAccess=true

Senate Hearing 107-390. (2001). The Global Reach Of Al-Qaeda. U.S. Government Publishing Office. https://www.govinfo.gov/content/pkg/CHRG-107shrg77601/html/CHRG-107shrg77601.htm

South China Morning Post. (2023). Singapore detains teenage Isis supporter for plotting three attacks. South China Morning Post. https://www.scmp.com/news/asia/southeast-asia/article/3208770/singapore-detains-teenage-isis-supporter-plotting-three-attacks

The Federal Bureau of Investigation (FBI). (2001). Testimony. The Federal Bureau of Investigation (FBI). https://archives.fbi.gov/archives/news/testimony/al-qaeda-international

TRM Labs. (2023). TRM Finds Mounting Evidence of Crypto Use by ISIS and its Supporters in Asia. TRM Labs. https://www.trmlabs.com/post/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia

U.S. Department of State. (2001). The Charges against International Terrorist Usama Bin Laden. U.S. Department of State Archive. https://1997-2001.state.gov/www/regions/sa/bin_laden_charges.html#:~:text=August 1996 Declaration of War, of Jihad Against the Americans

United Nations. (2005). Secretary-General Kofi Annan Launches Global Strategy Against Terrorism in Madrid. United Nations Press Release. https://press.un.org/en/2005/sg2095.doc.htm

United Nations Office for the Coordination of Humanitarian Affairs. (2018). Neo-Nazism and nationalist populism fuel hatred and intolerance, says UN expert. Press Release. https://www.ohchr.org/en/press-releases/2018/11/neo-nazism-and-nationalist-populism-fuel-hatred-and-intolerance-says-un

United Nations Office of Counter-Terrorism. (2022). Safeguarding the Metaverse: Countering Terrorism and Preventing Violent Extremism in Digital Space - Expert Panel. United Nations.

US Department of States. (n.d.). Members – The Global Coalition To Defeat ISIS. US Department of States. Retrieved October 6, 2023, from https://www.state.gov/the-global-coalition-to-defeat-isis-partners/

Ward, A. (2018). How Do You Define Terrorism? RAND Corperation. https://www.rand.org/blog/2018/06/how-do-you-define-terrorism.html

MALICIOUS USE OF ARTIFICIAL INTELLIGENCE BY TERRORISTS: ASSESSING FUTURE RISKS

Muhammad Afiq Ismaizam

ABSTRACT

Recent years have witnessed remarkable advancements in Artificial Intelligence (AI), including the proliferation of generative AI tools. While these technologies hold immense promise, they also present dual-use capabilities – the potential for both positive and malicious applications. This paper delves into the burgeoning concerns surrounding AI's exploitation by terrorists, underlining the urgency of addressing these emerging threats on a global scale. The discussion highlights the multifaceted ways in which terrorists can harness AI for malevolent purposes which encompass the dissemination of disinformation on social media, orchestrating cyberattacks, leveraging cryptocurrencies for illicit financing, deploying unmanned aerial systems (drones) in acts of terror, and disseminating personalized propaganda to recruit individuals. The paper also underscores the critical importance of proactive measures, such as intensified monitoring, robust cybersecurity protocols, and the establishment of ethical AI frameworks to mitigate these risks effectively. The need for international collaboration is emphasised, as terrorism transcends borders, necessitating a collective response to AI-related challenges. Moreover, interdisciplinary research is deemed essential to comprehending terrorists' AI strategies, tactics, and vulnerabilities fully.

Keywords: Artificial Intelligence, terrorists, drone, cryptocurrency, cyberattack, social media, policymakers, government

Major advances in Artificial Intelligence (AI) have been taking place in the past few years, with breakthroughs in AI-powered robotics and quantum computing. More recently, generative AI tools have entered the general consumer market. In fact, generative AI often headlines emerging technological trends with its ability to create new written, visual, and auditory content given prompts or existing data. However, new and innovative breakthroughs in AI could also usher in a new era of threats and risks that the international community may not be well prepared for.

AI, like any other tool used by humans, has dual-usage. This means that AI can either be used for a positive or a negative purpose, depending on the user or users. While AI technology can be beneficial, it may also bring detrimental harm to society if used maliciously. This is a largely an unexplored field of research, with a few documented cases. More specifically, terrorists are able to exploit these AI features and breakthroughs to either explore new ways to cause harm or enhance existing methods. As a result, this dual usage of AI brings about a level of uncertainty and risk that needs to be addressed urgently.

Equally important and concerning is the easy use and access of AI tools. This will force governments, policymakers, law enforcement agencies to prepare for possible terrorist attacks. The widespread global attention and concern towards AI has had governments and civil societies already deliberating its possible risks, especially the risk of it being misused by terrorists. In July 2023, United Nations (UN) Secretary General António Guterres convened the first-ever Security Council debate on AI at the UN headquarters in New York (Huaxia, 2023).

He commented on the harm that may be incurred should AI fall into the hands of terrorists, thus highlighting the global need to regulate AI.

As a response to the UN Secretary-General and the international community at-large, it is worth assessing possible usage of AI by terrorists. Maliciousness of AI can be categorically grouped into four five possible uses; (i) disinformation on social media, (ii) cyberattacks, (iii) terrorism financing, (iv) drone attacks, (v) personalised and targeted messages.

Since the late 1990s, the increase in global connectivity has allowed terrorists and violent extremist groups to be more sophisticated in their use of information and communications technologies. Nowadays, social media have been the go-to platforms for terrorists to radicalise and recruit supporters, spread propaganda as well as generate funds in support of their ideas and operations. According to the UN Security Council Counter-Terrorism Committee and ICT4Peace (United Nations, 2016);

"…Internet and social media, as well as by extension other ecosystems such as the online gaming platform, have become powerful tools for terrorist groups to radicalise, inspire, and incite violence; claim responsibility for attacks; recruit; raise and move funds; buy and transfer weapons; and make tutorials or instruments available to their members"

AI tools for audio and imagery are fast becoming available. As a result, this makes the spreading of disinformation with AI easy. In May 2023, a fake image was being circulated on social media which appeared to show an explosion had occurred at the Pentagon (Haddad, 2023). At first glance, the image does look convincing. However, upon confirmation with authorities, there was no such explosion. This fake image demonstrates the potential of generative AI to fool the general public, inciting a level of anxiety and chaos. AI tools such as Midjourney, Dall-e 2, and Stable Diffusion can create life-like images with minimal effort. With software improvements predicted to take place over time, the propensity for misuse then becomes high.

Cyberattacks are an all too familiar occurrence among the general population.According to IBM, cyberattack is defined as the effort to gain unauthorised access to a network, computer system or digital device with malicious intent. One of the most common cyberattacks is Denial-of-Service (DoS). A DoS temporarily disconnects any computer system from the internet. It has been recorded that the Islamic state launched its first-ever successful series of DoS attacks using a DoS tool named, "Caliphate Cannon". It targeted military, economic and education infrastructure (Haddad, 2023). Moreover, a famous cyberattack case was the "WannaCry" ransomware. In 2017, "WannaCry" affected more than 200,000 computers in across 150 countries (Reuters, 2017). Cybersecurity experts at Europol commented that the ransomware was used in combination with "a worm functionality" so that the infection spread automatically (Reuters, 2017). The "Caliphate Cannon" and "WannaCry" show that cyberattacks can inflict significant damage, and will be made worse as AI continues to progress. This is because Generative AI tools are now being used for phishing emails, keystroke monitoring malware and basic ransomware code (Mascellino, 2023). As cyberattacks become more targeted and sophisticated, it is expected that terrorists will take advantage of them to inflict greater damage onto public infrastructure.

The growing market of cryptocurrencies such as Bitcoin have provided a level of anonymity and decentralisation that can be exploited by criminals and terrorists. Although the systematic usage of cryptocurrencies by terrorist groups and individuals has not been seen (Dion-Schwartz et al., 2020), there is one documented case. Investigators in the 2019 Sri Lankan bombings had observed an increased a number of transactions in Bitcoin wallets used by Islamic state to raise funds prior to the bombing (Katsiri, 2019), which led to the suspicion that Bitcoins were transacted prior to the bombings. Moreover, ISIS has been reported to use cryptocurrencies to raise funds and move money across borders. They have used platforms like Telegram to solicit donations in cryptocurrencies. Finance and terrorism are inextricably linked, and there is reason to suspect that illicit finances via cryptocurrencies are increasingly directed towards more fundraising of terrorist activities. Moreover, terrorists can use AI-driven algorithms to navigate the dark web and access underground marketplaces where cryptocurrencies are commonly used for illegal transactions. They have the capacity to acquire weaponry, explosives, forged documents, and various unlawful commodities and services. Additionally, terrorists might utilise AI to obscure the trail of fund origins, rendering it difficult to trace illicit cryptocurrency transactions back to their source.

Uncrewed Aerial Systems (UAS) have been identified as one of the key terrorist threats by the United Nations (UN) Security Council Counter-Terrorism Committee. UAS are remotely piloted, pre-programmed, or controlled airborne vehicles. They are also referred to as Unmanned Aerial Vehicles (UAVs), or more commonly drones. There have been reports of drone attacks by terrorist groups which have either caused death, physical harm or infrastructural damage. Such drones have the ability to carry explosive payloads. In one incident, it was reported that Islamic state had deployed a UAS loaded with explosives in attacks in northern Iraq that killed two Kurdish Peshmerga fighters and wounding two operatives from the French Special Operations (Gibbons-Neff, 2016). With its commercial availability, affordability, and wide usage, it is no surprise that drones have been an easy option for terrorists deploy. It is worth noting that since 2020, energy infrastructure, international shipping, international airports, and capital cities have all been targeted by drones (Rogers, 2021).

AI-driven natural language generation (NLG) algorithms possess the capability to craft persuasive text-based content, spanning articles, narratives, and messages that resonate deeply with specific individuals. These tools enable terrorists to customise their textual narratives, strategically catering to the unique interests and convictions of their target audience.Moreover, AI can scrutinise publicly accessible data concerning individuals, encompassing their interests, affiliations, and online conduct. Armed with this information, terrorists can formulate highly personalised recruitment tactics, tailoring their messaging to align seamlessly with the pre-existing beliefs and grievances of the individual. Furthermore, AI chatbots and virtual assistants operate adeptly on social media platforms, actively engaging with users by responding to their comments and messages. These sophisticated bots skilfully mimic human interactions, progressively indoctrinating users with extremist ideologies.

With the profound risks that AI brings, certain steps need to be taken into consideration. Firstly, monitoring and analysis need to be enhanced. Governments, intelligence agencies, and social media platforms should collaborate to develop advanced AI systems capable of detecting and countering terrorist propaganda, recruitment efforts, and planning activities. Governments should enhance their monitoring capabilities to identify potential terrorist use of AI. This could include investing in AI-based tools to monitor social media and other online platforms for signs of radicalisation.

Secondly, it is imperative to enhance existing cybersecurity frameworks with robust measures to effectively counter AI-enabled attacks. This entails proactive vulnerability assessments, secure AI model development, and continuous vigilance against potential intrusions. These efforts may encompass the adoption of AI-driven cybersecurity tools and the training of cybersecurity experts to proficiently detect and respond to AI-based threats.

Thirdly, ethical AI frameworks need to be set up. Policymakers, researchers, and industry leaders must develop ethical guidelines and frameworks for the responsible development and deployment of AI to help minimise the potential for AI to be misused by terrorists whilst at the same time, respecting individuals' right to privacy and civil liberties. Governments should develop regulations to ensure that AI is developed and used in a responsible and ethical manner. These regulations should include strict controls on the development and use of autonomous systems and other technologies that could be exploited by terrorists.

Fourthly, international collaboration is essential to combat the global nature of terrorism and address the challenges posed by AI effectively. In April 2023, G7 Digital Ministers issued a call for a robust policy framework to guide the governance of AI (Komiya, 2023). In a strong stance against AI misuse that jeopardises democratic values and human rights, the ministers emphasised a commitment to human-centric and trustworthy AI. The ministers further pledged to craft guiding principles and an international conduct code for organisations spearheading advanced AI systems. Their vision encompasses AI development that champions democracy, human rights, and shared global values. As part of this endeavour, they've outlined key principles for AI system development, including safety measures, transparency mandates, and a focus on addressing global challenges.

Lastly, more research is needed to develop a more comprehensive understanding of the ways in which terrorists might employ AI technologies. This involves studying their strategies, tactics, and potential vulnerabilities. Governments should allocate dedicated research funding to academic institutions, think tanks, and research organisations specifically for the study of AI-related terrorism threats. Moreover, encouraging private technology companies and foundations to extend grants and financial backing to support these research initiatives is essential. This collaborative approach fosters a vibrant research ecosystem and bolsters the efforts to combat AI-related terrorism threats effectively. Furthermore, researchers hailing from various fields, including computer science, cybersecurity, social sciences, and counterterrorism studies, should collaborate closely. These interdisciplinary teams can collectively provide comprehensive insights into the intricate dynamics of AI misuse by terrorists. By adopting a holistic perspective, these research endeavours promise to yield a more profound understanding of the multifaceted issues at hand.

In conclusion, the dynamic relationship between AI and global terrorism necessitates continuous attention and cooperative efforts involving governments, technology firms, and civil society organizations. The aim is to harness AI for the betterment of humanity while preventing its malevolent exploitation. Through increased research initiatives and the implementation of ethical AI guidelines, evolving threats can be addressed proactively and uphold our shared security in an era shaped by artificial intelligence.

REFERENCES

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist use of cryptocurrencies: technical and organizational barriers and future threats. In *RAND Corporation eBooks*. https://doi.org/10.7249/rr3026

Haddad, M. (2023). Fake Pentagon explosion photo goes viral: How to spot an AI image. *Science and Technology News | Al Jazeera*. https://www.aljazeera.com/news/2023/5/23/fake-pentagon-explosion-photo-goes-viral-how-to-spot-an-ai-image

ICT4Peace, UNCTED. (n.d). Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes. *United Nations*. https://www.washingtonpost.com/politics/2021/08/19/last-month-three-drones-attacked-an-israeli-tanker-heres-why-thats-something-new/

Katsiri, R. (2019). Bitcoin donations to ISIS soared day before Sri Lanka bombings. *Globes*. https://en.globes.co.il/en/article-exclusive-isis-funded-sri-lanka-bombings-with-bitcoin-donations-1001284276

Komiya, K. (2023). G7 should adopt “risk-based” AI regulation, ministers say. *Reuters*. https://www.reuters.com/markets/europe/g7-should-adopt-risk-based-ai-regulation-ministers-say-2023-04-30/

Mascellino, A. (2023). *Artificial intelligence and USBs drive 8% rise in Cyber-Attacks*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/ai-usbs-drive-rise-cyber-attacks/

Rogers, J. (2021). Last month, three drones attacked an Israeli tanker. Here’s why that’s something new. *Washington Post*. https://www.washingtonpost.com/politics/2021/08/19/last-month-three-drones-attacked-an-israeli-tanker-heres-why-thats-something-new/

Staff, R. (2017). Cyber attack hits 200,000 in at least 150 countries: Europol. *U.S.* https://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX

Team, F. I. (2023). Cyber jihadists dabble in DDOS: Assessing the threat. *Flashpoint*. https://flashpoint.io/blog/cyber-jihadists-ddos/#:~:text=Ultimately%2C%20cyber%20jihadists’%20DDoS%20experimentation,approach%20problems%20in%20interesting%20ways.

(2023). UN chief warns of risks of artificial intelligence. (n.d.). https://english.news.cn/20230719/5dfd68d83e6a440a9485c100344c31b1/c.html

EXPLORING THE USE OF GAMES AND GAMIFICATION IN PREVENTING AND COUNTERING VIOLENT EXTREMISM (PCVE)

Nurul Hidayah Mohd Noar

ABSTRACT

This article seeks to highlight gaming as a social activity where gaming-adjacent platform offers social functionality such as text, voice, and video chat. Socialisation and community building in gaming spaces represent a double-edged sword, affording exploitation by extremist actors. This article also reviews the typology of harms, mainly the modification of games, use of gaming culture references, and communications concerns revolving gaming-adjacent platforms. As gamification become more prominent in the coming years, preventing and countering violent extremism (PCVE) approaches need to consider engaging in gaming spaces. Although there are limited examples of gamified approaches in PCVE directly, this article aims to list examples of games-related initiatives in other fields to learn and draw inspiration from. Some positive effects of gamification include the cultivation of social and emotional learning, and intercultural dialogue competencies. The article calls for enhanced subcultural knowledge and other relevant discipline such as psychology and linguistics, as well as a multi-stakeholder approach to reduce online harms.

Keywords: gaming, gamification, gaming-adjacent platform, PCVE

GAMING AS A SOCIAL ACTIVITY

Often when a gamer is portrayed in a movie, they are visualised isolated in the basement or in their room, playing games, and in the background an audible screaming of the parents telling them to get off their computers, consoles, or many other platforms available today. This portrayal is perhaps the reason why many would describe gaming as a solitary activity. While it could be an activity one enjoys alone, gaming can also be a social activity.

Rosenblat and Barrett (2023) described two broad categories of the gaming space. These spaces consist of the games themselves, and platforms that are adjacent to gaming where gamers host a large portion of video game content and discussions about gaming. Some examples of these platforms are Discord, Twitch, Steam and DLive. These spaces all provide avenues where social relationships between players can occur (Kowert et al., 2022) and offer extensive communication via text, voice, and video chat (Lakhani, 2021).

EXPLOITATION OF GAMING SPACES BY EXTREMIST ACTORS

The features that make gaming spaces distinctive and appealing to many users also make them vulnerable to exploitation (Rosenblat and Barrett, 2023). One of the strategies used is the modification or "modding" of existing games to twist the narrative into an extremist message or fantasy (Rosenblat and Barrett, 2023). Examples include the reenactment of Christchurch terror attack in sandbox games like Roblox and Minecraft, and modding of the first-person shooter video game, ARMA III where characters are created based on ISIS militants. Extremist contents are also generated from games such as the reference to Call of

Duty in posters by ISIS (El Ghamari, 2017). Lamphere-Englund and White (2023) viewed that the use of pop cultural references from gaming helps extremist actors to propagandise and recruit for their causes. Earlier this year in Singapore, a 16-year-old was handed a restriction order after having created ISIS propaganda videos using footage from the online gaming platform, Roblox (The Straits Times, 2023).

In December 2021, a 15-year-old who desired to become a suicide bomber was detained in Singapore under the Internal Security Act. The two teenagers were discovered to be in contact via Discord with another teenager aged 18 who was detained in December 2022 after he planned to stab and kill non-believers. Singapore's Internal Security Department has since then listed "radicalisation and recruitment through social media and gaming platforms" as one of the trends of concern in its Terrorism Threat Assessment Report 2023. These incidents raise concerns on the exploitation of gaming-adjacent platform where communication is made possible via text, voice, and video chat.

Many of these platforms were originally tailored to gamers specifically, but are now used by many individuals who are not avid gamers to connect with people of similar interests such as sports, music, and book clubs (Lakhani, 2021). Schlegel (2021) also highlighted other platforms with gaming-related content such as Reddit, YouTube, and chanboards. The attacks in Christchurch and Halle were not only livestreamed and mimicked a visual imagery commonly associated with FPS games, but perpetrators also posted comments and manifestos on chanboards before their attacks. The perpetrator behind the Bratislava attack in October 2022, however, did not seem to spend much time gaming, nor gamified his attack, but consumed content on gaming-adjacent sites like Reddit, 4chan, and 8kun. Language about "high scores", "leaderboards", and "achievements" demonstrated gamified narratives prevalent on the platform.

A sense of community could be one of the strongest appeals of gaming. While socialisation and community building are generally positive, when you have toxic gaming communities and those espousing extremist ideologies, socialisation turns into a potential radicalisation tool (Regeni, 2023). There is limited evidence however to demonstrate radicalisation and recruitment as a primary intent on gaming-adjacent platform (Lakhani, 2021), but rather in online spaces populated by extremists, gaming acts as a means of bringing already radicalised people together (Institute of Strategic Dialogue, 2021). Research has also found that some of the servers on these platforms have specific criteria of who is allowed to join (Schlegel, 2021). This allows for interaction amongst like-minded people where views are reinforced. Cases like the Unite the Right Rally on Discord and War Thunder pinpointed the powerful social bonds built through shared gamer identities and in-group dynamics created in community driven online gaming spaces.

USE OF GAMES AND GAMIFICATION IN PREVENTING ONLINE HARMS

Deterding et al. (2011) defined gamification as the use of game design elements within non game contexts. This may include the elements such as rewarding points, leaderboards, and badges. The next question would be: to what aim? Robson et al. (2015) referred gamification to be aimed at facilitating behavioural change in the users. Hence, why we are seeing gamification across domains such as fitness and education, in applications like Strava and Duolingo. Schlegel (2021) highlighted that some users are not motivated by quantifiable rewards, but by social experiences and the social relatedness offered in communities.

Therefore, gamification may also act as a measure to increase feelings of in-group social belonging and strengthen positive community building.

There are now many examples of games being designed to combat different types of online harm from violent extremism, gender-based violence, to disinformation or misinformation (Passey, 2023). To educate on common disinformation techniques, the game 'Cat Park' and 'Harmony Square' showcased tactics of media manipulation used to exploit social and political tensions. Moonshot developed the game 'Gali Fakta' (Dig for the Facts), with the purpose of better equipping individuals with the media literacy skills necessary to identify disinformation, both online and offline. The European project on 'Play 4 Your Rights' aimed at fighting sexist hate speech through social media education strategies and gamification practices.

The UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development (MGIEP) explored games as pedagogical tools in building social-emotional competencies. Examples of the game-based courses developed are 'Bury Me My Love' and 'Of Loss and Love' which explored concepts of migration, home, belonging, identity, resilience, and compassion. The interactive and immersive nature of digital games provided an opportunity for the cultivation of social and emotional learning, and intercultural dialogue competencies.

Online gaming can be an effective way to foster collaboration between players. Apart from creating games and gamification, one potential tool to be explored is eSports This medium could potentially be leveraged as a tool to teach principles like good sportsmanship and positive interpersonal engagement. The *#SamaSamaMenang* (#WinTogether) initiative by Malaysia's eSports Integrated (ESI), for instance, was to promote in-game positive communication, all while playing the mobile game PUBG.

CONCLUSION

Games and gaming communities contribute to social good in our society in many ways. Research have highlighted the positive effects of gaming, on individuals and groups, in many domains including the development of social, emotional, and cognitive skills. Could the similar effect be transferred over to encourage resilience to extremist narratives and ideologies? Games are generally not the problem, but socialisation from gaming and inside gaming-adjacent platform revealed to be a challenge. As extremists continue to exploit gaming spaces, there is a need to increase digital literacy and awareness of extremism taking place in these spaces.

It must also be emphasised that the gaming communities are not to be treated as at-risk group but rather a potential and valuable partner in ensuring a safe gaming space for all. Creating a safe gaming space is one of the pillars of the healthy gaming initiative by Malaysia Digital Economy Corporation (MDEC), aside from highlighting key opinion leaders from the gaming community, as well as building the right media perception and awareness (Gamer Matters, 2018). Thus, efforts in the gaming space may not necessarily use PCVE-specific language, but leveraged for pro-social and inclusive ends. This may include awareness on excessive toxicity, racism, sexism, cyberbullying, and other online harms.

The success of gamification in other fields have inspired practitioners to explore the possibilities of gamified elements in digital PCVE practices. The psychological mechanisms underlying its success and how to make use of these mechanisms for PCVE are to be investigated. Apart from that, communications within the gaming space used specific imagery, memes, symbols, and other linguistic references. In many of the research, psychological aspect of gaming such as identity building, emotions, and motivations were also explored. To design gamified PCVE intervention, practitioners may benefit from collaboration across multi-disciplinary domains such as psychology and linguistics.

PCVE practitioners need to develop subcultural knowledge of gaming spaces and learn to navigate these platforms. A research report by UNOCT suggested that this knowledge is a necessary precondition to develop effective PCVE campaigns with a gaming dimension. Hence, positive interventions in the gaming space are not on the shoulders of one single entity, but rather various actors. Engagements in these efforts may include game publishers and developers, policy makers, parents, educators, tech companies, and other relevant stakeholders. Some of these engagements on gaming could also take place at an earlier stage before individuals jump into these spaces. Younger aspiring gamers today are likely to have gamer parents themselves, in which how they are introduced to digital environments and the actions modelled can significantly affect their ability to navigate these environments.

REFERENCES

Deterding, S., Dixon, D., Khaled, R. and Nacke, L. (2011). From game design elements to gamefulness: Defining gamification. *Conference Paper*. https://www.researchgate.net/publication/230854710_From_Game_Design_Elements_to_Gamefulness_Defining_Gamification

El Ghamari, M. (2017). Pro-daesh jihadist propaganda: A study of social media and video games. *Security & Defence Quarterly*. 14(1):69-90. https://securityanddefence.pl/Pro-Daesh-jihadist-propaganda-A-study-of-social-media-and-video-games,103197,0,2.htm

ESports Integrated. https://www.esportsintegrated.com/2023/07/28/sama-sama-menang/

Gamer Matters. (2018). MDEC Wants to Promote "Healthy Gaming" In Malaysia: Playing Video Games Is Not a Bad Thing. https://gamermatters.com/mdec-wants-to-promote-healthy-gaming-playing-video-games-can-be-a-good-thing/

Harmony Square. https://harmonysquare.game/en

Institute of Strategic Dialogue. (2021). Gaming and Extremism: Extremists evade mainstream restrictions in corners of gaming world. https://www.isdglobal.org/digital_dispatches/gaming-and-extremism extremists-evade-mainstream-restrictions-in-corners-of-gaming-world/

Internal Security Department. (2023). Singapore Threat Assessment Report 2023. https://www.mha.gov.sg/docs/default-source/default-document-library/singapore-terrorism-threat-assessment-report-2023.pdf

Kowert, R., Martel, A., and Swann W.B. (2022). Not just a game: Identity fusion and extremism in gaming cultures. *Front Commun*. 7:1007128. https://www.frontiersin.org/articles/10.3389/fcomm.2022.1007128/full

Lakhani, S. (2021). Video gaming and (violent) extremism: an exploration of the current landscape, trends and threats. European Commission. https://home-affairs.ec.europa.eu/system/files/202202/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

Lamphere-Englund, G., and White, J. (2023). The online gaming ecosystem: Assessing socialisation, digital harms, and extremism mitigation efforts. Global Network on Extremism and Technology (GNET). https://gnet-research.org/wp-content/uploads/2023/05/GNET-37-Extremism-and-Gaming_web.pdf

Passey, K. (2023). Games as a tool for countering online harm. *Spotlight: Games, Gaming and Gamification*.https://home-affairs.ec.europa.eu/system/files/202307/spotlight_on_gamification_062023_en.pdf

Radicalisation Awareness Network. (2020). Extremists' use of video gaming – strategies and narratives. Conclusions paper. European Commission. https://homeaffairs.ec.europa.eu/system/files/202011/ran_cn_conclusion_paper_videogames_15-17092020_en.pdf

Regeni, P. (2023). The radicalisation challenge on gaming and gaming-adjacent platforms. *Spotlight: Games, Gaming and Gamification*. https://home-affairs.ec.europa.eu/system/files/202307/spotlight_on_gamification_062023_en.pdf

Robson, K., Plangger, K., Kietzmann, J., McCarthy, I. and Pitt, L. (2015). Is it all a game? Understanding the principles of gamification. *Business Horizons*. 58:411-420. https://www.researchgate.net/publication/275059704_Is_it_all_a_ _game_Understanding_the_principles_of_gamification

Rosenblat, M.O. and Barrett, P.M. (2023). Gaming the system: How extremists exploit gaming sites and what can be done to counter them. NYU Centre for Business and Human Rights. https://bhr.stern.nyu.edu/tech-gaming-report

Schlegel, L. and Amarasingam, A. (2022). Examining the intersection between gaming and violent extremism. United Nations Office of Counter-Terrorism. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf

Schlegel, L. (2020). Jumanji extremism? How games and gamification could facilitate radicalisation process. *Journal for Deradicalisation*. 23:1-44. https://journals.sfu.ca/jd/index.php/jd/article/view/359/223

Schlegel, L. (2021). Extremists' use of gaming (adjacent) platforms: Insights regarding primary and secondary prevention measures. European Commission. https://homeaffairs.ec.europa.eu/system/files/202108/ran_extremists_use_gaming_platforms_082021_en.pdf

Schlegel, L. (2021). The gamification of violent extremism & lessons for PCVE. European Commission. https://home-affairs.ec.europa.eu/system/files/2021-03/ran_ad-hoc_pap_gamification_20210215_en.pdf

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

UNESCO Mahatma Gandhi Institute of Education for Peace and Sustainable Development. https://mgiep.unesco.org/

PART 5

BOOK REVIEWS

COMBATING VIOLENT EXTREMISM AND RADICALIZATION IN DIGITAL ERA

By Khader, M., Neo, L. S., Ong, G., Mingyi, E. T., & Chin, J. (2018)
IGI Global, 382 Pages

Reviewed by Siti Aisyah Tajari

Advances in digital technologies have provided ample positive impacts to modern society; however, in addition to such benefits, these innovations have inadvertently created a new venue for criminal activity to generate. The book *Combating Violent Extremism and Radicalization in the Digital Era* describes the multidisciplinary approach of the online platforms used by violent extremists to recruit new members and plan terrorist attacks, the motivations and attributions involving online violent extremism, and the possible tools for assessing risk and countering violent extremism in the digital realm. In general, the book aims to provide a reminder that online radicalisation poses a serious threat to safety and security all over the world. Violent extremism has continued to evolve with new forms of social media. There is therefore a critical need for governments and communities across the world to step up their counter-terrorism efforts.

The chapters in this book have been organised broadly in the following themes, demarcated by sections. These sections are (i) Section 1: Exploitation of the Internet by Violent Extremists (Chapters 1-5); (ii) Section 2: Understanding the 'Person' within Online Violent Extremism (Chapters 6-11); (iii) Section 3: Countering Violent Extremism and Radicalisation (Chapters 12 20), (iv) Section 4: Emerging Trends (Chapters 21-23); and (v) Section 5: Summary and Future Directions (Chapter 24).

Section 1 on the theme of 'Exploitation of the Internet by violent extremists' comprises chapters that discuss the role of online platforms and how violent extremists can leverage them. In many cases, these extremists have leveraged online media for their needs and to propel their cause.Loo Seng Neo and his team in their chapter 'Understanding the Psychology of Persuasive Violent Extremists Online Platforms' highlight how violent extremist groups have not just exploited, but also created, online platforms that enhanced their recruitment campaigns across the world. The chapter examines the features of these platforms which enhance the appeal of violent extremist messages. Robyn Torok in her chapter 'Social Media and the Use of Discursive Markers of Online Extremism and Recruitment' examines the shift in recent years towards the use of social media to fuel violent extremism. The chapter discusses key discursive markers based on existing radicalisation models and how these markers are used to fuel violent extremism. Finally, David Romyn and Mark Kebbell in their chapter 'Using the Internet to Plan for Terrorist Attack' discuss how terrorists can use the internet as a source of information to plan for terrorist attacks, and how this information can be manipulated to reduce the likelihood or severity of a terrorist attack.

The theme for Section 2 is 'Understanding the 'Person' within Online Violent Extremism', providing a person-specific focus on the issue of online violent extremism. This section contains chapters which examine the motivations and psychological attributes of the individual who may increase his or her likelihood of becoming involved in online violent extremism. Joyce Pang's chapter 'Understanding Personality and Person-specific Predictors of Cyber-based Insider Threat' discusses the major challenges for understanding insider threat in the context of cyber security. It examines cyber-based insider threats from a personality and person-specific perspective that emphasises internal characteristics of the individual actor as explanations of actions and events. Omer Saifudeen in his chapter 'Getting Out of the Armchair - Potential Tipping Points for Online Radicalisation' highlights another interesting angle affecting the human actor, that is how the key to understanding tipping points in online violent extremism lies in understanding the cognitive, social, and emotional barriers to violent extremist thinking and action. He discusses the need for research and experimentation on persuasion tactics for countering online extremism. Erin Saltman in her chapter 'Western Female Migrants to ISIS: Propaganda, Radicalisation and Recruitment' highlights how women continue to play strong roles in online and offline recruitment to violent extremist organisations. The chapter addresses questions of gender within current radicalisation trends through an analysis of online data that tracks Western females migrating to territories under the control of ISIS. Finally, Loo Seng Neo in his chapter on 'An Internet-Mediated Pathway for Online Radicalisation: RECRO' introduces a framework to explain the interaction between cyber systems and personal factors, and highlights how this framework can be used to guide the identification of key behavioural markers for individual's involvement in online violent extremism.

In Section 3, the theme of 'Countering Violent Extremism and Radicalisation' comprises chapters that bring us into the thick of key areas valuable for implementing measures to counter online violent extremism. Geoff Dean in his chapter on 'Framing the Challenges of Online Violent Extremism: 'Policing-Public-Policies-Politics' Framework' uses a framework to expound real and relevant implications surrounding efforts to combat online violent extremism. Kumar Ramakrishna in his chapter on 'Towards a Comprehensive Approach to Combating Violent Extremist Ideology in the Digital Space: The Counter-Ideological Response (CIR) Model' introduces a model aimed to gradually diminish the appeal of violent extremist ideology. This model can potentially guide ideology-relevant policy interventions to impact the overall reach and appeal of the violent extremist narrative vis-a-vis any countervailing narrative against it. Damien Cheong in his chapter on 'Countering Online Violent Extremism: State Action as Strategic Communication' focuses on the utility of strategic communication strategies, particularly state action, in countering violent extremism both online and offline, while Jethro Tan and his team in their chapter 'Building National Resilience in the Digital Era of Violent Extremism: Systems and People' focus on building national resilience as a macro-level strategy for countering violent extremism. The latter chapter examines the 'systems' within a nation such as critical infrastructures and how they can be built 'resilient-by-design' to ensure continuity in times of crisis and also explores 'person' factors of crisis communication, cohesion, and social capital, and discuss how instilling these factors can engender a cohesive society that can overcome the cracks in social order and harmony often caused by violent extremism. Jennifer Yang in her chapter on 'Social Media Analytics for Intelligence and Countering Violent Extremism' discusses collection methods and analytical tools for the study of social media data to facilitate intelligence-gathering and efforts to counter violent extremism. The coverage in this chapter includes social network analysis, sentiment analysis, multilingual analysis, geo-coding, automated entity extraction, semantic search and multimedia analysis.

There are also chapters in section 3 that introduce tools for assessing the risk of online violent extremism and discuss the challenges of making assessments in the online domain. Neil Shortland in his chapter on '"On the Internet, Nobody Knows You're a Dog": The Online Risk Assessment of Violent Extremists' draws links on how psychology can contribute to conducting online risk assessment of violent extremism. Fredrik Johannson and colleagues in their chapter on 'Detecting Linguistic Markers of Violent Extremism in Online Environments' discuss the use of linguistic markers in natural language processing as warning behaviours to detect online violent extremism. Elaine Pressman and Cristina Ivan in their chapter 'Internet Use and Violent Extremism: A Cyber-VERA Risk Assessment Protocol' introduce a new tool named CYBERA (adapted from the pre-existing tool VERA-2), which is designed to be a systematic, empirically-grounded, cyber-focused assessment guide to assess the risk of online violent extremism. CYBERA focuses on cyber-related behaviours and content to guide the assessment of early signs of online violent extremism. Finally, Priscilla Shi in her chapter 'A Supplementary Intervention to Deradicalisation: CBT-Based Online Forum' propounds the idea of online deradicalisation and delves into online therapeutic engagement and its potential applicability to deradicalisation.

Section 4 on the theme of 'Emerging Trends' comprises chapters that highlight the potential threat posed by violent extremists as they adopt the modus operandi commonly associated with cyber criminals. Leevia Dillon in her chapter on 'Cyberterrorism: Using the Internet as a Weapon of Destruction' focuses on cyberterrorism and draws on parallels from research on cyber threats and terrorism based on six themes (modus operandi, domain, targets, impact, antagonists and motivations) to formulate a cyberterrorism conceptual framework. The chapter provides a hypothetical four-step cyberterrorism attack sequence and suggestions for best practices. Penelope Wang in her chapter on 'Death by Hacking: The Emerging Threat of Kinetic Cyber' focuses on kinetic cyber threat and highlights various forms of kinetic cyber as well as the vulnerabilities that make devices and systems (for example personal medical devices, cars, critical infrastructures) susceptible. The chapter introduces the motivations and characteristics of violent extremists who might engage in kinetic cyber-attacks. Arun Vishwanath in his chapter on 'Spear Phishing: The Tip of the Spear Used by Cyber Terrorists' focuses on spear phishing, which is an email spoofing fraud attempt that seeks unauthorised access to confidential data, highlighting it as the vector used to gain access to a computer network in almost all forms of cyber-attacks. The chapter, which emphasises the need for policy interventions, provides an overview of the different strategies being used to combat it and their relative effectiveness.

The final section, Section 5, brings the discourse on combating online violent extremism and radicalisation to a close by summarising the key learning lessons from the preceding chapters, as well as identifying future research directions. This concluding chapter on 'What We Know and What Else We Need to do to Address the Problem of Violent Extremism Online' by Majeed Khader, highlights potential future trends for online violent extremism and in tackling these trends, the need to understand the critical catalysts for change which violent extremists can exploit. The chapter also discusses the need to evaluate counter-violent extremism measures and identifies areas for future research.

COUNTER-TERRORISM, ETHICS AND TECHNOLOGY: EMERGING CHALLENGES AT THE FRONTIERS OF COUNTER-TERRORISM

By Henschke A., Reed, A. Robbins, S. & Miller, S. (2021)
Springer, 231 pages

Reviewed by Siti Hikmah Musthar

The utilisation of technology in the field of counter-terrorism has become a fundamental component of safeguarding individuals in the modern era. However, the proliferation of such technology has also raised a number of ethical issues that must be addressed. The utilisation of technology in a counter-terrorism context raises questions concerning the protection of privacy, the safeguarding of personal data, the protection of human rights, as well as the implementation of ethical principles. As we strive to develop and implement new methods of preventing terrorist attacks and other forms of violence, it is essential to ensure that security implementation is balanced with ethical considerations. This is due to the fact that an understanding of how existing or novel technologies are employed in the context of counter terrorism provides a foundation for distinguishing the myth from the reality.

In this book, the authors explored some of the ethical issues surrounding counter-terrorism technology, types of existing technology, and its application in the name of counter-terrorism. The book explored these ethical issues at the borders of counter-terrorism, examining a variety of technologies and practices across terrorism, counter-terrorism, and contemporary social practices. Although the threads are somewhat disconnected, they form a cohesive narrative of similar challenges: how technologies are transforming terrorist behaviours, shaping counter-terrorism responses, and what is the critique and justification for these behaviours and responses. One of the most significant contributions made by the discussions in the book is the emphasis made by the authors on the importance of understanding ethical issues associated with the use of counter-terrorism technologies because it is essential for maintaining a balance between security and individual rights, fostering accountability, and promoting responsible innovation in this critical area. It ensures that counter-terrorism efforts are not only effective but also ethically sound and in alignment with democratic values. Discussions and arguments presented by the authors in the book should be able to bring enlightenment to its reader in terms of gaining more knowledge on ethical issues related to counter-terrorism.

The book is organised into five main chapters, each of which explores different aspects of the broader narrative. Within each section, multiple chapters are presented in an article format authored by a single author. Each chapter invites the reader to reflect on the ethical implications of the use of technology in the context of the fight against terrorism. Each chapter encourages the reader to both agree with and be moved to their arguments, as all of the arguments are intended to motivate the reader to think beyond the knowledge acquired.

The first part of the book looked at how technologies shape the practice and understanding of counter-terrorism, looking at one of the most controversial sets of technologies used in efforts against terrorists, which is the drone. Precisely, it presents two case studies related to technology and counter-terrorism namely on police control technologies and drone warfare - its impact on counter-terrorism operations. The author examined how these technologies are used in the context of counter-terrorism efforts. It explored the ethical implications of technologies such as surveillance systems, facial recognition, and predictive policing algorithms. The second case study revolved around drone warfare and its impact on counter terrorism operations. It delved into the ethical challenges posed by using armed drones in targeted killings, including issues of civilian casualties, accountability, and the erosion of traditional notions of warfare. Both case studies aimed to shed light on the emerging challenges at the frontiers of counter-terrorism, highlighting the ethical considerations and dilemmas that arise from the use of technology in combating terrorism.

The proposed focus for identifying acts of terrorism, as mentioned in part one of the book, was to examine the impact of technologies of violence on those most affected. The author argued that the use of technology, such as police control technologies and armed drones, can hide and enable forms of state violence that can be considered terrorist acts. Therefore, the focus should be on understanding the consequences and implications of these technologies on individuals and communities, particularly in terms of harm and violence inflicted upon them. By examining the effects of technology on those impacted, a more comprehensive understanding of acts of terrorism can be achieved.

The second part of the book offered an analysis of three different technology types to show how the use of particular technology presents challenges for counter-terrorism. Three main discussions and arguments on weapons of mass destruction (WMD), Internet of Things (IoT), and Facial Recognition Technology (FRT). The author begins by emphasising on the notion of weapons of mass destruction (WMD) to offer an argument for a new way of considering these technologies. However, the challenges posed by technologies of terrorism and counter-terrorism are complex and multifaceted. For instance, the author argues their concerns on the concept of WMD and its relationship with CBRN, therefore he offers a complex understanding of the impact of technology use and their availability for terrorists. Then the author highlights the ethical implications of IoT-enabled cyber-terrorism, emphasising the need for proactive regulation and ethical considerations to mitigate risks and protect against harm. Additionally, while FRT offers significant advantages in terms of security and convenience, the author raised complex ethical and privacy questions. Striking a balance between its potential benefits and the protection of individual rights is an ongoing challenge that requires careful consideration, regulation, and public dialogue. The author concluded his argument which effectively highlighted the convergence of technology, insecurity, physical presence, scale, AI, and invisibility within the IoT that collectively make it a viable threat vector for cyber-terrorism. The acknowledgment of ethical responsibilities and the call for regulation underscore the importance of addressing these challenges in a rapidly evolving technological landscape.

The third part of the book shed light on how surveillance technologies can empower the state, raising important ethical questions about individual rights and privacy. The authors examined surveillance technologies to demonstrate how, when used as part of broader counter-terrorism programs, these technologies can make the state much more powerful. They also illustrate how such technologies can be integrated into broader political ideologies and agendas, as demonstrated in the case of China's "preventive" counter-terrorism campaign. These discussions contribute to a deeper understanding of the complex relationship between technology, ethics, and state power in the context of counterterrorism efforts. The book discussed that the ethical implications of anti-terrorism intelligence go beyond data collection and use of data. According to the authors, the emergence of a formal surveillance state at the beginning of the 21st century was driven by political pressure to expand the capabilities of security and intelligence organisations to carry out a wide variety of counter-terrorist tasks. The ethical debate over the implications of modern states' security intelligence reach has focused on how to balance individual's rights, liberties and privacy with the state's security. At the same time, the surveillance state has rapidly developed into an intelligence state, able not only to collect and use pervasive data, but also to use analytical modelling that broadens the scope of surveillance. The three emerging capabilities of a modern intelligence state are persistent data surveillance (SDS), pattern of life analysis (POL) and activity-based intelligence (ABI). The ethical ramifications of counter-terrorist intelligence extend beyond collecting and using data to use predictive modelling to de humanise patterns of behaviour, and the author argued that this process can redefine the definition of a person, especially by blurting out the distinction between thinking and actions that threaten the state.

The fourth part of the book explored and expanded on the ways in which encryption technologies can help limit state power, partly as a counterweight to surveillance technologies, and partly as a way for individuals to avoid certain state surveillance. In the chapter, the authors discussed the technology of encryption, and argued that encryption is "clearly good" because it protects privacy, but "potentially problematic" because it may unfairly impede legitimate counter terrorism operations. Then the authors examined the use of End-to-End Encryption (E2E), a widely used technology that has become increasingly popular on mobile phones that operate over the internet. This technology has been used by terrorists to plan operations that directly result in the death of innocent civilians, as well as by extremists to challenge cruel regimes and to challenge the rule of law in liberal democracies. It was rather analytical when the authors argued that while the use of E2E by terrorists may be unjustifiable in a liberal democracy context however, in an international context, the protection that E2E provides to those who seek to establish a law-abiding democracy cannot be ignored.

The fifth part of the book addressed the critical issue of responding to terrorism in the digital age, particularly focusing on extremism online. This section discussed the ethical challenges related to regulating online content and examined the role of online manifestos in terrorism. In this chapter, the authors argued who should determine what gets regulated, rather than asking how or what appropriate materials to use. This chapter prompted the argument that because there are so many different elements to how online content is regulated; it is difficult to answer "who should regulate online extremist content?" Instead, they suggested a more comprehensive and collaborative approach to regulating content online by looking at what institutions and services are offering.

In the last part of the chapter, the authors explored a specific element of online political extremism, identity construction, and the utility of analysing terrorist strategies through narrative frameworks, with the aim of demonstrating that strategies can be interpreted as a blueprint for a violent act in the realm of terrorism (the online world). This chapter investigated the dynamics of identity fusion and a particular online terrorist strategy that is associated with an activist and extremist agenda, partially aimed at exploiting the media within a national security context. Furthermore, the ethical implications of how this online material is presented by the media are discussed. The authors suggested that if the media changes its coverage of mass shooters, it may be able to deny them the personal attention they desire in their pursuit of meaning, and may discourage some future perpetrators from perpetuating the normalisation of violent behaviour.

In summary, this part of the work contributed to the ongoing discussions about ethical and practical challenges of addressing terrorism in the digital age and the roles that technology, regulation, and media coverage play in this complex landscape. There is no one-size-fits-all solution to the issues raised in this book, as the contributors brought a variety of tools and approaches. Furthermore, there is no consensus on how technology should be employed or regulated in the context of the fight against terrorism; this is partly because of the ongoing debates on counter-terrorism and technology, and partly a reflection of the book itself. These topics are vast and intricate, and attempting to navigate them is a difficult and demanding task. Nevertheless, there were common threads throughout the discussions; not only must we address terrorism as it develops, but we must also acknowledge and grapple with the role that technologies are playing in the battle against terrorism and violent extremism. While the challenges are immense, together we can find a way to advance the fight against terrorism and push back the boundaries.

NOTES ON CONTRIBUTORS

CÁTIA MOREIRA DE CARVALHO holds a Ph.D. in Psychology from the University of Porto, Portugal. Her research interests are on psychosocial processes of radicalisation and deradicalisation, new trends on violent extremism, and forced migrations. Currently she is a researcher at the University of Porto, a member of RAN Policy Support European Research Community on Radicalisation Researchers' Directory, and a consultant for the Organisation for Security and Co-operation in Europe. Her work has been funded by the European Union, Public Safety Canada and the USA Department of Homeland Security.

FARLINA SAID is a Senior Analyst in the Foreign Policy and Security Studies programme. She graduated from S Rajaratnam School of International Studies, Nanyang Technological University, Singapore with an M.Sc. (Strategic Studies). She was involved in crafting various dialogues and forums on cybersecurity, radicalisation and Malaysia-Korea relations. Her work and comments have appeared in the local and international media, such as New Straits Times and South China Morning Post. She was a part of SEARCCT's Experts on Violent Extremism and Community Engagement (EVOKE) Council (2018-2019).

KAMARULNIZAM ABDULLAH is Professor and Principal Fellow at the Institute of Malaysian and International Studies (IKMAS), Universiti Kebangsaan Malaysia (UKM), Malaysia. His areas of research focus on national and regional security; border studies; terrorism and political violence, and conflict studies. Among his recent publications are, "Navigating Against Salafi-Wahabi Expansion in Malaysia: The Role of State and Society (*Studia Islamika*, 2022); "Financial Innovations in Terrorism Financing: A Case Study of Malaysian Terror Financing (co-author, Journal of Criminological Research, Policy and Practice, 2023); "Malaysia: Adapting to the Dynamic Changes of Terrorist Threats.' (co-author, Non-Western Responses to Terrorism, Manchester University Press, 2019). He is also senior consultant for the Home Ministry's National Action Plan in Preventing and Countering Violent Extremism (NAPPCVE).

MURNI WAN MOHD NOR is a Senior Lecturer at the Department of Government and Civilisational Studies, Faculty of Human Ecology, Universiti Putra Malaysia (UPM), Malaysia. She is also a research associate at the Institute for Social Science Studies (ISAS) and fellow at the Centre for Human Rights Research and Advocacy (CENTHRA). She holds a Ph.D. in Law, focused on the issue of hate speech, the harms it brings, and the need for specific legislation. Her current research interests extend to media representation on racial and religious issues, Islamophobia, as well as combating hate speech and take news within the community through media literacy, anti-racism education and counter speech initiatives. She has held several consultancies on human rights and hate speech-related projects, such as The Centre's Research on Developing a Framework for Hate Speech Categorisation and Response, for UNDP on the Impact of Hate Speech and Misrepresentation in Relation to Covid-19 on social cohesion, and for CENTHRA's stakeholder's report for the UN's Universal Periodic Review on Human Rights.

NICOLE MATEJIC is a published Author and Preventing Radicalisation to Violent Extremism Pracademic. She is currently the Principal Advisor – Violent Extremism, at the Department of Internal Affairs in Aotearoa, New Zealand. Dr Matejic is also an Adjunct Lecturer at Charles Sturt University, Australia, in the School of Terrorism and Security Studies.

OSMAN BAKAR holds a Doctorate in Islamic Philosophy from Temple University, Philadelphia (USA) is currently Holder of Al-Ghazali Chair of Epistemology and Civilizational Studies and Renewal at the International Institute of Islamic Thought and Civilization (ISTAC), International Islamic University Malaysia (IIUM), Malaysia. He is also Emeritus Professor in Philosophy of Science at University of Malaya. He was formerly Distinguished Professor and Director of Sultan Omar 'Ali Saifuddien Centre for Islamic Studies (SOASCIS), Universiti Brunei Darussalam. Dr Osman was also formerly Malaysia Chair of Islam in Southeast Asia at the Prince Talal al-Waleed Center for Muslim-Christian Understanding, Georgetown University, Washington DC, and Deputy Vice Chancellor (Academic and Research) at University of Malaya. Dr Osman is an author and editor of 40 books and more than 300 articles on various aspects of Islamic thought and civilisation, particularly Islamic science and philosophy in which he is a leading authority. His most well-known books are *Classification of Knowledge in Islam* (1992) and *Tawhid and Science* (1992). His latest books are *Colonialism in the Malay Archipelago: Civilizational Encounters* (eds) (2020), *Environmental Wisdom for Planet Earth: The Islamic Heritage* (2022), and *Islam-Buddhism Eco Dialogue (IBED): Application of Religion and Science to Ecology and Sustainability* (eds) (2023). Dr Osman is a recipient of several prestigious awards, including Ibn Ishaq Al-Kindi Intellectual of the Year Award (National, 2020) and the 13th Farabi International Award on Humanities and Islamic Studies (International Top Researcher, 2022). His writings have been translated into numerous languages, including Arabic, Turkish, Persian, Chinese, Bosnian, Urdu, Bengali, and Spanish. He has been named among the 500 most influential Muslims in the world since 2009. He was made a *Dato'* title in 1994 by the Sultan of Pahang and a *Datuk* by the King in 2000.

TIFFANY JANE BUENA is currently serving as Information Officer III at the Defense Communications Service of the Department of National Defense. Among her work in the Department is to enhance the situational awareness of defense leaders on pertinent defense issues through daily media monitoring. She also spearheaded institutional reforms such as the establishment of communications officers in offices in the Department, as well as the crafting of the DND Social Media Handbook. She has led the crafting of communications plan branding for various Department efforts, including the 10-Point Defense Agenda and the branding guide for the Task Force Balik Loob. Tiffany has undergone training in strategic communication with the Armed Forces of the Philippines Civil-Military Operations School, Department of Defence Australia, and the United Nations Office for Counter-Terrorism.

HO KIAN WEI currently resides in The Hague, The Netherlands. He holds an M.Sc. in Crisis and Security Management with a specialisation in Governance of Radicalism, Extremism, and Terrorism from Leiden University and a Bachelor's degree in International Relations from Staffordshire University, United Kingdom.

KENNIMROD SARIBURAJA is a Director of Research and Publications at the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs, Malaysia. He holds a B.A. (Hons) majoring in Southeast Asia Studies and a minor in International and Strategic Studies from the University of Malaya, Malaysia. In 2015, he was awarded a Chevening Scholarship to pursue an M.Litt. in Terrorism and Political Violence at the University of St Andrews, Scotland. Over the years, he has published monographs and articles on terrorism, counter-terrorism, international security, and global politics. His current research interests cover online extremism, terrorism and border security, and new and emerging technologies and terrorism.

MOHD MIZAN MOHAMMAD ASLAM holds a position as Professor in Security & Strategic Studies at the National Defence University of Malaysia (NDUM), Malaysia. Mizan is also a Senior Fellow at the Global Peace Institute (GPI), London, United Kingdom. Mizan holds a position as National Panel for Deradicalisation, a special task-force unit for rehabilitation programs for terrorist's inmates. Mizan also works with the Ministry of Home Affairs (MOHA) of Malaysia in developing modules on deradicalisation program. Mizan was a former professor in Counter Terrorism Studies at the Naif Arab University for Security Sciences (NAUSS), Riyadh, Saudi Arabia where he established the Centre for Terrorism & Extremism Studies (CTES). He holds a position as Chairman of Perdana Global Peace Foundation (PGPF). Mizan also works with Middle Eastern Institute (MEI), Washington, USA as Country Expert in analysing terrorism and extremism issues in SEA and MENA.

SINDUJA UMANDI WICKRAMASINGHE JAYARATNE is a Ph.D. candidate in Faculty of Defence Studies and Management in National Defence University of Malaysia (NDUM), Malaysia. Sinduja was a Lecturer in General Sir John Kotalawela Defence University (KDU), Sri Lanka teaching political science, terrorism, violent extremism and intelligence to undergraduate and postgraduate students. She obtained M.Sc. in Strategic Studies from Nanyang Technological University, Singapore, and B.Sc. in International Relations from University of London (London School of Economics and Political Science), United Kingdom. Prior to her current position, she has been working as an Intelligence Analyst in Sri Lanka, dealing with national security related issues. Sinduja was also a 'Student Research Assistant' in S. Rajaratnam School of International Studies (RSIS), Singapore, conducting research on violent extremism and counterterrorism. She also poses six years of working experience in the humanitarian sector contributing to the reconciliation and rehabilitation process during the post-conflict era in Sri Lanka.

MUHAMMAD AFIQ ISMAIZAM works as a Research Officer at the Southeast Asia Regional Centre for Counter Terrorism (SEARCCT), under the Ministry of Foreign Affairs, Malaysia. His research focuses on the development of Artificial Intelligence (AI) and its misuse by terrorists. 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 is also pursuing an M.A. in International Affairs (part time distance learning) at King's College London, United Kingdom.

NURUL HIDAYAH MOHD NOAR is a Research Officer at the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs, Malaysia. She obtained her undergraduate degree in Social Science (Political Science) from the National University of Malaysia (UKM), Malaysia. She did her M.A. in Media and Information Warfare Studies in 2018 at the Centre for Media and Information Warfare Studies, Faculty of Communication and Media Studies, Universiti Teknologi MARA (UiTM). Her role at SEARCCT includes conducting research activities on issues related to terrorism and counter-terrorism, organising SEARCCT's public awareness programmes such as the university lecture series and public forums, as well as moderating content on SEARCCT's very own podcast channel called the No-Book Book Club. Her current research interest covers gaming and extremism, particularly looking into how games and gaming can be used to prevent and counter violent extremism.

SITI AISYAH TAJARI is a Research Officer at the Southeast Regional Centre for Counter-Terrorism (SEARCCT), under the Ministry of Foreign Affairs, Malaysia. She graduated from the National Defense University of Malaysia (NDUM), Malaysia with a Bachelor in Strategic Studies. She is currently pursuing her Master's in Strategic Analysis and Security at the Faculty of Social Science and Humanities, National University of Malaysia (UKM), Malaysia. Prior to completing her three years of training in the Reserve Officer Training Unit during her undergraduate studies, she was commissioned as a Second Lieutenant and served as a Reserve Officer in the Territorial Army Regiment of the Malaysia Army. Her current research area focuses on gender perspective and gender-sensitive approaches in terrorism, specifically in the rehabilitation and integration of female terrorist offenders.

SITI HIKMAH MUSTHAR is currently a Research Officer at the Southeast Asia Regional Center for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs, Malaysia. Previously, she was a Research Assistant at the Center for Transportation Research, University of Malaya (UM). Despite a diversion of research field, she was exposed to a wide range of research-related tasks, including data collection, data analysis, and data management as well as research methodology and article writing. She graduated from Universiti Teknologi MARA (UiTM) with a Master of Mass Communication in 2013. She is currently pursuing a Doctor of Philosophy (PhD) in Communication and Media Studies at her alma mater, focusing her research on the area of components of persuasion. Her research interests include persuasive communication, hate speech, theory of human behaviour, and audience involvement.