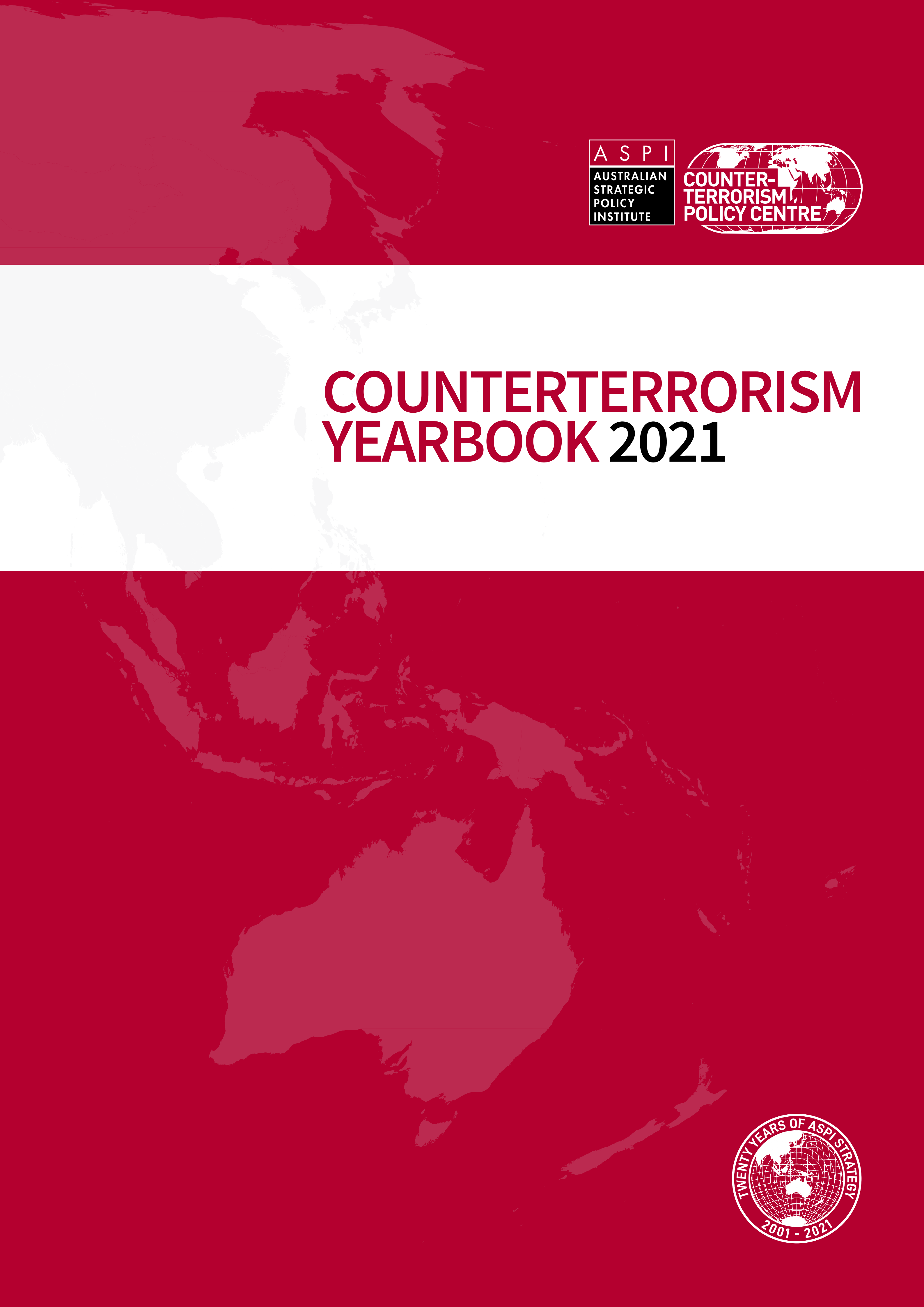


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

COUNTER-
TERRORISM
POLICY CENTRE

COUNTERTERRORISM YEARBOOK 2021

TWENTY YEARS OF ASPI STRATEGY
2001 - 2021

ABOUT ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at http://www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality and innovation, quality and excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

ABOUT THE COUNTER-TERRORISM POLICY CENTRE

ASPI's Counter-Terrorism Policy Centre (CTPC) was established in late 2015. The centre undertakes research across the spectrum of counterterrorism topics, facilitates dialogue and discussion amongst stakeholders, and provides advice to government, community and industry stakeholders, with a particular focus on what can be done to counter terrorism.

ACKNOWLEDGEMENTS

ASPI would like to thank the authors for their contributions, insights and recommendations, as without them the *Counterterrorism yearbook 2021* could not have been compiled. Special thanks to the Hon Peter Dutton, MP, Minister for Home Affairs for providing the preface to this 5th edition of the yearbook. The editors would also like to thank Michael Shoebridge for his additional editorial recommendations; as well as Steve Clark, Emily French and James Dixon, the ASPI publication team, for their assistance with the production of this publication. Finally, thanks to everyone at ASPI for their ongoing support.

IMPORTANT DISCLAIMER

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

No specific sponsorship
was received to fund
production of this report

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

COUNTER-TERRORISM POLICY CENTRE

COUNTERTERRORISM YEARBOOK 2021

Edited by Leanne Close and Daria Impiombato

© The Australian Strategic Policy Institute Limited 2021

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, Educational Institutions (including Schools, Independent Colleges, Universities, and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published March 2021

Published in Australia by the Australian Strategic Policy Institute

ISSN 2209-2420

ASPI

Level 2,
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
Facebook/ASPI.org
@ASPI_org

Contents

PREFACE 05
THE HON PETER DUTTON MP

INTRODUCTION 07
LEANNE CLOSE

THE CURRENT TERRORISM ENVIRONMENT

GLOBAL TERRORISM INDEX 2020: THE SHIFTING LANDSCAPE OF TERRORISM 11
THOMAS MORGAN, OLIVIA ADAMS AND DR DAVID HAMMOND

TERRORISM IN NEW ZEALAND: HOW A DIFFERENT APPROACH MIGHT HAVE PREVENTED THE CHRISTCHURCH MOSQUE ATTACKS 15
DR JOHN BATTERSBY

LONE ACTOR TERRORISM IN 2019 AND 2020: TRENDS AND IMPLICATIONS 19
CHRISTOPHER WINTER AND RAMÓN SPAAIJ

EVOLVING TERRORISM THREATS AND COUNTERTERRORISM RESPONSES DURING THE COVID-19 PANDEMIC IN SOUTHEAST ASIA 23
JEREMY DOUGLAS AND NIKI ESSE DE LANG

THE IMPACT OF ONLINE PLATFORMS, SOCIAL MEDIA AND TECHNOLOGY ON TERRORISM

THE IMPACT OF TECHNOLOGY ON EXTREMISM 29
LEVI J WEST

BOOGALOO BOIS: THE BIRTH OF A ‘MOVEMENT’, FROM MEMES TO REAL-WORLD VIOLENCE 33
ELISE THOMAS

ASSESSING THE MAGNITUDE OF THE THREATS POSED BY HOAX DEVICES IN TERRORIST ATTACKS AND EFFECTIVE COUNTERMEASURES 39
DR JOSHUA SINAI

TERRORISM FINANCING, SUPPORT AND THE ORGANISED CRIME NEXUS

TERRORIST FINANCING: GLOBAL POLICY CHALLENGES AND INITIATIVES IN 2020 43
DR GORDON HOOK

COUNTERING TERRORIST FINANCING: STRENGTHENING INDONESIA–AUSTRALIA COLLABORATION 49
SYLVIA LAKSMI

DEMYSTIFYING THE TERROR–CRIME NEXUS IN AUSTRALIA 55
DR JOHN COYNE

FIGHTING ORGANISED CRIME, PREVENTING TERRORISM: THE ITALIAN CASE 61
DARIA IMPIOMBATO

REVISITING THE TERROR–CRIME NEXUS IN LATIN AMERICA: MILITANT PROTO-STATE GOVERNANCE AND CHALLENGES TO STATE SECURITY 67
DR ALEXANDRA PHELAN

COUNTERING AND PREVENTING VIOLENT EXTREMISM 71

AN EVOLUTION OF TERRORISM: THE INTERSECTION OF CYBERCRIME AND TERRORIST ACTIVITY 71
DR ANNE ALY MP

THE EVOLUTION OF RESILIENCE TO VIOLENT EXTREMISM 77
PROFESSOR MICHELE GROSSMAN

OPERATIONAL PERSPECTIVES ON TERRORISM AND MANAGING THE RISK 83
COMMANDER SANDRA BOOTH AND
ASSOCIATE PROFESSOR DR NATALIE DAVIS

UNDERSTANDING TRANSITIONS TO VIOLENCE AND THE ROLE OF PRACTITIONER–ACADEMIC PARTNERSHIPS 87
DEPUTY COMMISSIONER ROSS GUENTHER AND ASSOCIATE PROFESSOR DEBRA SMITH

COUNTERING VIOLENT EXTREMISM: THE NEW SOUTH WALES APPROACH 91
PIA VAN DE ZANDT, AFTAB MALIK AND MADELEINE COOREY

THE NEW FAR RIGHT: CONSTRUCTION OF HATRED AGAINST THE ISLAMIC COMMUNITY IN MULTICULTURAL AUSTRALIA 97
ANGEL ADAMS

YOUNG PEOPLE AND VIOLENT EXTREMISM IN THE COVID-19 CONTEXT 101
PETA LOWE

THE IMPACT OF NATURAL DISASTERS ON VIOLENT EXTREMISM 107
LYDIA KHALIL

THE IMPORTANCE OF INTER-OFFICE COORDINATION IN COUNTERTERRORISM: THE ISRAELI CASE STUDY 113
PROFESSOR BOAZ GANOR

ABOUT THE AUTHORS 119

ACRONYMS AND ABBREVIATIONS 127

Preface

THE HON PETER DUTTON MP

Minister for Home Affairs

Terrorism poses an enduring and evolving threat requiring a coordinated and collaborative approach between governments, the private sector and community. Addressing the threat requires sustained effort and responsive policies that are informed by a robust understanding of the changing risk environment and operational experience of law enforcement.

As the Director-General of ASIO has observed, the threat from Islamic extremism endures, with groups including the Islamic State of Iraq and the Levant and al-Qaeda continuing to inspire attacks globally and in Australia. However, this does not mean our agencies are blind to other extremist threats. Unfortunately, there are groups of individuals in Australia motivated by Nazism, white supremacy and other hateful ideologies. We will not tolerate any form of extremism that resorts to intimidation or violence to spread a message of hate.

At the time of writing, the Australian Government is in the process of listing Sonnenkrieg Division as a terrorist organisation under the Criminal Code. Sonnenkrieg Division's encouragement, promotion and glorification of terrorism has inspired UK-based extremists, and has the potential to similarly inspire Australia-based extremists. Listing ensures that Criminal Code offences with penalties of up to 25 years imprisonment apply to this organisation.

The Parliamentary Joint Committee on Intelligence and Security is also undertaking an inquiry into extremist movements and radicalism in Australia. Once the inquiry is complete, the government will carefully consider the committee's recommendations in relation to current legislative settings and other matters.

Since the national terrorism threat level was raised to PROBABLE in August 2014, there have been 19 major terrorism disruptions and 129 people charged with relevant terrorism offences in Australia as a result of almost 60 counterterrorism operations. Over that time, the Australian Government has invested an additional $2.3 billion to strengthen our national response and support the outstanding men and women of our security, police and intelligence communities. It is thanks to their efforts that Australians can live safely, enjoying the freedoms we do.

As we learned from the horrific 2019 London Bridge attack and 2020 Streatham attack in the UK, convicted terrorists can pose a very real and ongoing threat to public safety when they are released back into the community after serving their sentences. In Australia, we have introduced a presumption against parole for all convicted terrorist offenders, as well as critical measures providing for the continued detention of high-risk terrorist offenders after the conclusion of their custodial sentences, and control orders, where a court finds that relevant thresholds are met.

With 15 high-risk terrorist offenders due for release in the next five years, the government has sought to further strengthen these laws by introducing a Bill to establish an extended supervision order scheme. The scheme will provide a robust alternative in circumstances where continued detention is not available, ensuring that high-risk terrorist offenders who are released into the community are subject to close supervision in proportion to the level of risk they pose to community safety.

The Australian Government continues to work in partnership with our regional and international allies to assess and counter the threat of terrorism. The government has put in place measures to prevent the travel of Australians to support terrorism abroad and to manage the return of foreign terrorist fighters.

I thank ASPI for its continued leadership in counterterrorism research and I encourage continued analysis and thoughtful dialogue to advance consideration of counterterrorism strategies that strengthen the safety of our communities.

Introduction

LEANNE CLOSE

This 5th edition of ASPIs *Counterterrorism (CT) yearbook* provides a comprehensive picture of the global terrorism landscape, as well as emerging themes and recommended policy responses for governments and communities. Our authors found Covid-19—a key theme in most chapters—to have had an impact on global terrorism. However, pervasive online social media platforms have played a more significant role, increasing terrorists' ability to radicalise and incite individuals to commit terrorist acts, as well as encouraging financial support to terrorist groups.

2021 themes

Global overview

The yearbook begins with an overview of current trends and the terrorism landscape in 2020 identified in the 8th Global Terrorism Index (GTI) produced by Australia's Institute for Economics and Peace. The GTI notes a 50% decrease in terrorism-related deaths in the past five years, from more than 33,000 in 2014 to under 14,000 in 2019. While the impact of radical jihadist terrorism has subsided in the West, there's been a rise in politically motivated terrorism, rising from 13 deaths in 2014 to 90 deaths in 2019 (including 51 people in Christchurch in March 2019). There's now a regional concentration of ISIL-supported activities in South Asia and sub-Saharan Africa. This corresponds, however, with a sharp increase in far-right terrorism in the West, concurrent with the rise of strong nationalism, civil unrest and political violence more generally. Between 2002 and 2014, far-right violence accounted for 14% of total attacks in the West; however, that grew to 40% in 2015 and to 46% in 2019 (49 far-right incidents out of 108 attacks).[1] Statistics in 2020 obviously don't include examples like the 6 January riot on the Capitol in Washington D.C., for example, so 2021 seems set to continue the trend.

The remaining chapters in Part 1 explore the trends identified in the GTI, with a focus on several regions, including the New Zealand historical experience, leading to the Christchurch events in 2019, and an overview of Southeast Asian incidents, with a particular focus on the Philippines and Indonesia.

Christopher Winter and Ramón Spaaij provide an overview of lone-actor attacks and dispel the notion 'that lone actors are truly alone and operate in a social vacuum'. They find that lone actors are usually active in online communities and signal their intent before carrying out their attacks.[2]

Social media and new technologies

Terrorist ideology now attracts larger, more diverse sections of our societies because propaganda and online rhetoric are increasingly sophisticated, making the rapid spread of misinformation and disinformation harder to contain.[3] Anne Aly outlines the intersection of cybercrime with online radicalisation into terrorist activities and calls for a comprehensive approach to CT incorporating online prevention and early intervention strategies.

Conspiracy theorists abound on the internet, and many have used the Covid-19 pandemic, the installation of 5G cell towers and the Black Lives Matter protests, or the US election process, as a catalyst for violent protest or terrorist actions in 2020 and into 2021. Elise Thomas examines this in greater detail, assessing the rapid transition of the 'Boogaloo Bois' from online memes into real-world extremist violence.

Online extremist and fringe groups are gaining more prominence and credence in the real world and are difficult to counter. While several global social media companies have proactively attempted to reduce the exposure and reach of extremist narratives on their platforms, there are limitations. As the live streaming of the Christchurch events in 2019 demonstrates, a recording can be disseminated so widely and rapidly that it's impossible to eradicate. The online spread of propaganda continues to encourage lone actors to commit terrorist acts, which can be planned overseas and enacted locally.[4]

Terrorists' tactics and the impact of emerging technologies are explored in this edition of the yearbook, with a clear acknowledgement that terrorist groups have always embraced new technologies not only to spread their propaganda but also to incite violence. Levi West delves into the history of terrorists' exploitation of technologies, from powerful weapons and extreme tactics to 'low capability tactics such as stabbings and vehicle ramming'.

New technologies, such as unmanned aerial platforms, 3-D printing, artificial intelligence or deep fakes and—of extreme concern—biological agents, can all be exploited by terrorists. The regulation and potential negative impact of new technologies must be constantly and quickly analysed by governments to remain ahead of new developments. That hasn't traditionally been the case; legislation and capability investment to counter emerging terrorist threats has often lagged, causing gaps in efforts to prevent or counter terrorist actions.

The use of hoax devices by terrorists, outlined by Joshua Sinai, also raises serious concerns. Sinai provides a chronology of hoax events from the turn of the century to recent events in 2020, noting that the impact of those hoaxes was as significant as impacts from the use of real weapons.

Levi West notes that the 'exploitation of communications technology has been, and will continue to be, an essential requirement for terrorism to achieve effect'. While online environments have allowed for the acceleration and growth of extremist rhetoric and incitement to violence, Covid-19 has had a compounding effect. Peta Lowe finds this particularly concerning for young people, who are digital natives and have spent much time online during lockdowns.

The Covid-19 pandemic

Several authors highlight attempts by terrorist groups to use the Covid-19 pandemic to legitimise their activities, spread their propaganda and gain community support by providing charity to vulnerable groups. Jeremy Douglas and Niki Esse de Lang show that the terrorist group Jemaah Islamiyah provided family support, health care and welfare to Indonesians following the 2004 Aceh tsunami and the 2006 Yogyakarta earthquake. Recently, the group installed 13,000 charity boxes at marketplaces across Indonesia and has used the pandemic to raise funds for its terrorist activities.[5] Alexandra Phelan shows that terrorist groups in Brazil and Colombia have used the Covid-19 crisis to enhance their own power and legitimacy and provide local support where states have failed to respond effectively.

Lydia Khalil provides a thought-provoking chapter on the impact of natural disasters on violent extremism, highlighting a study of 167 countries over 30 years from 1970, which found that an increase in deaths from natural disasters resulted in an increase in terrorism-related deaths and attacks in the following two years.[6] The researchers suggested that the turmoil caused by emergencies exacerbated vulnerabilities that terrorists then exploited. Khalil also points to recent research showing that the portrayal of government responses to natural disasters affects subsequent terrorism activities because poor disaster and emergency management, or the perception of it, can exacerbate existing grievances and manifest as terrorism or violent extremism.[7] Government responses to Covid-19, therefore, have the potential to sharpen grievances about social and economic inequality in coming years and to provoke further violent extremism.

Terror financing and the organised crime nexus

The 5th edition of the yearbook contains a new theme focused on the global challenges of countering terrorism financing and the nexus between terrorism and organised crime. The GTI estimated that the economic impact of terrorism was as high as US$104 billion in 2014, declining to US$26.4 billion in 2019. This is the fifth consecutive year that it has declined, and the authors assert that the improvement over the past four years has been driven largely by the declining level of terrorism in Iraq, Nigeria, Pakistan and Syria.[8]

Gordon Hook explores the UN requirements for and global efforts aimed at reducing terrorist financing through the work of the Financial Action Task Force (FATF). Fundraising by terrorist groups has grown to range from small remittances by supporters to large-scale sales of oil and gas, investment in real estate and offshore tax havens, to counterfeit medical drugs during the pandemic. While a reduction in the estimated economic impact of terrorism financing is encouraging, the FATF reports that there are fundamental gaps in legal frameworks and compliance endeavours globally, leading to very few convictions for terrorist financing.

Sylvia Laksmi assesses the opportunities for greater global collaboration to diminish terrorist money flows in her review of the counter-terrorism-financing partnership between Indonesia and Australia. Her chapter highlights the abuse of funds donated to charities, the risks associated with new digital currency platforms and the requirement for appropriate mechanisms to be implemented to verify the digital identities of customers.

John Coyne, Daria Impiombato and Alexandra Phelan analyse the role of organised crime activities, such as drug distribution,[9] in funding terrorist actions. The 2018 edition of the GTI explored this issue, finding in a study of 13 countries that more than 45% of terrorist recruits had criminal backgrounds. The study with the largest sample was of ISIL foreign fighters from Germany; it found that 66% of the 778 foreign fighters had prior criminal convictions. The second largest study made a similar finding; 64% of 319 foreign fighters and ‘would be’ foreign fighters from the Netherlands had criminal backgrounds.[10] Analysis of their motivation allows policymakers and investigators an opportunity to consider other methods to target their activities.

In Australia, the facilitation of terrorism and organised crime funding, for example through real estate, offshore tax havens and other money-laundering activities, should be addressed through Australia’s long proposed anti-money-laundering and counter-terrorism-financing (AML/CTF) legislation focused on real estate agents, lawyers and accountants.[11] Recent amendments to Australia’s AML/CTF legislation didn’t address this significant legislative gap.[12] Phelan makes the case that governments, which are responsible for economic regulation and protection, should limit the ability of individuals and terrorist groups to launder money, legitimise their criminal financing activities or move funds to special tax havens.

Preventing and countering violent extremism

The final section of the *CT yearbook* focuses on strategies being applied in preventing and countering violent extremism (P/CVE). Community resilience is a key topic discussed in those chapters. The impact of the devastating bushfires in Australia and the global Covid-19 pandemic provided strong examples of community resilience and lessons for CT practitioners throughout 2020.

Michele Grossman finds that resilience to terrorism is evolving as communities experience and recover from various crises and disasters. She stresses that resilience is a social process involving health, education, cultural, legal, economic and environmental strategies, complemented by interventions focused on an individual or group. Likewise, current CT practitioners in NSW, Victoria and the Australian Federal Police highlight the importance of well-coordinated P/CVE strategies as well as alliances between social science researchers, non-government organisations, governments and law enforcement and intelligence agencies to inform evidence-based decision-making on the intent, motivation and ideological drivers to violent extremism (see the contributions from Pia van de Zandt et al.; Aftab Malik and Madeleine Coorey; Ross Guenther and Debra Smith; Peta Lowe; and Natalie Davis and Sandra Booth).

Boaz Ganor examines lessons from Israel’s focus on CT over many decades and the strength of the role of the Counter-Terrorism Coordinator. The coordinator oversights the country’s CT activities, reporting directly to the Prime Minister and providing an effective mechanism for a constant focus on and enhancement of CT and P/CVE strategies. The importance of maintaining and regularly reviewing Australia’s Counter-Terrorism Strategy and coordination framework, led by an independent and properly supported national security adviser, is crucial for ensuring that the focus is maintained and that coordination and capability development are continuously assessed and enhanced across state and territory boundaries.

This coordination effort is increasing in importance as terror risks in Australia expand. Multiple terrorism offenders are scheduled for release from prison over the next five years, and right-wing extremists are becoming increasingly organised and sophisticated.[13] Our authors agree that the key to effective P/CVE strategy implementation is building trust and transparency in process and decision-making, as well as engaging individuals and various community sectors in design and delivery.

Conclusion

Each author in the 2021 *CT yearbook* provides governments and CT practitioners with contemporary analysis of current and emerging challenges and offers key policy recommendations. Emerging technologies need to be monitored for the potential for their use by terrorists. Technologies and methods for the funding of terrorist groups also need constant monitoring and agile regulatory responses.

The findings of the New Zealand Royal Commission of Inquiry into the Attack on Christchurch Mosques on 15 March 2019,[14] released in December 2020, also provide a strong framework for governments throughout the world to consider when developing CT strategies. While the commission recommended some tactical legislative changes, for example in firearms and hate crimes regulation, it emphasised a strong focus on leadership and building community cohesion, as well as embracing diversity.

Covid-19 has resulted in significant funding for important health and economic responses. While that funding may concurrently support P/CVE strategies, addressing broader radicalisation factors such as socio-economic inequality must remain a focus. P/CVE work must be further supported to develop it into a whole-of-systems approach encompassing all actors involved in the prevention of terrorism, including governments, communities and businesses. Effective state governance and credible institutions, maintaining the rule of law and building or sustaining trust in government and its systems are crucial for combating the activities of terrorists and delegitimising their actions in the eyes of the community.

Notes

1 Institute for Economics & Peace (IEP), *Global Terrorism Index 2020: measuring the impact of terrorism*, November 2020, online.

2 M Hamm, R Spaaij, *The age of lone wolf terrorism*, Columbia University Press, 2017, 91, online.

3 Katja Theodorakis, Leanne Close, *The impact of the Covid-19 pandemic on extremism dynamics: towards national resilience*, ASPI/KAS, Canberra, 8 December 2020, online.

4 Theodorakis & Close, *The impact of the Covid-19 pandemic on extremism dynamics*.

5 Anugrah Kumar, 'Indonesia: Al-Qaeda linked terrorists use thousands of fake charity boxes to raise funds', *The Christian Post*, 14 December 2020, online.

6 Claude Berrebi, Jordan Ostwald, *Earthquakes, hurricanes, and terrorism: do natural disasters incite terror?*, RAND Corporation, Santa Monica, 2011, online.

7 Daren Fisher, Laura Dugan, 'The importance of governments' response to natural disasters to reduce terrorist risk', *Justice Quarterly*, 2019, doi: 10.1080/07418825.2019.1685120.

8 IEP, *Global Terrorism Index 2020*.

9 'Italian police seize 14 tonnes of amphetamines allegedly produced by Islamic State', *ABC News*, 2 July 2020, online.

10 IEP, *Global Terrorism Index 2018*, online.

11 'Greens additional comments: Um, tranche 2?', Senate Standing Committees on Legal and Constitutional Affairs, Australian Parliament, 2019, online.

12 Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019, Australian Parliament, online.

13 Mike Burgess, statement to Senate Legal and Constitutional Affairs Committee, Budget Estimates, 20 October 2020, online.

14 Royal Commission of Inquiry into the Attack on Christchurch Mosques on 15 March 2019, *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019*, 8 December 2020, online.

Global Terrorism Index 2020: the shifting landscape of terrorism

THOMAS MORGAN
Senior Research Fellow, Institute for Economics and Peace
Sydney, Australia

OLIVIA ADAMS
Research Fellow, Institute for Economics and Peace
Sydney, Australia

DR DAVID HAMMOND
Director of Research, Institute for Economics and Peace
Sydney, Australia

Measuring the impact of terrorism

Measuring the impact of a phenomenon as complex as terrorism is challenging. However, without the ability to gauge levels and trends, it's difficult to have an informed discussion of the shifting landscapes of terrorism. The 2020 Global Terrorism Index (GTI), now in its eighth year, was designed to provide just that kind of base measure. This article provides a comprehensive summary of the key global trends and patterns in terrorism and places a special emphasis on trends since 2014, which corresponds with the start of the fall of the Islamic State of Iraq and the Levant (ISIL).

The GTI is produced by the Institute for Economics & Peace (IEP) using data from the Global Terrorism Database (GTD) and other sources. Data for the GTD is collected and collated by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland. The GTD contains more than 170,000 terrorist incidents for the period from 1970 to 2019.

The GTI ranks 163 countries based on four indicators weighted over five years. A country's annual GTI score is based on a unique scoring system to account for the relative impact of terrorist incidents in the year. Four factors are counted in each country's yearly score:

- the total number of terrorist incidents
- the total number of fatalities caused by terrorism
- the total number of injuries caused by terrorism
- the approximate level of total property damage from terrorist incidents.

Each of the factors is weighted differently, and a five-year weighted average is applied to reflect the lingering psychological and cultural impact of terrorist acts over time. By generating and synthesising new information on evolving trends in terrorism at the national and global levels, IEP hopes to inform a positive, practical debate about the future of terrorism and the required policy responses.

Global trends

The past five years have seen a large decrease in terrorism across the globe. Deaths from terrorism declined steadily, from more than 33,000 in 2014 to just under 14,000 in 2019—a 59% reduction. The largest decreases occurred in Iraq and Syria, while deaths in Nigeria fluctuated over time. The winding down of the Syrian civil war, the territorial defeat of ISIL and increased counterterrorism coordination at both state and international levels have all played a role in reducing the impact of terrorism around the world.

In the West, terrorist attacks and deaths from terrorism peaked slightly after the global peak of incidents in 2015, when 340 attacks were recorded, and deaths peaked in 2016 when 233 people died in terrorist attacks. Although the impact of radical jihadist terrorism has subsided in the West, there's been a rise in the level of politically motivated terrorism. The number of deaths from politically motivated terrorism in the West has increased significantly over the past five years, rising from 13 deaths in 2014 to 90 deaths in 2019.

The impact of terrorism lessened in seven of IEP's nine global regions in 2019. This matches the trend for the world as a whole, which has recorded a consistent decline in terror-related deaths and incidents. The largest improvement occurred in the Middle East and North Africa (MENA) for the second consecutive year. South Asia had the largest deterioration, followed by Central America and the Caribbean. The deterioration in South Asia was predominantly caused by the large increase in deaths in Sri Lanka as a result of the Easter Sunday bombings, which killed more than 266 people and injured at least 500.

Although the MENA region has recorded the highest number of deaths from terrorism since 2002 (more than 96,000 deaths in total), the region has recorded a substantial decline in the past three years. Deaths in MENA have fallen by 87% since peaking at 13,800 in 2016, reaching the lowest level since 2003. More recently, terrorist activity has been concentrated in South Asia and sub-Saharan Africa, both of which recorded more terrorism deaths than MENA in 2018 and 2019. Collectively, South Asia and sub-Saharan Africa accounted for over 80% of all terrorism deaths in 2019 (6,583 and 4,635 deaths, respectively).

Terrorism in 2019

The total number of deaths from terrorism declined for the fifth consecutive year in 2019, falling by 15% compared to 2018, to 13,826 deaths. The fall in terrorism deaths wasn't restricted to a single region: the MENA, Russia and Eurasia, South America and South Asia regions all recorded falls in deaths from terrorism of at least 20% from 2018 to 2019.

Deaths from terrorism fell in 46 countries, and Afghanistan recorded the largest year-on-year reduction. Since the peak of violence in 2018, deaths from terrorism in Afghanistan have fallen by 1,654, or over 22% in a year. This was driven by a decline in terrorism deaths attributed to the Taliban and the Khorasan Chapter of Islamic State; 1,111 and 494 fewer deaths were attributed to each group, respectively. The Khorasan Chapter of the Islamic State has faced significant territorial losses in Kunar and Nangarhar provinces following attacks by coalition and Taliban forces. Despite the fall in terrorism deaths, 2019 was the second deadliest year on record after 2018, and Afghanistan remains the country most affected by terrorism, as measured by the 2020 GTI.

Countering the overall fall in terrorism deaths, several sub-Saharan African countries recorded significant rises in terrorism deaths in 2019. Burkina Faso recorded the largest increase; the number of people killed in terror attacks rose from 86 in 2018 to 593 in 2019. Mozambique, the Democratic Republic of the Congo and Mali all recorded an additional 100 terrorism deaths from 2018. Much of the increase in terrorist activity can be attributed to the proliferation of jihadist groups throughout the region, including newly established ISIL provinces and affiliates as well as groups aligned with al-Qaeda. In particular, Burkina Faso and Mali have seen a sharp increase in terrorism deaths attributed to Jamaat Nusrat al-Islam wal Muslimin, which is an affiliate of Al-Qaeda in the Islamic Maghreb, and the Islamic State in the Greater Sahara, along with other extremist groups and militias that appear to be gaining influence in the Sahel region by exploiting existing ethnic tensions.[1]

The global expansion of ISIL

While ISIL has been severely weakened, it hasn't been eliminated. Instead, the group's global provinces and affiliates have become increasingly deadly in some countries, indicating the strength of ISIL's global brand of terrorism beyond Iraq and Syria—and that's been in parallel with a collapse in the number of deaths attributable to the ISIL core in Iraq and Syria as a result of the group's territorial defeat (from a peak of more than 8,907 in 2016 to some 611 in 2019).

Deaths attributed to ISIL provinces and affiliates peaked in 2015 at 3,769 and have since fallen to 1,784 in 2019—a fall of more than 2,000 deaths in four years. Although ISIL-related terrorism as a whole has begun to decrease in the past few years, ISIL-related deaths are still 36% higher than in 2013, when the group first emerged. With the proliferation of ISIL provinces and affiliates around the world, and the concurrent demise of ISIL in Iraq and Syria, provinces and affiliates now record more terrorism deaths a year. In 2019, ISIL provinces and affiliates accounted for 74% of 2,396 ISIL-related terrorism deaths.

Since their first emergence in 2013, ISIL-related groups and individuals have mounted more than 3,000 attacks in 48 countries, other than Iraq and Syria, and caused over 12,000 fatalities. The number of countries experiencing ISIL-related attacks each year has steadily increased from two in 2013 to 27 in 2019, including Mozambique and Sri Lanka, which recorded ISIL-related attacks for the first time. Countries such as Burkina Faso, the Democratic Republic of the Congo, Mozambique and Niger have all recorded sharp rises in terrorist attacks with the emergence of several new ISIL provinces and affiliates (the Central Africa Province of the Islamic State and the Islamic State in the Greater Sahara), and the expansion of existing groups, namely the Islamic State West Africa Province (ISWAP), into neighbouring countries.

The emergence of new ISIL provinces and affiliates and the problems of the ISIL core have led to a regional shift in which ISIL-related terrorist activity is now concentrated in South Asia and sub-Saharan Africa. By 2019, ISIL-related terrorism in sub-Saharan Africa accounted for 41% of the total, or 982 deaths, while South Asia accounted for 25% of the total, with 596 fatalities.

In sub-Saharan Africa, ISIL-related terrorism has predominantly been driven by ISWAP, which has been the deadliest ISIL province since it emerged in 2015. Formally a part of Boko Haram, the group pledged allegiance to ISIL and was accepted as a regional province in March 2015, when it subsequently renamed itself ISWAP.[2] In 2016, a dispute over the leadership of ISWAP resulted in the emergence of two factions of the group; while one faction continued to operate as ISWAP, the other faction reverted to the use of Boko Haram's formal name, Jama'atu Ahlis Sunna Lidda'awati Wal-Jihad.[3]

In South Asia, the increasing trend of ISIL-related deaths was driven by the Khorasan Chapter of the Islamic State. The group was responsible for 3,134 terrorism deaths between 2015 and 2019, or 89% of the region's ISIL-related deaths. Of the 596 ISIL-related terrorism deaths in South Asia in 2019, more than half were attributed to the Khorasan Chapter in Afghanistan, India and Pakistan. The remaining deaths were the result of the deadliest terror attack of the year when eight coordinated suicide bombings were conducted across Sri Lanka on Easter Sunday. The bombings, which killed more than 266 people, were allegedly carried out by National Thowheeth Jama'ath, a previously unknown group that pledged allegiance to former ISIL-leader Abu Bakr al-Baghdadi.[4]

Far-right terrorism and political violence

There's also been a sharp increase in far-right terrorism in the West, concurrent with the rise of populism, civil unrest and political violence more generally. This increase has been the focus of intense political and media scrutiny, particularly after a number of high-profile attacks in 2019. In March 2019, a lone gunman attacked two mosques in Christchurch, New Zealand, killing 51 people and injuring a further 49. Five months later in El Paso, Texas, another lone gunman shot and killed 23 people and injured 23. In total, 89 of the 108 deaths from terrorism in the West in 2019 were inflicted by far-right extremists.

Far-right terrorism has also been growing as a proportion of total terrorism in the West. Between 2002 and 2014, far-right incidents never accounted for more than 14% of total attacks in the West, or no more than 16 attacks in a year. However, that number grew to 40% in 2015, to 55 attacks out of 139, and had risen to 46% by 2019 to 49 far-right incidents recorded out of 108 attacks.

The US recorded the highest number of deaths from far-right terrorism, or 113 deaths since 2002. Norway had the second highest number of deaths at 78, of which 77 occurred in a single day when Anders Behring Breivik carried out the 2011 Norway attacks. New Zealand had the third highest number of deaths with 51, all of which occurred during the Christchurch mosque shootings in 2019. The US is the only country in the West to have experienced multiple attacks resulting in more than 10 deaths; three such attacks have occurred since 2002.

Much of the discourse about far-right terrorism, and extremism more generally, has focused on the threat that far-right groups pose to civil society. However, most far-right terrorist attacks are carried out by 'lone-wolf' actors who aren't affiliated with a specific terrorist group or far-right organisation, even if they may have had contact with other far-right individuals or been inspired by other far-right attacks. This shift from affiliated to unaffiliated terrorism and online rather than in person radicalisation has also been seen across most other forms of ideologically driven terrorism in the West.

The prevalence of unaffiliated far-right terrorism is even higher when looking at terrorist attacks that result in at least one death. From 2002 to 2019, there were 52 far-right attacks that resulted in at least one fatality. Of those, only seven were attributed to a specific group, while all the attacks that occurred in the past decade were classified as unaffiliated.

This doesn't mean that far-right terrorists have no contact with extremist organisations, or that the radicalisation of far-right individuals occurs entirely in isolation. Contact with like-minded individuals can be a significant factor in the radicalisation process and has traditionally been a strong predictor of whether a person will engage in violence.

Conclusion

Terrorism and violent extremism co-evolve with political, technological and social changes. The GTI provides a comparable metric to conduct analysis and observe trends. Understanding these shifting landscapes allows PVE, CVE and CT policymakers to:

- focus attention on what's increasing
- investigate how recruitment strategies are evolving
- discuss areas of actions.

Notes

1 Bureau of Counterterrorism, *Country reports on terrorism 2019*, Department of State, US Government, 2020, online.

2 Australian Government, 'Islamic State West Africa Province', *Australian National Security*, no date, online.

3 Australian Government, 'Islamic State West Africa Province'.

4 Thomas Joscelyn, 'Terrorists in Sri Lanka swore allegiance to Abu Bakr al-Baghdadi', *FDD's Long War Journal*, 23 April 2019, online.

Terrorism in New Zealand: how a different approach might have prevented the Christchurch mosque attacks

DR JOHN BATTERSBY
Teaching Fellow, Centre for Defence and Security Studies, Massey University
Wellington, New Zealand

‘Terrorism’ is an abstract noun applied collectively because of the common characteristics of terrorist organisations, groups, cells and individuals. But its collective nature is also problematic, because those same terrorist organisations, groups, cells and individuals are the product of specific historical, social and political contexts. They present in different and nuanced ways depending on the circumstances in which they have emerged. Terrorism in New Zealand has similarities but also distinct differences from Australia’s and other terrorist actions further afield. This paper outlines that nuanced terrorism experience and considers why New Zealand has struggled to take terrorism seriously for half a century, leaving a historical legacy of dragging the chain when it comes to countering terrorism. For the future, the country must break this habit to more effectively combat terrorism.

International influences on terrorism in New Zealand

Over the past 50 years, terrorism in New Zealand has tended to follow some international trends. The movements against the Vietnam War, nuclear concerns and apartheid all emerged overseas as popular protest movements associated with violent activity. New Zealand emulated those trends, although terrorism tended to be less frequent with less severe consequences than in other countries.

In 1970, more than a dozen bombings were carried out in New Zealand by anti-war activists targeting military and government buildings, and the attacks continued at a lower frequency in following years.[1] Much like in Australia in the early 1970s, those terrorist acts caused no deaths and the perpetrators weren’t readily labelled as ‘terrorists’.[2] However, the link between civil or popular unrest and terrorists on the fringes of those movements was already a noticeable theme when it occurred again during the South African Rugby Union Team’s tour to New Zealand in 1981. Along with widespread protests came several bombings, as well as bomb and death threats against players, Rugby Union officials and police.

Overall, the terrorists were usually, although not exclusively, on the far left of politics, and their acts and intentions were almost tacitly accepted as an extension of protest. The lack of any counterterrorism legislation suggested an inability or unwillingness by New Zealanders to clearly understand what terrorism was, and governments certainly appeared to have no obvious desire to do anything about it, given that public sentiment. The convoluted definition of terrorism in New Zealand’s *Terrorism Suppression Act 2002* (TSA), which remains largely unchanged since its enactment, suggests a continuing lack of clarity in New Zealand about what terrorism is considered to be.

Internationalised terrorism surfaced in New Zealand in 1975 when a few followers of New Zealand’s small chapter of the Ananda Marga sect were caught in a plot to bomb the Indian High Commission.[3] Ten years later, the French Directorate-General for External Security bombed the Greenpeace flagship *Rainbow Warrior* in Auckland Harbour.[4] A cabinet paper in 1985 declared that the *Rainbow Warrior* incident showed New Zealand wasn’t immune from terrorism, as if the events of the 1970s had never happened. In March 2019, multiple commentators and media sources again declared that New Zealand’s immunity from terrorism had come to an end, even though no such ‘immunity’ had ever really existed.

Terrorism in New Zealand has often occurred as dispersed single events. One event fades from memory by the time a subsequent event occurs, leading to the recurring belief (illusory though it is) that some form of immunity from terrorism exists. The severity of the 15 March 2019 attack, when 28-year-old Australian terrorist Brenton Tarrant brutally murdered 51 people at two mosques in Christchurch, has broken that illusion.

New Zealand’s nuanced terrorism

New Zealand has always shown a propensity to generate its own unique causes for political violence, in unusual or unexpected circumstances and with very nuanced targets. The institution of 6 o’clock closing of public houses after World War I prompted bombings in 1919, and again in 1932 in Greymouth.[5] Mining strikes involved the bombing of a railway line in Denniston in 1913 and a railway bridge in Huntly in 1951.[6] In 1976, two followers of the Hare Krishna movement planned to bomb a meatworks, but accidently killed themselves when their bomb detonated prematurely in Auckland.[7] In 1981, a troubled youth with a penchant for criminal acts connected with political messaging deliberately located himself along Queen Elizabeth II’s route during her visit to Dunedin and fired a shot with a stolen .22 rifle.[8] The following year, a punk-rock anarchist bombed the Police National Computer Centre in Wanganui, deliberately killing himself as he did so.[9] The 1981 shooter and the 1982 bomber had both previously been involved in Springbok tour anti-apartheid protests. Both leaked their intentions to associates, but no one reported them, and their defining acts were discovered only after the fact. In 1984, an unknown perpetrator left a bomb in Wellington’s Trades Hall; the bomb detonated and killed the building’s caretaker. The political nature of the target strongly suggests a political motive, but the case has never been solved.[10]

New Zealand didn’t have any terrorist legislation until after the *Rainbow Warrior* bombing, so calling any of those events ‘terrorism’ has been intermittent. Commentators sympathetic to the bombers have avoided the term altogether, preferring to idolise them more often as heroic actions for noble, protest-related, causes. The desire for a pejorative label for the actions of the *Rainbow Warrior* bombers, however, saw them widely labelled as terrorists. The same is true of the 2019 Christchurch killings perpetrator: New Zealanders have readily used the term to distance themselves from him, rather than understanding how the New Zealand legal definition of terrorism applied to his actions.

In 2007, New Zealand Police terminated a surveillance operation (Operation Eight) that targeted activists for a range of causes.[11] Police cited the TSA as their key legal instrument for proceeding. The affidavit supporting the application for search warrants for Operation Eight clearly evidenced multiple references in electronic intercepts of those under surveillance to starting a 'race war', proposing assassinations and bombings, discussions about the acquisition of semi-automatic weapons and ammunition, and camps where 'training' with those weapons occurred, including the preparation of Molotov cocktails and other 'tactical training'.[12]

Despite multiple arrests, the Solicitor-General didn't authorise charges under the TSA, stating that the wording of the Act was too complicated for the evidence collected to meet the legal criteria required. It wasn't for any lack of evidence that charges weren't laid: the Solicitor-General publicly stated that it was the tautology of the Act that led to his decision not to charge:

> The fundamental problem is that the legislation focuses upon an entity that carries out a terrorist act, and if individuals are actually developing towards … carrying out a terrorist act, they aren't yet an entity that is carrying out a terrorist act, and so there is a tautology in the legislation which is extremely difficult to unravel.[13]

The media interpreted the Solicitor-General's decision as a failure on the part of the New Zealand Police to substantiate their suspicions.[14] Political leaders distanced themselves from both the police investigation and the decision not to prosecute. Supporters of those arrested usurped the public narrative, depicting the suspected perpetrators as the victims of a heavy-handed police over-reaction. Academic and independent commentary failed to balance the 'debate'.[15] The fact that a successful detection and surveillance operation had potentially disrupted a dangerous evolving threat was overlooked, and addressing the shortfalls of the TSA was quietly side-lined. That experience set the context for counterterrorism in New Zealand leading up to New Zealand's worst terrorist attack 12 years later, in 2019.

Legislative and systemic shortfalls

In the 12-year time lapse between 2007 and 2019, successive New Zealand governments failed to review and repair the TSA. Despite the international evolution of terrorism towards actions by individualistic and impulsive cyber-activated adherents of extreme ideologies who are geographically dispersed and disconnected, no updates were made to the TSA to address the possibility that this new brand of terrorism might occur in New Zealand. Foreign terrorist fighter (FTF) legislation lagged behind the phenomenon and initially neglected any concern that New Zealand FTFs might return home.[16] New Zealand had very few of them, and the fear of their return in most countries was far greater than the reality of the risk they posed when they did, but nowadays lone actors are highly effective and dangerous. Historically, with the exceptions of the Vietnam War and Springbok tour periods, terrorism in New Zealand generally only involved one or a few individuals in single, non-sequential and unconnected acts of violence.

The Operation Eight experience produced an opportunity to address what were clear deficiencies in New Zealand's firearms regulations that had so easily allowed those suspects to acquire arms and ammunition. If this wasn't enough, there were further warning signs. A man with a cache of firearms, including semi-automatic weapons, shot three police officers and a civilian (killing one officer and then himself) in Napier in 2009. The subsequent coronial inquiry called for a review of the Arms Act and careful reconsideration of the 1996 Thorp Inquiry report.[17] Thorp recommended a firearms licensing and registration regime similar to Australia's in the wake of the Port Arthur massacre. The recommendations were deemed too expensive to implement in 1996 and, despite the subsequent coronial recommendation, weren't implemented. A firearms register may have alerted police to Tarrant's rapid acquisition of semi-automatic weapons and thousands of rounds of ammunition. A more restrictive regime might have prevented him acquiring those items. New Zealand's firearms licensing regime had long been under-resourced, and former officers have recently come out critical of New Zealand Police's own lack of commitment in properly administering it.[18]

In 2015, reporter Heather Du Plessis-Allan demonstrated how easy it was to obtain a firearm without a licence, publicly reporting her own illegal internet purchase of a .22 rifle from a Gun City store. Ironically, the police subsequently executed a search warrant on her home and investigated her illegal action, while the store owner she purchased the gun from labelled her a 'terrorist'![19] The irony deepened when it came to light that it was a Gun City store, operating within the laws and regulations in force, that had sold Tarrant four of his firearms as well as ammunition prior to the 15 March 2019 attacks.[20] In the absence of political leadership, loopholes in legislation and an administrative malaise meant natural resistance points that might have upset Tarrant's preparations were diluted. Multiple opportunities to take steps to prevent the development of modern modes of terrorism in New Zealand were simply never taken. It is hoped that may now change.

Hope for the future

The Royal Commission of Inquiry into the attack on Christchurch Mosques was set up with an ambitious completion date in December 2019, which it was unable to meet. The report was made public in December 2020 and provides comprehensive recommendations, including establishment of a new National Security and Intelligence agency focused on coordinating counterterrorism efforts. While the Royal Commission's terms of reference were quite narrow, it has delved into commentary focusing political, resourcing or legislative decisions that ultimately influenced the actions of the specific agencies under review. Those agencies were criticised variously, but importantly no intelligence failure or act or omission was found that would have prevented the 2019 attacks.

The Royal Commission of Inquiry Report is detailed and needs to be properly considered before an informed assessment can be made. Certainly, whether additional bureaucracy is actually required is questionable but, for the future, the recommendations recognise broader strategic concerns must be dealt with. The Royal Commission has called for deficiencies in legislation, coordination of effort and agency resources to be addressed and it would be remiss of the New Zealand government not to do so. New Zealand's recently launched counterterrorism strategy was a positive step, but a tentative one. The strategy document is thin on detail and more substance is required for it to set out a genuinely useful path for the future.[21] The findings and recommendations of the Royal Commission provide the opportunity for the New Zealand government, collaborating with the community, to set out on this pathway.

Notes

1 John Battersby, 'The ghost of New Zealand's terrorism: past and present', *National Security Journal*, 2019, 1(1):35–48.

2 Sean Brawley, '"Days of rage" downunder: considering American influences on "home-grown" terrorism and ASIO's response in 1970s Australia', *Australian Historical Studies*, 2016, 47(2).

3 John Battersby, 'Can old lessons inform current directions: Australia, New Zealand, and Ananda Marga's trans-Tasman "terrorism" 1975–1978', *Studies in Conflict and Terrorism*, 2019.

4 James Veitch, 'A sordid act: the Rainbow Warrior incident', *New Zealand International Review*, 2010, 35(4):6–9.

5 'Dastardly act: Explosion at Denniston', *Evening Post*, 11 November 1913, National Library of New Zealand (NLNZ); 'Beer bombings: files released', *Otago Daily Times*, 4 November 2017, online.

6 'Attempt to blow up bridge', *The Dominion*, 1 May 1951, NLNZ.

7 'Death blast linked to bomb plot', *New Zealand Herald*, 15 May 1976, NLNZ.

8 Christopher John Lewis, *Last words*, The Moon Productions, Auckland, 1997, 72–79.

9 Battersby, 'The ghost of New Zealand terrorism', 38.

10 Thomas Manch, 'Trades Hall bombing evidence points to a key suspect, retired marine engineer Edgar Kidman', *Stuff.co.nz*, 16 July 2019, online.

11 'The terrorism files', *The Dominion Post*, 14 November 2007. This report and others associated with it were removed from this media sources website after it was prosecuted for publishing material from the leaked affidavit. I sourced from hard copy held at NLNZ.

12 'Affidavit of Detective Sergeant Aaron Pascoe', NZ Police, 10 October 2007, obtained under Official Information Act request, 2018.

13 'Act too complex to use, says Collins', Dominion Post, 31 January 2009.

14 John Battersby, 'Security sector practitioner perceptions of the terror threat environment before the Christchurch attacks', *Kotuitui: New Zealand Journal of Social Sciences Online*, 2020, 15(2):299.

15 Danny Keenan (ed.), *Terror in our midst: searching for terror in Aotearoa New Zealand*, Huia, Wellington, 2008.

16 Battersby, 'Security sector practitioner perceptions', 300.

17 'Call for Arms Act review after Napier siege', *Dominion Post*, 3 September 2010.

18 'Police bosses accused of neglecting firearms control for years, as Government plans new arms authority', *Stuff.co.nz*, 22 June 2020, online.

19 Shabnam Dastgheib, 'Reporter's gun purchase "like a terrorist activity"', *Stuff.co.nz*, 22 October 2015, online.

20 'Gun City sold Brenton Tarrant four guns and ammunition', *Otago Daily Times*, 18 March 2019, online.

21 Countering terrorism and violent extremism national strategy, Department of Prime Minister and Cabinet, February 2020, online; see John Battersby, Rhys Ball, Nick Nelson, 'New Zealand's Counter-Terrorism Strategy: a critical assessment', *National Security Journal*, 2020, 2(1):79–96.

Lone actor terrorism in 2019 and 2020: trends and implications

CHRISTOPHER WINTER
PhD Candidate, Victoria University
Melbourne, Australia

RAMÓN SPAAIJ
Sociologist, Victoria University and University of Amsterdam
Melbourne, Australia

Terrorist attacks by lone individuals aren't a new feature of the contemporary security environment, and the decade leading up to 2019 saw the widespread adoption of the tactic. However, the threat posed by terrorism is never a static one, as would-be terrorists shift their tactics, targets and messaging in the context of wider security, political and cultural environments.

The years 2019 and 2020 involved a continuation of many of the trends witnessed over the past decade. Europe continued to experience the threat of low-tech, low-effort, close-combat attacks against seemingly random targets, such as in the 2019 London Bridge stabbing attack. However, a significant number of attacks were by heavily armed perpetrators who displayed relatively sophisticated targeting and operational capabilities. Further dispelling the notion that lone actors are truly alone and operate in a social vacuum, those terrorists were often active in online communities, sometimes signalling their intent before carrying out their attacks, and also wanting online validation from extremist 'fellow travellers' after the act.[1] Moreover, attacks by non-political, idiosyncratic or poorly articulated perpetrators have continued to be a threat.

In this chapter, we discuss recent international developments in lone-actor terrorism, with a focus on how lone-actor terrorists operationalise their attacks and the policy implications of these developments in the Australian context. Understanding the constantly shifting threat of how lone-actor terrorism is operationalised is essential in understanding how it may be interdicted and prevented.

The decade before: 2009 to 2018

Lone-actor terrorist violence isn't a new threat: the mid-1990s were a period of heightened far-right violence in the US.[2] In the post-9/11 period, the perceived terrorist threat shifted to organised conspiracies from various religious groups, although lone-actor terrorist attacks remained a constant, if relatively low-level, threat.

If we can accept the idea that terrorism can emerge in 'waves' of ideological and operational similarities, then the years between 2009 and 2012 framed a rising tide of lone-actor violence globally. Increasing in both frequency and societal impact in comparison to any period before then, those attacks were carried out by perpetrators informed by a variety of ideologies and using equally varied levels of operational sophistication.[3] Examples include the 2009 Fort Hood shooting, the attempted knife assassination of British parliamentarian Stephen Timms and the 2011 Frankfurt Airport shooting.

The period from 2013 to 2018 marked another escalation in the prevalence of lone-actor terrorist attacks. That increase largely coincided with the rise of the self-titled Islamic State. At the same time, the relative sophistication and complexity of attacks decreased, as many perpetrators eschewed sophisticated attack plans or long periods of preparation to instead opt for low-effort, quickly actioned attacks. Often, the weapons used were little more than kitchen knives. Dozens of attacks were performed in this manner, mostly in Europe and particularly in France. Both al-Qaeda and ISIS recognised the utility of low-tech attacks. Indeed, in a 2016 issue of Al-Qaeda in the Arabian Peninsula's *Inspire* magazine, an article titled 'O Knife Revolution, head towards America' called for a series of knife attacks against various targets, including Jewish people.[4] Australia also experienced several such incidents: the 2014 Endeavour Hills stabbing, the 2016 Minto stabbing, the 2018 Mill Park stabbing and the 2018 Bourke Street stabbing. One analysis has found that internationally (excluding the US), close-combat weapons were the preferred weapon of lone-actor terrorists, being used in 56% of all attacks. Although those attacks killed relatively few people, the short planning period and the unpredictability of target selection meant that security forces were responding to attacks in progress, rather than disrupting them during the planning or preparation stages. That unpredictability was a key element in a shift towards the promotion of concepts such as 'open-source jihad' by groups such as al-Qaeda and, subsequently, by ISIS.[5]

The use of vehicles as a weapon was also a significant attack method during that period. The 2016 Nice truck attack, although not conducted by a lone actor, was the most devastating of those attacks and a powerful illustration of the possible impact of attacks using vehicles as weapons.

This period also included some of the worst lone-actor terrorist mass shootings in history. The 2011 multi-stage attack in Oslo and Utøya Island by Anders Behring Breivik and the 2016 Pulse nightclub shooting in Orlando demonstrated the potential for well-armed lone actors to inflict serious harm. In the Breivik case, the in-depth Gjørv report commissioned by the Norwegian Government identified several missed opportunities when security services could have interdicted the perpetrator as he prepared for his attack, among other failings in responding to a mass shooting incident. Of great concern is also the fact that other would-be lone actors were inspired by Breivik's attack.

The Christchurch cluster

On 15 March 2019, Brenton Tarrant, an Australian citizen living in New Zealand and armed with several firearms, shot and killed 51 people and wounded another 40 during afternoon prayers at two mosques in Christchurch. Before his attack, like Breivik, Tarrant published a manifesto in which he provided justifications for his actions and explained his targeting process.[6] Indeed, while Tarrant specifically cited Breivik as his 'true inspiration' ideologically, both attacks shared strong operational similarities. Both perpetrators went through a years-long planning phase, carefully selecting their chosen victims on the basis of the victims' availability, symbolic importance and vulnerability. Both considered a variety of attack methods that would maximise their ability to inflict harm, and both used semi-automatic rifles.

Just as the Utøya attack served as a model for Christchurch, elements of the Christchurch attack would directly inspire several other attacks in 2019. Those attacks included the Poway synagogue shooting in California (1 killed, 3 injured),[7] the Walmart shooting in El Paso,[8] Texas (23 killed, 23 injured), the Al-Noor mosque shooting in Bærum, Norway (1 killed before the attack, 1 injured),[9] and the Halle synagogue shooting in Germany (2 killed, 2 injured).[10] Those attacks were all shootings in which the perpetrator, explicitly inspired by Tarrant's actions, aimed to inflict mass casualties against a specific ethnic or religious group using one or more firearms. The perpetrators themselves recognised the cluster. Going further than citing Tarrant's actions as an inspiration, the Halle attacker called himself one of the 'chosen' followers of 'Saint Tarrant', alongside the Poway and El Paso perpetrators.[11]

In their weaponry, lone-actor terrorists are typically constrained by resourcing, sometimes lacking the social ties, financial resources or knowledge to obtain black market weapons.[12] Instead, they often simply use weapons they already have, or what's legally available. This cluster of attacks demonstrates this constraint well. Only the Halle attacker, a former soldier, used a crude shotgun and submachine gun he had manufactured.[13] The others used legally sourced rifles, and the Poway and El Paso shooters used semi-automatic rifles, as had Breivik and Tarrant. The availability of semi-automatic rifles is an important element in exacerbating the impact of lone-actor terrorists; a growing evidence base shows that the use of those weapons results in significantly higher casualties during mass shootings.[14]

Shooting attacks also have a visceral power that other methods sometimes lack. A month before the Poway attack, the perpetrator had set a mosque on fire, damaging the building but failing to cause any injury.[15] Despite the perpetrator leaving graffiti at the scene directly linking the mosque fire to the Christchurch attack, it was the subsequent shooting attack at Poway that granted him widespread recognition. The inability of lone-actor terrorists to source these weapons can force them to use suboptimal alternatives, making firearms laws and regulation a powerful mitigator of risk here. Indeed, while streaming his attack on the Twitch gaming platform, the Halle terrorist apologised to his audience, saying that his improvised submachine gun was 'shit'.[16]

Another commonality in this cluster of what we label 'lone actors' was the role of the internet and online communities. The perpetrators were all deeply embedded in the far-right communities found on the 'chans' (including 4chan, 8chan and less popular derivatives such as EndChan[17]) and other social media services. Before their attacks, and much like Tarrant, these lone actors all announced their plans online (the Poway, El Paso and Bærum attackers on 8chan, and the Halle attacker on a similar chan-based derivative).[18] It isn't surprising that these people all visited similar platforms and participated in the same online communities—the tendency for lone-actor terrorists to emulate prior exemplars has only been exacerbated by the communicative power of the internet.[19] That the Christchurch, Halle and Bærum attacks were all live-streamed on different platforms is another example of how individuals are being empowered by technology to inspire the like-minded, as they use those platforms to spread their atrocities to large audiences and gain notoriety. It also shows that some kind of company and sense of being part of a group is important to lone actors, and this results in them having online connections to radicalising material and groups.

Clustering isn't new. Previously, the viral spread of attack methodologies among lone-actor terrorists was seen in the use of vehicles as weapons. High-profile events such as the 2016 Nice attack inspired an 'imitative wave' of copycats, such as the 2016 truck attack on a Christmas market in Berlin and the 2017 Westminster Bridge attack in London.[20] A similar wave was observed in Israel, which, despite experiencing low but persistent rates of lone-actor vehicle attacks since 2000, faced a sudden increase: 53.2% (33 out of 62) of all such attacks occurred in 2015 alone.[21] The widespread use of knives in attacks, particularly in Europe, also has viral quality. The use of weapons such as knives isn't necessarily a demonstration of operational effectiveness; rather, these often suicidal attacks serve as an ideologically acceptable blueprint for action.

Recommendations

As researchers continue to emphasise, and as demonstrated so vividly by the Christchurch cluster, lone-actor terrorists are very likely to leak their intent, because they aren't wholly alone.[22] This presents obvious opportunities for security forces to identify people who present a high level of risk, but, more than that, it presents an opportunity for counterterrorism forces to understand how extremists may prepare for an attack, including their proposed attack methodologies, weapon choice, targeting and planning. That's particularly true in the wake of major attacks such as in Christchurch, where an ensuing wave of copycat and inspired attacks is a strong possibility. This is a unique time in which the 'randomness' of lone-actor terrorism is somewhat mitigated, at least until another unique exemplar attack occurs.

Maintaining the capability to nimbly identify and react to these emerging waves of lone-actor violence should be a priority for security agencies, particularly in the online space, where images and videos of attacks serve not only as entertaining memetic tokens to bond over but as demonstrations of what a successful terrorist operation might look like. For law enforcement, maintaining an intelligence presence in those online communities, whether they exist in relatively accessible web forums (such as the chan-based platforms) or in more private and secure communities found on a variety of chat and social software suites (such as Discord) should be a priority. Access to the latter category poses a significant challenge for law enforcement, although the potential intelligence utility is significant.

I have also identified the importance of firearms in contemporary lone-actor terrorism. Reducing the availability of firearms is one obvious way to mitigate lone-actor violence. As in many lone attacks in the US, apart from the Halle attack, the weapons used in the Christchurch cluster were legally obtained. The concept of risk-based firearm seizure laws has been increasingly adopted in the US. Under those laws, government agencies are empowered through court-issued warrants to confiscate firearms from individuals who demonstrate concerning behaviours.[23] Although not necessarily applicable to jurisdictions with strong existing controls on firearms, such an approach has obvious utility, given the tendency towards leakage to lone actors.

Notes

1 P Gill, J Horgan, P Deckert, 'Bombing alone: tracing the motivations and antecedent behaviors of lone-actor terrorists', *Journal of Forensic Science*, 2014, 59(2):425–435; Clare Ellis, Raffaello Pantucci, *Lone-actor terrorism: 'leakage' and interaction with authorities*, policy paper 4, Royal United Services Institute, London, 2016; R Spaaij, 'Lone actors: challenges and opportunities for countering violent extremism', in A Richman, Y Sharan (eds), Lone actors—an emerging security threat, IOS Press, Amsterdam, 2015, 120–131.

2 M Hamm, R Spaaij, *The age of lone wolf terrorism*, Columbia University Press, New York, 2017, 50–52.

3 R Spaaij, *Understanding lone wolf terrorism: global patterns, motivations and prevention*, 1st edition, Springer, New York, 2012, 29–31.

4 'Latest issue of *Inspire* magazine encourages small scale attacks', Anti-Defamation League, 19 May 2016.

5 A Reed, H Ingram, 'Exploring the role of instructional material in AQAP's *Inspire* and ISIS' *Rumiyah*', Europol, 26 May 2017, online.

6 Elise Thomas, 'Manifestos, memetic mobilisation and the Chan boards in the Christchurch shooting', in I Kfir, J Coyne (eds), *Counterterrorism yearbook 2020*, ASPI, Canberra, 2020, 19–22.

7 'Poway synagogue shooting captured in video prosecutors say, as they describe attack', *Los Angeles Times*, 2 May 2019, online.

8 'El Paso shooting: what we know', *The Guardian*, 4 August 2019, online.

9 'Norway court jails mosque gunman Manshaus for 21 years', *BBC News*, 11 June 2020, online.

10 Jenny Hill, 'Halle shooting: trial begins for Germany synagogue attack suspect', *BBC News*, 21 July 2020, online.

11 Jason Burke, 'Norway mosque attack suspect "inspired by Christchurch and El Paso shootings"', *The Guardian*, 12 August 2019, online.

12 F Burton, S Stewart, 'The "lone wolf" disconnect', STRATFOR Global Intelligence, 2008, online; R Spaaij, *Understanding lone wolf terrorism: global patterns, motivations and prevention*, Springer, New York, 2012.

13 Eric Woods, 'Right-wing extremists' new weapon', *Lawfare*, 15 March 2020, online.

14 E Greene-Colozzi, J Silva, 'Contextualizing firearms in mass shooting incidents: a study of guns, regulations, and outcomes', *Justice Quarterly*, 10 September 2020.

15 Christine Hauser, 'Graffiti citing New Zealand attack is found after mosque fire in California', *New York Times*, 26 March 2019, online.

16 Philip Oltermann, Lois Beckett, 'Germany's Jewish leaders condemn police response to Halle attack', *The Guardian*, 11 October 2019, online.

17 'Norway mosque attack: Bruised suspect Manshaus appears in court', *BBC News*, 12 August 2019, online.

18 'Die wirre Welt des Attentäters', *Der Spiegel*, 14 October 2019, online.

19 Hamm & Spaaij, *The age of lone wolf terrorism*, 47–48.

20 V Miller, K Hayward, '"I did my bit": terrorism, Tarde and the vehicle ramming attack as an imitative event', *The British Journal of Criminology*, January 2019, 59(1):1–23.

21 S Perry, B Hasisi, G Perry, 'Lone terrorists : a study of run-over Attacks in Israel', *European Journal of Criminology*, 2018, 9.

22 Hamm & Spaaij, *The age of lone wolf terrorism*, 91; C Clemmow, P Gill, N Bouhana, J Silver, J Horgan, 'Disaggregating lone-actor grievance-fuelled violence: comparing lone-actor terrorists and mass murderers', *Terrorism and Political Violence*, 19 February 2020, 11.

23 J Vernick, T Alcorn, J Horwitz, 'Background checks for all gun buyers and gun violence restraining orders: state efforts to keep guns from high-risk persons', *The Journal of Law, Medicine & Ethics*, 2017, 45(1):98.

Evolving terrorism threats and counterterrorism responses during the Covid-19 pandemic in Southeast Asia

JEREMY DOUGLAS

Regional Representative, Southeast Asia and the Pacific,
United Nations Office on Drugs and Crime

Bangkok, Thailand

NIKI ESSE DE LANG

Counter-Terrorism Advisor, United Nations Office on Drugs and Crime

Bangkok, Thailand

Introduction

The Covid-19 pandemic has affected many aspects of our lives. Southeast Asia, where some countries have been hit hard by the virus, has been no exception. Terrorist groups—as well as counterterrorism practitioners—have been forced to adapt the way they plan and run operations.

This chapter gives an overview of the (counter)terrorism situation during Covid-19 in Southeast Asia, with a focus on terrorism by or inspired by Islamic State (IS), al-Qaeda, or both. We reflect on how terrorist attacks have continued and evolved during the pandemic; how terrorists have adopted new (or adapted old) ways of fundraising to finance their objectives; and how the use of misinformation, especially online, with the aim of gaining sympathy, recruiting and inciting terrorist acts has surged due to increased reliance on web-based interactions. We also discuss the threat posed by returning and relocating terrorists from outside and inside the region, considering the travel restrictions in place. Finally, we consider the potential long-term impacts of the pandemic on the terrorism landscape in Southeast Asia.

Evolving terrorism threats in Southeast Asia during Covid-19: a causal link?

In August 2020, the UN Secretary-General published his 11th report on the threat posed by IS of Iraq and the Levant (ISIL) to international peace and security, in which he stressed that the picture for Southeast Asia 'remains mixed'. He reported that attacks on security forces in the region occur regularly, but that the pandemic doesn't appear to have contributed to additional attacks. However, the Secretary-General also said that 'ISIL affiliates continue to operate and find safe haven in the southern Philippines' and that 'ISIL sympathizers have used the virus as a pretext for fundraising and to advance their propaganda.'[1]

The Philippines

There were ongoing clashes in 2020 between security forces and several IS-affiliated groups in the Philippines. One of the deadliest was between the Abu Sayyaf Group (ASG) and the Philippine Army in Sulu, where 11 army personnel were killed.[2] Another example was an attack by the Bangsamoro Islamic Freedom Fighters on three Philippine Army detachments that reportedly resulted in the displacement of more than 6,000 villagers. Two days later, the group fired mortar rounds, hitting a cluster of civilian houses, killing two children and injuring 13 others.[3]

The UN Secretary-General's report was published before a major twin-suicide bombing in Jolo on 24 August 2020, which killed 14 and injured 75.[4] Both suspected female suicide bombers were Philippine nationals and widows of well-known Filipino ASG terrorists.[5] The ASG claimed responsibility for the attack by issuing a statement through online channels on behalf of IS East Asia Province.[6] The first explosion took place near a Philippine Army truck carrying out Covid-19 humanitarian efforts, while the second took place in front of the Development Bank of the Philippines, not far from the Cathedral of Our Lady of Mount Carmel, which had suffered a twin-suicide bombing earlier in January 2019 carried out by an Indonesian couple, which killed at least 23 and injured 102.

Jolo is strategically located in the Sulu Sea, close to Sabah State (Malaysia), North Kalimantan Province (Indonesia) and the Mindanao region in the southern Philippines. Many foreign terrorist fighters (FTFs) have made their way to or through Jolo, as well as many of the neighbouring southern Philippines islands in the Sulu Sea. The US considers those areas to be 'terrorist safe havens'.[7] It's estimated that, as of 2019, at least 59 FTFs had illegally entered the Philippines.[8] It's estimated that fewer than 40 FTFs, mostly Indonesian and Malaysian nationals, remain in the country.

The Sulu and Sulawesi seas are infamous for a high number of kidnappings for ransom. The most recent took place on 17 January 2020 when eight Indonesian crew were abducted from a fishing vessel by the ASG off the coast of Sabah, Malaysia.[9] According to the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP), the risk of the abduction of crew in the area and waters off eastern Sabah remains high, and new warnings were issued on 2 July 2020.[10] However, no new kidnappings have been reported during the pandemic. In comparison, throughout 2019, there were two incidents of abductions of crew by the ASG, and in 2018 there were three incidents.[11] This downward trend in kidnappings for ransom may have to do with the 2017 Trilateral Cooperative Arrangement between Indonesia, Malaysia and the Philippines for coordinated maritime patrols in the Sulu Sea, as well as increased Philippine Army operations against the ASG since 2017.[12]

The 2020 Jolo suicide bombing, ongoing clashes between security forces and terrorist groups and the threat of kidnappings for ransom don't have a clear link with the pandemic. However, the threat situation shows that Covid-19 hasn't limited terrorist groups' operations. While it's been argued that militants are trying to take advantage of Covid-19 while the military is 'stretched thin by the pandemic',[13] that isn't particularly evident. Moreover, the pandemic has limited the ability of FTFs to travel to the Philippines.[14] That said, the porous maritime borders between Borneo and the southern Philippines remain susceptible to abuse by transnational organised criminal networks and terrorist groups, despite the increased patrols as a result of the Trilateral Cooperative Arrangement.[15]

Indonesia

Incidents in Indonesia included the planned bombing of a police station in central Java by Jamaah Ansharut Daulah (JAD) in March 2020; the abduction and beheading of two farmers by Mujahidin Indonesia Timur (MIT) fighters on 8 and 19 April 2020, for allegedly being informants; a failed attack by MIT on a police officer in Poso, central Sulawesi, on 15 April 2020, which left two terrorists dead; and the killing of a police officer by an IS and JAD supporter in south Kalimantan in June 2020.[16] Reportedly, MIT documented those incidents—including the beheadings—and uploaded images to pro-IS social media. The Institute for Policy Analysis and Conflict (IPAC) concluded that 'the arrival of COVID-19 in Indonesia instilled a new optimism in MIT.'[17]

The online terrorism landscape

Terrorists' increased use of online platforms in the region shows the strongest link to Covid-19. At the outset of the pandemic and for several months after, terrorists, their supporters and potential recruits have been increasingly accessing social media platforms.[18] The Financial Action Task Force has warned that Covid-19 has led to a rise in cybercrime such as fraud and could lead to increased online fundraising by terrorists posing as Covid-19-related charities.[19]

According to another UN report, a Southeast Asian member state 'observed that ISIL propaganda in the region was highlighting an "end-times" narrative, suggesting that Covid-19 represented divine punishment'.[20] Others reported that IS globally has been publishing propaganda calling Covid-19 'God's little soldier', which was sent to infect and punish unbelievers,[21] and that a plague that would precede a catastrophe was foretold in religious texts.[22] More action-oriented IS-propaganda messages calling followers to carry out *amaliyat* (operations) and attacks against the *kuffar* (unbelievers) or the 'oppressors' have also been disseminated on Indonesian pro-IS and MIT social media channels. Some excerpts from those messages were reproduced in IPAC reports.[23] IS propaganda messages have found their way to Southeast Asia through different social media, including Facebook, Twitter and pro-IS Telegram channels.[24]

Malaysia and the Philippines have reported similar trends, but online recruitment and incitement to terrorism were already a major issue in those countries before the pandemic and, while there may be a larger audience during Covid, aren't new phenomena.

Fundraising, recruitment and potential exploitation of Covid-19 and the non-profit sector

The Financial Action Task Force has warned of terrorist groups exploiting Covid-19 by fraudulently raising funds in the name of humanitarian assistance during the pandemic. For example, several 'charities' in Southeast Asia have been 'actively raising funds through terrorist-affiliated Telegram channels and Facebook groups to support the families of IS fighters from Indonesia and the Philippines'.[25] JAD, the terrorist group responsible for the May 2018 Surabaya suicide bombings and a less successful November 2019 suicide attack against a Medan police station, both in Indonesia, are also said to have used the pandemic 'downtime' to raise funds through Telegram to support 'families of the mujahideen' rather than for operations.[26]

Experts mentioned in May 2020 that some IS supporters in Indonesia 'were collecting funds to buy essentials such as rice and sugar to distribute among themselves, as well as the public affected by the pandemic'. Another example is Jamaat Ansyarul Khilafah, a group claiming to be non-violent but with links to individuals who have committed attacks in the name of IS, which has reportedly been raising funds before and during the pandemic for humanitarian assistance through its Islamic healing clinics, religious study centres and affiliated charities.[27]

An additional threat is Jemaah Islamiyah (JI), the al-Qaeda-affiliated group responsible for the 2002 Bali bombings and other major incidents, including the 2009 JW Marriot hotel bombing. This group, formerly led by Abu Bakar Bashir and more recently by Para Wijayanto (captured in June 2019 and currently on trial), is far from defunct, although it has changed tactics. Wijayanto's arrest and trial have revealed that JI still has financial and human resources at its disposal. At the time of his arrest, the group was still able to run a network of preachers, schools, corporations, mosques and palm oil plantations. While this network is on the authorities' radar and parts of it have been shut down, there's still an active 'underground' JI network that could exploit the pandemic.[28] JI has done that in the past, after the 2004 Aceh tsunami and the 2006 Yogyakarta earthquake, by providing family support, health care and welfare, with an intent to recruit new members.[29] The arrest of another major JI leader and one of the masterminds behind the 2002 Bali bombings, Zulkarnaen (also known as Aris Sumarsono), on Sumatra island in December 2020, and the news that JI recently installed 13,000 charity boxes at marketplaces across Indonesia, confirms these suspicions.[30]

Counterterrorism in the face of Covid-19: achievements and challenges

The UN Secretary-General stated that authorities in Indonesia and the Philippines 'have maintained pressure on ISIL activities through counter-terrorism operations, many of which have succeeded in disrupting planned attacks at early stages'. In fact, between January and July 2020 there were more than 80 terrorism-related arrests in Indonesia, and several planned attacks were disrupted. Most of the individuals arrested were members of JAD or MIT.[31]

According to IPAC, many early 2020 arrests in Indonesia were linked to MIT. There were also reported arrests of pro-IS individuals without links to MIT or JAD. During one arrest in Batang, central Java, on 25 March 2020, the police allegedly found explosive materials meant for making bombs, but no evidence of targets was found.[32] Apart from those apparent successes, there have also been challenges, one of them being the killing of a 20-year-old male by police in Poso, central Sulawesi in April 2020, after the man was mistaken for an MIT terrorist.[33]

A recent example of regional collaboration on the maritime front involved an Interpol-led operation codenamed 'Maharlika III' in February and March 2020. Brunei, Indonesia, Malaysia and the Philippines deployed their personnel at strategic points along known terrorist transit and other illicit trafficking routes in the Sulu and Celebes seas. They conducted a series of operations, including sea patrols, passenger and vehicle checks, and secondary identity inspections of any suspicious individuals, resulting in the arrest of more than 180 people, including a suspected member of the ASG. In addition, 134 victims of human trafficking were rescued and more than €1 million worth of firearms, illegally assembled explosives and other illicit goods and substances was seized.[34]

However, authorities committed serious mistakes in disrupting planned attacks, especially in relation to the August 2020 suicide bombing in Jolo. Reportedly, four army intelligence officers, on a mission to locate suspected ASG suicide bombers, were shot and killed by police. Accounts of what transpired differ, and the incident is currently under investigation.[35]

The importance of gender dimensions when countering terrorism—an issue long overlooked and still inadequately addressed—was highlighted on 10 October 2020 when an Indonesian woman suspected of preparing a suicide attack was arrested with two ASG members. She was identified as Rezky Fantasya Rullie, and a suicide bomb vest was found during the raid. She's said to be the daughter of the Indonesian couple who committed the twin-suicide attack in Jolo in January 2019 and the widow of Indonesian FTF Andi Baso, who was killed in the Philippines in August 2020.[36] It's likely she was living in the Philippines and had travelled there before the Covid-19 pandemic broke out. Initially, it was reported that she would be deported to Indonesia, but a later report states that she'll be prosecuted in the Philippines under the new Anti-Terrorism Act of 2020 (ATA 2020).[37]

It's seen as a welcome development that she'll be prosecuted in the Philippines, rather than being deported to Indonesia. Before the adoption of the ATA 2020, deportation seemed to have been the preferred method to deal with Indonesian FTFs in the Philippines, which was worrying because of the risk of terrorists potentially escaping justice. In September 2020, for example, Minhati Madrais, the widow of Omarkhayam Maute of the pro-IS Maute Group in the Philippines, was deported to Indonesia. She's alleged to be one of the key people controlling the Maute Group's financing and is undergoing a mandatory deradicalisation program in Indonesia, but it isn't clear whether there's sufficient evidence for her prosecution.[38]

While the use of the ATA 2020 in the Philippines for the prosecution of FTFs is seen as a positive change, the legislation was passed under a cloud of criticism by civil society groups and the UN human rights office for a lack of consultation and for having provisions with potentially negative implications for human rights and freedoms.[39] To date, civil society groups have filed 37 petitions with the Supreme Court opposing the new law.[40]

Indonesia has also been pursuing some legislative changes by adopting a presidential regulation on the role of the military in counterterrorism, effectively giving the military more powers. This was met with criticism from civil society groups citing concerns over such a broad mandate for the military and the implications that may have for human rights.[41]

While these legislative developments aren't directly related to the pandemic, they may be perceived by the public as bad timing and choice of priorities in a time when people are already facing additional security restrictions.

Longer term impacts on Southeast Asian counterterrorism

The socioeconomic fallout from the Covid-19 crisis could exacerbate grievances against government and other drivers conducive to terrorism. For example, government budgets available for socio-economic goals, including health and education, may decrease, as well as resources currently allocated for counterterrorism work, especially on the preventive side. In addition, a reduction in available funding from international donors will negatively affect civil society and intergovernmental organisations that are dependent on contributions to sustain and upscale programs addressing conditions conducive to terrorism.

An additional important aspect is that travel restrictions in place due to Covid-19 have severely reduced the ability of FTFs and their family members currently outside Southeast Asia to return or relocate to the region. However, when those restrictions are lifted, it's likely that many Southeast Asian FTFs and their family members will return. As recent history has shown, it's also likely that FTFs from other regions will continue to be attracted to conflict-prone areas in Southeast Asia.

Conclusions and recommendations

The pandemic isn't likely to hamper terrorist groups in Southeast Asia. We've mainly discussed examples from the Philippines and Indonesia attributable to IS-affiliated groups. However, there are other active groups in the region that also pose serious threats to regional peace and security, including those active in Thailand and Myanmar and the New People's Army in the Philippines.

Counterterrorism practitioners should pay attention to other groups, such as Jamaat Ansyarul Khilafah and the remnants of JI, that might operate under the radar and try to recruit and raise funds. One potential approach is through increased dialogue and outreach to the non-profit sector and the general public on terrorism financing risks and the importance of ensuring that donations are going to the charitable causes they're intended for.

A more securitised approach that involves shutting down certain organisations suspected to be at high risk, or preventing unregistered charities from operating, might do more harm than good.

There have been some successful counterterrorism operations in response to threats in Indonesia and the Philippines, including subregional or international cooperation efforts under the auspices of the Trilateral Cooperative Arrangement and Interpol. Sustaining and expanding those efforts will be beneficial for the security of the region, especially in 'hotspot' areas in and around the Sulu and Celebes seas. International cooperation and domestic multiagency collaboration remain the keys to success in counterterrorism operations, as terrorists and criminals don't respect international boundaries and benefit from internal disputes and competition between national counterterrorism actors.

At the operational and policy levels, it's important to understand what conditions might be conducive to terrorism. They can include social, political and economic inequality; ethnic or religious discrimination; lack of self-determination by ethnic or indigenous minorities; lack of resources for education and socio-economic support; corruption; and grievances that result from heavy-handed counterterrorism operations or the adoption of policy, laws and regulations that are perceived as repressive. Consultative processes, fair and transparent accountability measures and an overall primacy of the rule of law and human rights principles are the keys to addressing those conditions and will reduce the pool of people susceptible to terrorist narratives.

Notes

1 UN, *Eleventh report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat*, UN doc. S/2020/7744, *ReliefWeb*, August 2020, online.

2 UN, *Twenty-sixth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities*, UN doc. S/2020/717, online, paragraph 73.

3 Jasminder Singh, Muhammad Haziq Jani, 'COVID-19 and terrorism in the southern Philippines: more trouble ahead', *The Diplomat*, 26 August 2020, online.

4 Jason Gutierrez, 'At least 14 killed after suicide bombers hit Philippines', *New York Times*, 24 August 2020, online; '14 killed in Jolo twin bombings in southern Philippines', *al-Jazeera*, 24 August 2020, online; 'Philippines: twin explosions hit Jolo, killing at least 14', *BBC News*, 24 August 2020, online.

5 'Suspected Jolo suicide bombers both Filipinos, tracked by soldiers killed by cops in June—officials', *CNN Philippines*, 26 August 2020, online.

6 Jeoffrey Maitem, 'IS militants claim responsibility for Sulu blasts', *Inquirer.net*, 25 August 2020, online.

7 Bureau of Counterterrorism, *Country reports on terrorism 2019*, State Department, US Government, 2020, 206, online.

8 Bong Sarmiento, 'ISIS thrives in Covid-19 shadows in Philippines', *Asia Times*, 22 May 2020, online.

9 Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in the Asia–Pacific (ReCAAP), *Monthly report: Piracy and armed robbery against ships in Asia, July 2020*, online; ReCAAP , *ReCAAP ISC weekly report: Piracy and armed robbery against ships in Asia: 29 Sep—5 Oct 2020*, online.

10 ReCAAP, *Monthly report: Piracy and armed robbery against ships in Asia, July 2020*.

11 ReCAAP, *Piracy and armed robbery against ships in Asia: Annual report, January–December 2019*, 16–17, online.

12 Ian Storey, 'Trilateral security cooperation in the Sulu-Celebes seas: a work in progress', *Perspective*, ISEAS—Yusof Ishak Institute, Singapore, 27 August 2018, issue 48, online.

13 Kenneth Yeo, 'Are Philippine militants looking to take advantage of COVID-19?', *The Diplomat*, 1 May 2020, online.

14 Kenneth Yeo Yaoren, Unaesah Ramah, 'Southeast Asia: returning foreign fighters', *The Defense Post*, 23 June 2020, online.

15 Prashanth Parameswaran, 'Are Sulu Sea trilateral patrols actually working?', *Asia Dispatches*, Wilson Center, 29 January 2019, online.

16 UN, *Twenty-sixth report of the Analytical Support and Sanctions Monitoring Team*, paragraph 71.

17 Institute for Policy Analysis of Conflict (IPAC), *Covid-19 and the Mujahidin of Eastern Indonesia (MIT)*, IPAC short briefing no. 3, 28 April 2020, 5, online.

18 Counter-Terrorism Committee Executive Directorate (CTED), *The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism*, UN Security Council, June 2020, online.

19 Financial Action Task Force, *COVID-19-related money laundering and terrorist financing: risks and policy responses*, May 2020, online.

20 UN, *Twenty-sixth report of the Analytical Support and Sanctions Monitoring Team*, paragraph 75.

21 Muhammad Sinatra, *Terrorism landscape in the COVID-19 pandemic*, policy brief, Institute of Strategic and International Studies Malaysia, 20 July 2020, online; Mia Bloom, 'How terrorist groups will try to capitalize on the coronavirus crisis', *Just Security*, 3 April 2020, online.

22 Arlina Arshad, 'Indonesian terrorists "wait for end of world" as coronavirus bites', *The Star*, 18 May 2020, online; IPAC, *COVID-19 and ISIS in Indonesia*, short briefing no. 1, 2 April 2020, online.

23 IPAC, *COVID-19 and ISIS in Indonesia; IPAC, Covid-19 and the Mujahidin of Eastern Indonesia (MIT)*, 5.

24 IPAC, *COVID-19 and ISIS in Indonesia*.

25 Iftekharul Bashar, Kenneth Yeo Yaoren, 'Combating extremist charities during COVID-19', *East Asia Forum*, 15 July 2020, online.

26 Zachary Abuza, Alif Satria, 'How are Indonesia's terrorist groups weathering the pandemic?', *The Diplomat*, online.

27 IPAC, *COVID-19 and ISIS in Indonesia*; V Arianti, Muh Taufiqurrohman, 'The quiet threat of Indonesia's Jamaah Ansharul Khilafah', *The Diplomat*, 11 August 2020, online.

28 Abuza & Satria, 'How are Indonesia's terrorist groups weathering the pandemic?'; Prashanth Parameswaran, 'Where is Jemaah Islamiyah in Southeast Asia's terrorism landscape?', *The Diplomat*, 8 July 2020, online; Farouk Arnaz, 'Indonesian police detect resurgence of Jemaah Islamiyah', *Jakarta Globe*, 15 June 2020, online; Bilveer Singh, 'Jemaah Islamiyah: still Southeast Asia's greatest terrorist threat', *The Diplomat*, 7 October 2018, online.

29 Bashar & Yeo Yaoren, 'Combating extremist charities during COVID-19'.

30 Tri Iswanto, 'Indonesian militant linked to Bali bombings flown to Jakarta for questioning', *Reuters*, 16 December 2020, online; Anugrah Kumar, 'Indonesia: Al-Qaeda linked terrorists use thousands of fake charity boxes to raise funds', *Christian Post*, 14 December 2020, online.

31 UN, *Twenty-sixth report of the Analytical Support and Sanctions Monitoring Team*, paragraph 70.

32 IPAC, *COVID-19 and ISIS in Indonesia*.

33 IPAC, *Covid-19 and the Mujahidin of Eastern Indonesia (MIT)*, 6.

34 'Hundreds arrested in crackdown on terrorist routes in Southeast Asia', news release, Interpol, 22 April 2020, online.

35 Associated Press, 'Philippine police kill four army soldiers in deadly shoot-out "mix-up"', *South China Morning Post*, 30 June 2020, online; Associated Press, 'Philippine police fatally shoot 4 army soldiers in south', *Wtopnews*, 29 June 2020, online.

36 'Philippines: suspected female bomber from Indonesia to face charges, expulsion', *Benar News*, 12 October 2020, online.

37 'Indonesian woman first to be tried under Philippines' new anti-terror law', *Arab News*, 14 October 2020, online.

38 Amy Chew, 'Widow of Filipino militant now undergoing deradicalization in Indonesia', *Benar News*, 30 September 2020, online.

39 Mong Palatino, 'How Duterte's anti-terror law unleashed public outrage against his leadership', *The Diplomat*, 13 July 2020, online.

40 Kristine Joy Patag, 'With anti-terror law IRR done, time running out for SC to grant immediate relief—petitioners', *Philstar Global*, 15 October 2020, online.

41 Fynn-Niklas Franke, 'Talking about counterterrorism in times of crisis', *Bangkok Post*, 6 June 2020, online.

The impact of technology on extremism

LEVI J WEST

Director of Terrorism Studies, Australian Graduate School of Policing and Security, Charles Sturt University

Canberra, Australia

Technology will continue to play a central role in the ongoing evolution of the character of terrorism, including the way terrorist organisations of all ideological persuasions perpetrate violence and the way they communicate their messages. Technological developments have always shaped the character of terrorism. The discovery of dynamite, the expansion of international air travel and the ubiquity of social media have all been exploited by terrorists. Ensuring that counterterrorism (CT) policy and practice remain abreast of technological developments that are being, and will likely continue to be, exploited by terrorists and other violent non-state actors is integral to the ongoing success of international CT.

Evolving technology applications to terrorism

The development, accessibility and affordability of contemporary technology has had a substantial impact on modern life.[1] The ubiquity of advanced technological devices such as tablets and smartphones, when coupled with ready access to an almost infinite body of information and data, has shaped contemporary society in ways that few imagined.[2] It should be unsurprising that terrorists and other violent non-state actors, such as Mexican drug-trafficking organisations,[3] have exploited technology for their own purposes.

Technology has been at the centre of recent developments in terrorism and CT. Those developments reflect a willingness and a need by terrorists to embrace technology for their operational and strategic purposes. The Islamic State's (IS's) social media campaign brought tens of thousands of foreign fighters to Syria and Iraq and inspired countless 'lone actors' to commit terrorist violence in the group's name. That resulted in the emergence of a broad range of innovative national and international CT policies and practices involving private-sector technology companies and integrated multilateral CT efforts.[4] Additionally, the live streaming of the Christchurch terrorist attack in 2019 led to a renewed effort by governments and the private sector to attempt to address the proliferation of extremist and terrorist content in the online environment, including content related to extreme right-wing ideology.[5]

The exploitation of technology for terrorist purposes has been central to the capacity of terrorists and other asymmetrically weak actors to achieve effect. Historically, this has occurred in two core domains: technologies of violence and communications technology. Since the invention of dynamite, terrorists have embraced novel and accessible technologies of violence that support their strategic objectives.[6] That approach has underpinned the deployment of now familiar tactics such as aircraft hijacking, suicide terrorism, the refinement and improvement of improvised explosive devices, and more. While the nature of terrorism and the deployment of instrumental and communicative violence for ideological purposes has endured throughout the modern history of terrorism, the specific manner in which terrorists practise violence reflects the political, social and technological context from which they emerge.

Even the recent spike in the use of low-capability tactics such as stabbings and vehicle ramming has been reliant on technology. IS has run a sophisticated and diverse propaganda campaign in social media, identifying targets, endorsing tactics and providing theological and strategic permissions. The IS social media campaign was fundamental to inspiring lone actors to commit acts of terrorism and to enabling their violence to be perceived and understood as terrorism.[7]

The exploitation of communications technology has been, and will continue to be, an essential requirement for terrorism to achieve effect. The print media industry underpinned the spread and impact of anarchist terrorism across Europe and the US in the late 1800s and early 1900s, in the same way that satellite television and screen media made Palestinian terrorism and political violence emblematic of an entire period of terrorism in the 1960s and 1970s.[8] In the contemporary environment, social media and digital technologies have served the same purpose. Social media have made extremist and terrorist content more accessible, and digital technology has enabled a dramatic expansion in the quality, volume and diversity of content available across all ideological categories. The ease with which terrorist ideology, terrorist narratives and terrorist operational instructions can be accessed has been dramatically enhanced by modern digital technology.[9]

The campaigns that IS ran, focusing on specific issues or specific theatres, are reflective of the way digital technology has enhanced terrorist propaganda capabilities. The Marawi conflict in the Philippines is instructive in this regard.[10] From May 2017 onwards, IS ran a diverse and coordinated campaign that sought to contextualise and justify its actions in Marawi while actively encouraging supporters to migrate to the Philippines in support of its efforts. That included multiple episodes of the *Inside the Caliphate* video series that featured an Australian jihadist explicitly encouraging IS supporters to either travel to Marawi or to:

> … kill them wherever you find them. If you're a tradesman, use your nail gun and nail the kaffir to the head and crucify his body to the woodworks. If you're truck driver, ram their crowds until their streets run with their filthy blood. Or pour petrol over their houses whilst they're asleep and engulf their houses with flames. That way the message will be burnt into their memories.[11]

The June 2017 edition of the *Rumiyah* magazine, IS's English-language online publication, featured a cover story focused on the 'Jihad in East Asia'[12] as well as a five-page interview with the so-called 'Amir of Khilafah in East Asia'. Those are but a sampling of the Marawi- and Philippines-oriented content released to augment operations on the ground in Marawi. The operation highlights a microcosm of the approach that IS used to substantial effect, enabled by the propagation of digital technologies.

Implications for counterterrorism operations

In much the same way that terrorism is shaped by the availability and exploitation of technology, CT agencies must ensure that they remain at the forefront of technological capabilities and have a sophisticated and up-to-date understanding of terrorists' uses of technology. The exploitation of social media by IS and the live streaming of the Christchurch attack in 2019 both provided an important impetus for CT policies and practices to develop new approaches.

The IS social media campaign drove the expansion and refinement of the High Value Targeting program, which sought to identify important terrorist actors and 'remove them from the battlefield', to include a focus on those with substantial online influence and whose primary capability lay in the propaganda domain. This is reflective of the power that digital technology has provided to contemporary terrorist organisations and the way in which CT operations have changed as a result. Targeting propagandists rather than key leaders or explosives experts reflects the growing power of digital technologies.

IS's use of social media also resulted in the formation of a range of multilateral organisations and private-sector-led initiatives, such as the Global Internet Forum to Counter Terrorism. The forum was established in 2017 as a partnership between Facebook, Twitter and YouTube with the stated aim of 'disrupting terrorist abuse of members' digital platforms'.[13] The emergence of private-sector-led CT efforts reflects some of the limits that states have in seeking to operate in and regulate large-scale private-sector technology companies.

Both the IS campaign and the Christchurch attack have also provided the impetus for increased political and public pressure on various unconventional platforms that have become the domicile of terrorists and extremists as conventional platforms have become more proactive at addressing their presence. For example, as IS increasingly migrated its online presence to the encrypted platform Telegram, broad public and political pressure resulted in some efforts to prevent the group exploiting the platform.[14] In a similar manner, the Christchurch attack led to companies such as Cloudflare ultimately removing their cybersecurity services from 8Chan[15]—the platform most closely associated with the Christchurch attack and numerous other extreme right-wing incidents.

While there's been some evidence of terrorists' use of new technologies, such as drones,[16] there hasn't been a wholesale take-up of those technologies by terrorists or other non-state actors. While communications technology such as social media has become nearly ubiquitous in its usage by terrorists, the use of drone technology, despite the opportunities it presents for terrorist organisations, hasn't become a central element of terrorist capability. The Christchurch terrorist used a drone to undertake surveillance of the two mosques he targeted in his attack,[17] and that's been one of the primary ways that terrorists have used drones. It has contributed substantially to terrorist propaganda, both in the Middle East and South East Asia, but its use as an offensive capability—as distinct from either a propaganda or a surveillance tool—has been limited.[18]

The limited take-up of drone technology shouldn't suggest that it's unlikely to contribute substantially to ongoing developments in the terrorist operational arsenal. Audrey Cronin argues that much of the next wave of technological advancement that will be exploited by terrorists will emerge from what she refers to as convergent technologies—'specifically UAVs … other robots, 3D printing (additive manufacturing), and nascent autonomy.'[19] Those technologies offer the potential for a substantial step change in the affordability, accessibility and lethality of offensive technological capabilities for terrorists and other non-state actors. Policymakers and commanders in theatre will need to remain abreast of these emerging technologies and their potential adoption and deployment by terrorists and insurgents. The demonstration of their effectiveness by IS and others will increase the likelihood of their increased use by terrorists.

Future challenges and recommendations

There remain numerous challenges for CT policy and practice as it pertains to technology, in terms of both capability and broader policy considerations. Governments and, increasingly, the private sector must maintain a difficult balance between ensuring that they retain leading-edge CT capability while ensuring that their policy settings are proportional and necessary, and that the foundational principles of liberal democracy are preserved and defended:

- It will be essential, as communications technologies continue to evolve, that CT capability remains up to date with those technologies' surveillance and disruption capabilities while ensuring that appropriate platforms for open public discourse remain accessible and that the broader public continues to engage in free and open political debate.

- There's an increasing need for a broader understanding of the types of material that contribute to radicalisation. While violent content is now addressed in various ways, the ideological tracts of extremists remain misunderstood and more difficult to regulate. It's essential to develop and operationalise an improved recognition of the role played by manifestos, statements of ideology and doctrinal material.
- New communications technologies will emerge and will need to be considered through the lens of their potential exploitation by terrorists and extremists. While those technologies are likely to become ubiquitous before they're regulated or considered for their hostile application, it will be necessary to ensure that governments and the private sector, through the various instruments they have developed in response to IS and Christchurch, continue to engage in order to stay abreast of new developments.
- It's also imperative, both from an operational perspective and from a broader community engagement perspective, that online content, be it jihadist or extreme right-wing, be treated with equal severity and urgency. As the ongoing debate about Facebook's handling of extreme right-wing content demonstrates,[20] there's a need to ensure that extremist content, regardless of its ideological character or its proximity to power, is dealt with in a transparent, equitable and timely manner.

As contemporary communications technology has become a key element of social infrastructure, it's increasingly necessary that those platforms are dealt with in a manner that recognises their significance and the influence they have over public and political discourse. That will require governments to increasingly engage with technology companies, and especially social media companies, to play a more proactive role in not just the CT space but in the broader domain of public discourse. Additionally, foreign interference and extremism increasingly evidence concurrence and interrelationships,[21] so ensuring that democratic discourse and the central role it plays in democratic processes are protected is a core obligation of governments and social media companies. The protection of democracy and the countering of efforts to undermine it, be that through the promotion of extremist ideas, the propagation of disinformation or the undermining of trust in institutions, must all become part of a broader effort to ensure that the benefits of modern communications technology aren't overwhelmed by the costs.

Extensive lessons have been learned in recent years that create opportunities to improve our CT approaches. This requires leveraging the multilateral collaborations that facilitated earlier successes, reinforcing the public–private engagement that was born of those challenges, and building a broader coalition focused on protecting democratic discourse and public debate from an increased array of threats.

Notes

1 AC Madrigal, 'Tech experts are pessimistic about their industry', *The Atlantic*, 21 February 2020, online.

2 A Newitz, 'A better internet is waiting for us', *New York Times*, 30 November 2019, online.

3 Joseph Cox, 'Mexico's drug cartels love social media', *Vice*, 5 November 2013, online; 'Twitter, guns and money: Mexico's cartels live large on social media', *NBC News*, 14 June 2014, online.

4 Bipartisan Policy Center, *Digital counterterrorism: fighting jihadists online*, March 2018, online.

5 K Veale, 'The "Christchurch Call" is just a start. Now we need to push for systemic change', *The Conversation*, 16 May 2019, online.

6 TX Hammes, 'Terror and technology: from dynamite to drones', *War on the Rocks*, 4 September 2020, online.

7 L West, '#jihad: understanding social media as a weapon', *Security Challenges*, 2016, 12(2), 9, 26, online.

8 K Hawa, 'From Palestine to the world, the militant film of the PLO', *The New York Review*, 17 October 2020, 17, online.

9 Ines von Behr, Anaïs Reding, Charlie Edwards, Luke Gribbon, *Radicalisation in the digital era*, RAND Corporation, Santa Monica, 2013, online.

10 C Knight, K Theodorakis, *The Marawi crisis: urban conflict and information operations*, ASPI, Canberra, 31 July 2019, 31, online.

11 'Australian IS fighter calls in video for countrymen to fight in Marawi or stay and kill "disbelievers"', SITE Intelligence Group, 7 August 2017, online.

12 'IS says losing territory redoubled its efforts and shifted focus to "Crusader soil" in Rumiyah', SITE Intelligence Group, 7 June 2017, 10, online.

13 Global Internet Forum to Counter Terrorism, online.

14 M Bernhard, 'Telegram app tackles Islamic State online propaganda', *Wall Street Journal*, 26 November 2019, online.

15 E Stewart, '8chan, a nexus of radicalization, explained', *Vox*, 5 August 2019, online.

16 MS Schmidt, E Schmitt, 'Pentagon confronts a new threat from ISIS: exploding drones', *New York Times*, 11 October 2016, online.

17 Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019, 'Planning the attack', *The report*, 2020, online.

18 E Archambault, Y Veilleux-Lepage, 'Drone imagery in Islamic State propaganda: flying like a state', *International Affairs*, 2020, 96(4):955–973, online.

19 AK Cronin. *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford University Press, 2020, p. 202. online.

20 C Knaus, M McGowan, N Evershed, O Holmes, 'Inside the hate factory: how Facebook fuels far-right profit', *The Guardian*, 6 December 2019, online; L Beckett 'Michigan terror plot: why rightwing extremists are thriving on Facebook', *The Guardian*, 10 October 2020, online.

21 A Romano, 'Twitter released 9 million tweets from one Russian troll farm. Here's what we learned', *Vox*, 19 October 2018, online; A Glaser, 'Russian bots are trying to sow discord on Twitter after Charlottesville', *Slate*, 23 August 2017, online.

Boogaloo Bois: the birth of a ‘movement’, from memes to real-world violence

ELISE THOMAS
Former researcher, International Cyber Policy Centre, ASPI
Canberra, Australia

Online memes have been a tool for recruitment and propaganda for established extremist movements for many years. Whether the memes are created spontaneously by grassroots sympathisers or are part of coordinated and deliberate strategies laid out by the leadership of extremist groups, they reflect and transmit the movement's ideology. Overt or coded references serve as a wink to insiders and, their creators may hope, an intriguing hint that will make outsiders want to know more.

However, what's occurred over the past several years, and accelerated dramatically since the beginning of the global Covid-19 crisis, is the opposite process. Beyond just extremist movements generating memes, memes are now also inspiring extremist violence.

It's too early to fully understand how the dynamics of these digital-native forms of extremism may differ from more traditional extremism, which begins offline and later moves into online spaces. This analysis will be further complicated by issues involving the recording of digital history,[1] particularly where crucial historical evidence is in fringe or ephemeral social media spaces that may be deleted before it can be archived or analysed.

The clearest example of this so far is the Boogaloo, a US-based phenomenon that's been linked to several violent attacks in 2020. At least two people have been charged with terrorism offences,[2] multiple murders of law enforcement officers,[3] and an alleged plot to kidnap Michigan Governor Gretchen Whitmer.[4]

These forms of extremism are born and nurtured in online spaces. The ambiguity of memes and of meme culture plays a crucial role, but other factors unique to digital platforms are also important, such as the potentially radicalising role of algorithms and the ways in which social media platforms that prioritise engagement create inherently escalatory social dynamics. The media spotlight has also been a major galvanising factor.

Understanding the ways in which these digital-native extremisms differ from traditional or even digitised extremist movements (that is, extremist groups that began with a well-established offline existence and later moved into being active in online spaces) will be important in order to respond to them effectively.

The phenomenon now known as the Boogaloo can be traced back at least as far as 2018, through references to the 'Civil War 2: Electric Boogaloo' on the social media platforms Facebook and Reddit.[5] This was an adaptation of an existing meme that used 'Electric Boogaloo' (a reference to the *Breakin' 2: Electric Boogaloo* movie) as a reference to a poor quality sequel.[6] The 'Civil War 2: Electric Boogaloo' meme was originally used by US-based gun rights activists to refer to the consequences of government or law enforcement passing stricter gun control laws or trying to 'take their guns'.

The meme bubbled along over the course of 2019, spreading across multiple social media platforms. It cross-propagated with other memes and cultural narratives and received a particular boost on anonymous imageboard 4chan, especially from its /k/ board, which is dedicated to discussing weapons. 4chan and other chan boards, including 8chan and now 8kun, are infamous for having incubated toxic, misogynist, racist, anti-Semitic and at times overtly white supremacist cultures. Across 2019, the /pol/ boards (dedicated to discussing politics) on both 4chan and 8chan were linked to multiple mass shootings, including the Christchurch shooting.

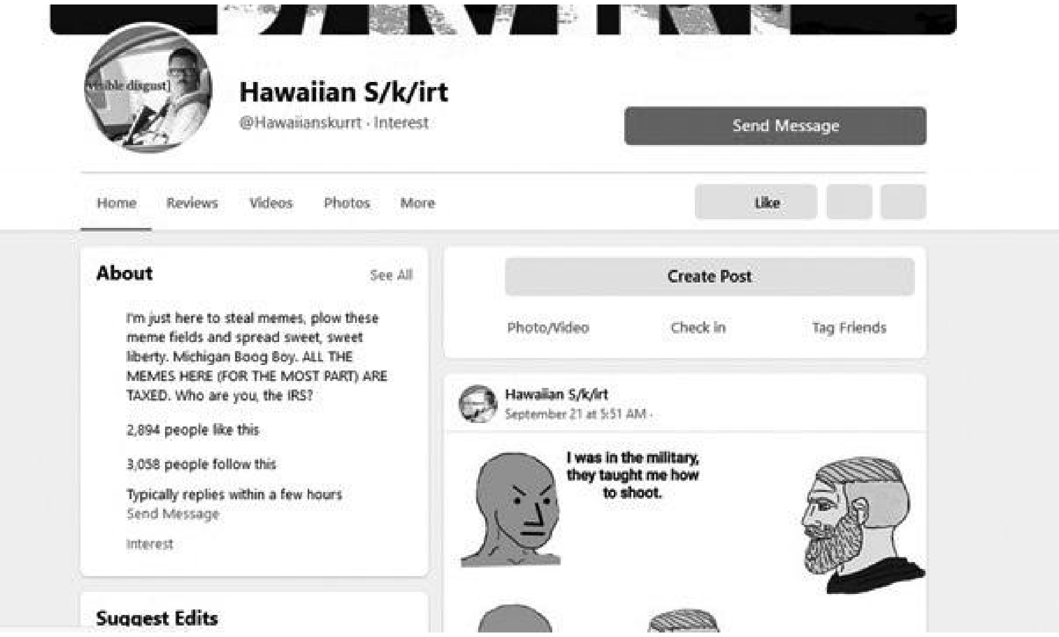
Meanwhile, on the /k/ board the Boogaloo meme was picking up steam. The legacy of this /k/ board connection can be seen even on different platforms, for example in the names of Facebook groups. In the example in Figure 1, run by a self-professed 'Michigan Boog Boy', the visual style and references of the Boogaloo, including the infamous Hawaiian shirt,[7] sit alongside /k/ board and other chan culture references.[8]

Leading up to early 2020, some of the visually distinctive elements of the Boogaloo began to emerge. Many were jokey references to codewords, which social media users adopted to avoid content moderation. The Hawaiian shirts, for example, started as a nod to the 'big luau', which some users began using in place of 'Boogaloo' in an effort to avoid detection. The igloo was also adopted as a symbol after the 'big igloo' became another Boogaloo codeword.

The important thing to understand is that, at this stage, there was nothing that could reasonably be considered a Boogaloo ideology. Conceptually, the Boogaloo consisted of vague references to desiring civil unrest, opposition to law enforcement (and tax agencies) and a heavy emphasis on gun rights, but beyond those broad attitudes there was no coherent ideological basis common to all or even most people engaging with the meme. There was no widely held consensus on what should spark the civil war, or what should happen after it. There was also no centrally organised group structure or clear dividing line between who was or was not a 'Boogaloo Boi'. For many, it was more a long-running social media joke than a meaningful belief or desire for real violence.

Over the course of 2020, however, that dynamic began to evolve rapidly. This was partly a result of external events and how the social dynamics of social media platforms drive responses to those events. The social dynamics of platforms such as Facebook and Reddit create cycles of escalation, in that the design of the platform encourages users to compete with each other to generate engagement, and the most engaging content is often the most extreme. It's also the most likely to be algorithmically recommended or surfaced to others. Algorithms also play a role in spreading and cross-propagating Boogaloo content by recommending users who join one Boogaloo group to join more groups and pages connected to the Boogaloo.

Figure 1: Facebook page, captured 29 September 2020



Hawaiian S/k/irt

@Hawaiianskurrt · Interest

I'm just here to steal memes, plow these meme fields and spread sweet, sweet liberty. Michigan Boog Boy. ALL THE MEMES HERE (FOR THE MOST PART) ARE TAXED. Who are you, the IRS?

2,894 people like this

3,058 people follow this

Typically replies within a few hours

Send Message

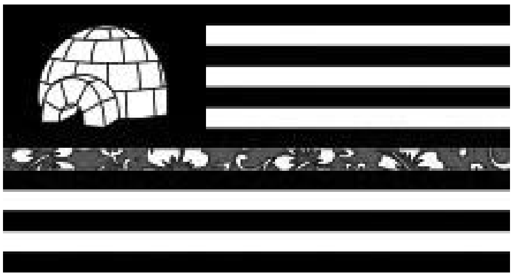
Interest

Hawaiian S/k/irt

September 21 at 5:51 AM ·

I was in the military, they taught me how to shoot.

Figure 2: The Boogaloo flag mimics the US flag, featuring an igloo and a Hawaiian patterned stripe



However, by far the greatest factor in driving the evolution of the Boogaloo from a series of loosely linked social media groups into something much closer to an extremist movement seems to have been the media spotlight.

As the tumult of 2020 began to unfold, Boogaloo Bois, in their Hawaiian shirts and often heavily armed, became a highly visible presence in protests across the US. They were active in gun rights rallies in January,[9] anti-lockdown protests in May[10] and George Floyd protests in June.[11]

Three men in Nevada, who were described in court documents[12] as self-identified members of the Boogaloo and belonged to a Nevada-based Boogaloo Facebook group, were charged with terrorism offences in connection with plans to use the protests as a pretext for escalating violence and targeting law enforcement.[13] In another dramatic incident, an Air Force sergeant allegedly inspired by the Boogaloo ambushed and killed a California sheriff's deputy, shot to death a federal security officer outside a courthouse and critically injured another, stole a car and wrote Boogaloo-related phrases across it in his own blood before finally being caught.[14] Over the course of one week in October, a string of at least 16 arrests took place, most connected to a plot to kidnap Michigan's Governor, Gretchin Whitmer, potentially murder her and spark a civil war.[15] A senior law enforcement official reportedly told *NBC News* that the group 'believes' in the Boogaloo.[16] The group's leader, Brandon Caserta, had also posted videos to TikTok of himself in a Hawaiian shirt as he went on an anti-government tirade.[17]

There's a reasonable debate to be had over how pivotal the Boogaloo was in inspiring those incidents and whether, if the Boogaloo hadn't existed, these individuals would simply have gone on to commit violence in the name of some other cause. The same questions could be posed about almost any form of extremism, however. The fact that law enforcement consider the movement significant enough to mention it in court filings—and that one perpetrator considered it significant enough to write in his own blood—suggests that the Boogaloo is important to consider as a form of extremism in its own right as well as in combination with other forms of anti-government extremism.

All of those incidents were accompanied by waves of mainstream media attention, which sought to define and characterise the Boogaloo for their audiences. The Boogaloo was described variously as a 'group', a 'movement', a 'far-right militia', 'white nationalists' or even 'white supremacists'.

This coverage was, of course, voraciously consumed by the Boogaloo Bois themselves. The subsequent debates and arguments over whether the media's characterisation of the Boogaloo was accurate (for example, between those who objected to being characterised as white nationalists and those who were happy to own the label) exposed contradictions that had previously been papered over.

In short, the ambiguity of memes and meme culture had, for a time, allowed the Boogaloo to mean almost anything to almost anyone, so long as violence against the state was involved. Libertarians and anarchists saw an uprising of the people against the oppressions of government; white nationalists saw an uprising of *white* people against political correctness and the perceived oppression of whites in a multiracial state. They both hung out in the same Facebook groups and shared the same Pepe, Shiba Inu and Hawaiian shirt memes, largely unaware that those memes were being interpreted differently by each of them.

Under the harsh glare of the media spotlight, however, those internal fractures were exposed. It was the media's efforts to define the Boogaloo that pushed them to begin to define themselves.

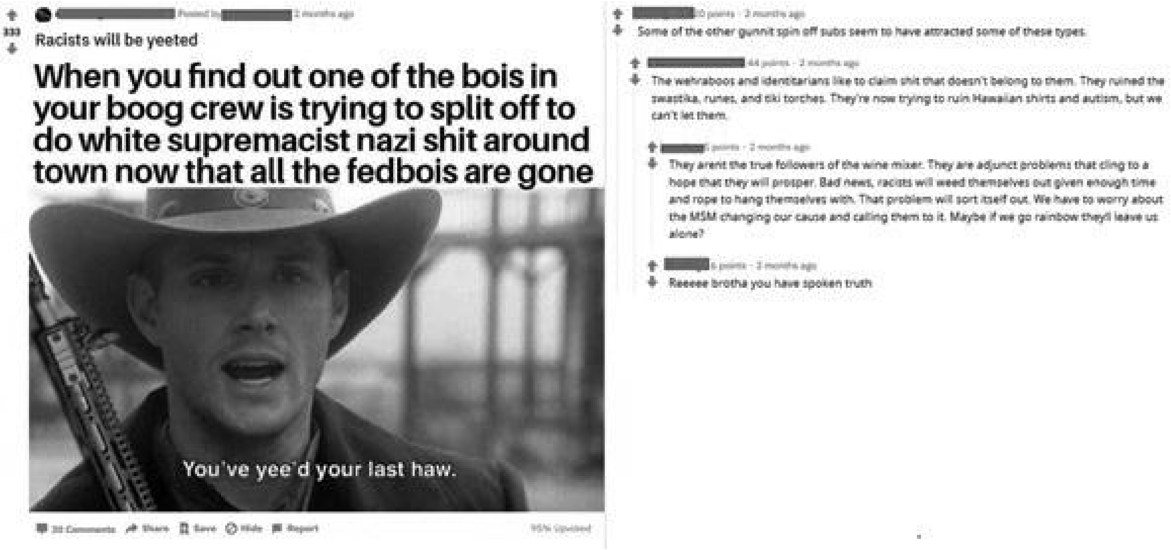
The media coverage complicated this in another way, too. As is so often the case, the visibility that the media gave sent a wave of new people flooding into the Boogaloo groups across social media, and particularly on Facebook. These new users *thought* they were joining the kinds of groups that the media had told them to expect: far-right and with at least a lean towards white nationalism. What this meant is that, just at the time the Boogaloo groups were seeking to define themselves, they also faced an influx of people looking to join far-right and white nationalist groups, thereby adding support to those elements of the existing Boogaloo community.

The closest thing the Boogaloo had to leaders at the time were the administrators and moderators of the largest Boogaloo Facebook groups, some of which had tens of thousands of members. Some of those individuals used their platform to reject the idea that the Boogaloo was a racist movement, expressing support for Black Lives Matter protesters and asserting that the Boogaloo was about opposition to law enforcement and the state, not about racial hierarchies.

That overt rejection of racism wasn't uniform, however, and there continues to be a significant racist element running through the memes and conversations in Boogaloo communities. For example, there was a brief period on some Boogaloo Reddit boards in which Boogaloo Bois of colour were posting pictures of themselves to prove that Boogaloo followers were neither all white nor white supremacists. Some of those posts garnered hundreds of positive comments and upvotes. On the same Reddit boards, however, thinly coded references to shooting black people are casually dropped in with no disapprobation from other posters.

What this has led to is an argument over who the 'true' Boogaloo Bois are, who has the right to use their symbols and who has the power to decide what they stand for. In the screenshot in Figure 3, for example, moderators of a Reddit board took a stance opposing racism (while implicitly acknowledging that 'white supremacist nazi shit' *is* a problem within Boogaloo groups). As commenters on the post noted, however, other explicitly white supremacist communities on Reddit are also using the Boogaloo symbols. Commenters suggest those groups are 'not the true followers' of the Boogaloo.

Figure 3: Discussion on a Boogaloo Reddit board



[redacted] Posted by [redacted] 2 months ago

Racists will be yeeted

When you find out one of the bois in your boog crew is trying to split off to do white supremacist nazi shit around town now that all the fedbois are gone
You've yee'd your last haw.
Comments
Share
Save
Hide
Report
95% Upvoted

[redacted] points · 2 months ago

Some of the other gunnit spin off subs seem to have attracted some of these types.

[redacted] 44 points · 2 months ago

The wehraboos and identitarians like to claim shit that doesn't belong to them. They ruined the swastika, runes, and tiki torches. They're now trying to ruin Hawaiian shirts and autism, but we can't let them.

[redacted] points · 2 months ago

They arent the true followers of the wine mixer. They are adjunct problems that cling to a hope that they will prosper. Bad news, racists will weed themselves out given enough time and rope to hang themselves with. That problem will sort itself out. We have to worry about the MSM changing our cause and calling them to it. Maybe if we go rainbow they'll leave us alone?

[redacted] 6 points · 2 months ago

Reeeee brotha you have spoken truth

To be sure, internal disagreements over what the movement stands for and where power lies are nothing new for extremist groups. The Boogaloo and other similar digital-first forms of extremism aren't completely different or separate from other forms of extremism and are likely to demonstrate many of the same dynamics and characteristics.

What does appear to be different, however, is the speed of escalation (with barely a year from a series of mostly joking memes to all-too-real murders and alleged terror plots), accompanied by lingering confusion and decentralisation. The lightning pace of radicalisation has far outstripped the process of ideological growth; in short, despite multiple committed and planned attacks, it's still not clear who the Boogaloo Bois are or what they stand for, other than violence for violence's sake.

That hollowness at the heart of the Boogaloo doesn't make it less dangerous. If anything, it makes it more volatile. For the majority, it's still mostly a funny internet joke; for a handful, it's something to kill and die for. This memetic ambiguity is likely to be easily hijacked to serve a range of agendas, or to feed into the world views of self-radicalising individuals who can read into it almost anything they want.

Depending on how you want to count, the Boogaloo as something closer to a meaningful movement than a meme is barely a year and perhaps even only a few months old. It's far too early to say what its ultimate impact will be. What it's already proven, however, is the way in which, given the right digital environment and the right external circumstances, something as ambiguous as a series of memes and jokes can rapidly transform into the kind of radicalising force that drives some individuals to ambush law enforcement, commit murder, write in their own blood across a stolen car or plot to kidnap a politician. Whatever the Boogaloo may evolve into, one thing's clear: it's not just a joke anymore.

Notes

1 Anne Helmond, Fernando N van der Vlist, 'Social media and platform historiography: challenges and opportunities', *TMG Journal for Media History*, 2019, 22(1):6–34, online.

2 Amy Forliti, 'Alleged Boogaloo members face terrorism charges in Minnesota', *ABC News*, 5 September 2020, online.

3 Richard Winton, Maura Dolan, Anita Chabria, 'Far-right "boogaloo boys" linked to killing of California law officers and other violence', *Los Angeles Times*, 17 June 2020, online.

4 Taylor Hatmaker, 'Militia tied to plot to kidnap Gov. Whitmer was removed from Facebook in boogaloo purge', *Tech Crunch*, 9 October 2020, online.

5 'Boogaloo', *Know Your Meme*, online.

6 Matt Patches, 'How "Breakin' 2: Electric Boogaloo" became a movie and then a meme', *Grantland*, 22 December 2014, online.

7 Henry Navarro Delgado, 'Far-right "boogaloo" movement is using Hawaiian shirts to hide its intentions', *The Conversation*, 23 July 2020, online.

8 Blyth Crawford, 'Chan culture and violent extremism', *Global Network on Extremism & Technology*, 31 December 2019, online.

9 Jane Coaston, 'The Virginia gun rights rally raising fears of violence, explained', *Vox*, 17 January 2020, online.

10 Tess Owen, 'The "Boogaloo Bois" are bringing their AR-15s and civil war ideology to the lockdown protests', *Vice*, 5 August 2020, online.

11 EJ Dickson, 'Far-right "Boogaloo Boys" are trying to incite violence at protests', *Rolling Stone*, no date, online.

12 US District Court, District of Nevada, 'USA vs. Stephen T Parshall, aka "Kiwi", Andrew Lynam and William L Loomis', 2 June 2020, online.

13 Derek Hawkins, 'Federal authorities file charges against 3 alleged Boogaloo followers in Nevada', *Washington Post*, 5 June 2020, online.

14 Lois Beckett, 'Air force sergeant linked to "boogaloo" movement charged in federal officer's death', *The Guardian*, 17 June 2020, online.

15 Kelly Weill, 'Sixteen "Boogaloo" followers have been busted in 7 days', *Daily Beast*, 9 October 2020, online.

16 'Brandon Caserta in anti-government TikTok video', *Detroit News*, 8 October 2020, online.

17 Ben Collins, Brandy Zadrozny, Tom Winter, Corky Siemaszko, 'Whitmer conspiracy allegations tied to "boogaloo" movement', *NBC News*, 9 October 2020, online.

Assessing the magnitude of the threats posed by hoax devices in terrorist attacks and effective countermeasures

DR JOSHUA SINAI

Professor of Practice, Counterterrorism Studies, Capitol Technology University

Laurel, Maryland, USA

Terrorist attackers generally employ real weapons in their attacks, such as firearms, improvised explosive devices (IEDs), edged weapons such as knives and new technologies such as weaponised unmanned aerial vehicles (drones).[1] Such weapons are intended to be as lethal as possible as part of the attackers' intention to cause mass fatalities and spread mass panic and anxiety throughout the larger public as a way to publicise the extremists' cause. When real weapons aren't available, terrorists will use 'hoax' firearms or explosive devices, harmless powders in the form of fake weaponised letters, or even threatening telephone calls about imminent attacks that don't occur to terrify their intended victims and harass the responding law enforcement agencies. That's especially the case for lone-actor terrorists, who lack the financial and logistical means of organised groups to acquire real weapons. In some attacks, a weapon or a vehicle used to run down pedestrians might be accompanied by an additional hoax weapon, such as a toy gun or a fake explosive device, to increase the perceived lethality of the attack. Some terrorist plots that are thwarted by counterterrorism agencies can involve hoax threats by terrorist 'wannabes'.

This article covers only the use of hoax weapons and devices during the course of real attacks by ideologically driven extremists. To discuss the magnitude of the threat posed by these types of hoax tactics and weaponry, I explore the motivation for terrorists to resort to such tactics, the types of hoax weapons used, a chronology of significant hoax incidents, and some of the early warning indicators that may be useful to law enforcers in identifying them as hoaxes, although there's always a residual risk in assessing an incident as a hoax.

Motivations to employ hoax weapons and devices

The use of hoax weapons and devices is due to several factors, such as the attackers' difficulty in acquiring real firearms, IEDs or weaponised letter bombs and packages. In these cases, the next best weapon becomes a weapon-like hoax device or a fake threatening telephone or email warning. Terrorists wearing hoax explosive belts, in particular, make it difficult for responding law enforcement officers, who might be wary of shooting at short range for fear that such a belt could be detonated and kill them and others.

Other motivating factors include a desire to cause at least some degree of disruption and panic. The attackers understand that even hoax attacks will generate massive headlines in the targeted country's media, thereby publicising their cause and projecting them as 'heroic' actors among their supporters. A final motivation is to disrupt and tie up law enforcement agencies that are forced to unnecessarily expend valuable public safety resources in responding to hoax incidents, which they must assume to be genuine.

Types of hoax attacks

In general, there are three types of hoax terrorist attacks. The first type, which is indirect, consists of communicated hoax claims of responsibility by terrorist groups or lone actors for incidents they didn't conduct, as a way to exaggerate their fighting capability. Such claims are usually made one day after an attack via a group's media arm, its supporting extremist social media forums, or both. High-profile examples include a claim (which the US Government confirmed was false) by the Islamic State of Iraq and Syria (ISIS) in mid-June 2016 that its 'covert unit' had assassinated an American military officer who was working at the Incirlik air base in Turkey, and an October 2016 claim (which the US Central Command denied) that its fighters had shot down a US A-10 Warthog aircraft in Syria.[2] A second type of hoax consists of using hoax devices as a secondary part of a real attack using a real weapon. The final type consists of issuing a hoax warning of an imminent attack, generally communicated via a telephone call or an email.

Chronology of significant hoax incidents

This is a listing of significant hoax attacks of the second and third types that have occurred worldwide since 9/11.

- 11 September 2011: The four Al-Qaeda operatives who hijacked United Airlines Flight 93 claimed to possess a bomb they were going to detonate on board the aircraft as they forced passengers to the back of the plane, although no bomb was used in the attack.[3]
- March 2016: Seif Eldin Mustafa used a hoax explosive belt to hijack EgyptAir Flight 181, which had departed from Alexandria *en route* to Cairo. The hoax device turned out to be iPhone cases tied together with cloth. When the aircraft was forced to land in Cyprus, the hijacker surrendered following several hours of negotiation.[4]
- January 2016—March 2017: Hundreds of threats, in the form of phone calls and emails, threatening imminent bomb attacks or active shooters were made to schools, social centres, and other facilities associated with Jewish communities in Australia, Britain, Canada, New Zealand and the US. The threats resulted in evacuations and police responses. In all instances, security sweeps found no evidence of physical threats. It's alleged that the suspect,

Michael Ron David Kadar, had started making the threats in 2015, but he was charged for the threats made in 2016, when he turned 18.[5] Kadar, an American-born Israeli with a history of mental instability, was subsequently arrested in Ashkelon, Israel, in March 2017 and convicted in June 2018.[6]

- June 2017: Three *jihadi* attackers rammed a van into pedestrians on London Bridge before exiting the vehicle armed with knives and wearing fake explosive belt devices and indiscriminately stabbing people in the nearby Borough Market.[7]
- August 2017: A *jihadi* driver rammed pedestrians on an avenue that was packed with tourists in Cambrils, a coastal town in Catalonia, killing 14 people and injuring more than 100 before fleeing on foot. Eight hours later, as part of the coordinated attack, a black Audi A3 ploughed into pedestrians at Cambrils, killing a female pedestrian. When the Audi overturned, five jihadists got out, some wearing fake suicide belts. Four were killed by a policeman at the scene. The fifth escaped but was later killed by the responding police.[8]
- October 2017: After using his truck to ram pedestrians along a mile-long bike path in Lower Manhattan, killing eight people and wounding 11 others, Sayfullo Saipov smashed the truck into a school bus. He jumped out of the vehicle brandishing what appeared to be two guns, but were in fact a paintball gun and a pellet gun, shouting ‘Allahu akbar’ (Arabic for ‘God is great’). At that point, a responding New York Police Department officer shot him dead.[9]
- March 2018: Daniel Frisiello sent several threatening letters containing a suspicious-looking white powder to several prominent people, including US President Donald Trump’s sons. One of the letters was opened by Donald Trump Jr’s then-wife, Vanessa Trump, inside their New York apartment. This wasn’t the first time Frisiello had sent suspicious-looking white-powder letters. He had also reportedly sent one to family members of presidential candidate Donald Trump during the 2016 presidential election campaign, threatening that the next letter wouldn’t be fake if Trump didn’t drop out of the race. In September 2018, Frisiello pleaded guilty to 13 counts of mailing a threat to injure a person and six counts of false information and hoaxes.[10]
- November 2019: Usman Khan, who had been convicted and sentenced to eight years in prison for ‘terrorism offences’ and released from prison the previous year, stabbed several pedestrians, killing two, near London Bridge. He had also strapped a fake bomb to his body. He was killed by responding police.[11]
- February 2020: Sudesh Amman, recently released from prison after serving time for terrorism-related offences, strapped a fake bomb to his body and stabbed two people on a busy street in London.[12]
- November 2020: Fejzulai Kujtim carried out a shooting and knifing attack in Vienna, killing four people and wounding 22 others. He was armed with an automatic rifle, a hand gun and a machete and wore a fake suicide vest. He was killed by responding police nine minutes after the attacks began.[13]

Advantages of using hoaxes in attacks

As demonstrated by those ten cases, there are several advantages for the perpetrators in using hoaxes in their attacks, whether as a primary or a secondary tactic. Those advantages include the relative ease of manufacture of fake weapons, their use as force multipliers when combined with real weapons, their use to intimidate potential victims by convincing people that a more lethal attack might be underway, and their use to give attackers extra time to defend against law enforcers who are uncertain about whether additional weapons, such as IEDs, might be involved.

For terrorists, especially lone actors with limited resources, even the simplest fake devices can be made to appear to be real weapons, and their deployment in an attack can generate maximum fear among potential victims. For example, the fake devices used by the London Bridge attackers in June 2017 were belts mounted with plastic water bottles wrapped in silver duct tape.[14]

In two of the 2017 attacks (August and October), the terrorists used vehicles to ram pedestrians before exiting the vehicles with hoax devices (toy guns and fake explosive belts), intending to look as though they were escalating their attacks with additional weapons. Those tactics also made the attacks appear more threatening to the responding police officers, who were concerned that firearms would be used to shoot additional victims or that bombs might be exploded to inflict greater casualties.

During an attack in which the use of a knife might be accompanied by the detonation of a possible IED, bystanders are likely to be reluctant to intervene, fearing that they might be killed in an ensuing explosion.

Indicators to pre-empt hoax attackers

It's difficult to identify hoax weapons, especially when they're used alongside by real weapons. It's possible, in the case of fake threats, to identify indicators such as references by an attacker to his exaggerated lethality, grandiose threat scenarios, the wide geographical dispersal of claimed targets, the claimed involvement of additional attackers who aren't likely to be part of the plot, and other details that often aren't present in real attacks. On the other hand, in the heat of the moment, law enforcement responders and others in the immediate vicinity mightn't be able to distinguish fake weapons from real ones, and the consequences of wrongly judging a weapon to be fake are grave enough to prevent people making that call without compelling evidence.

Conclusion

The use of hoax weapons and devices in attacks, whether as an attack's primary or secondary tactic, is likely to continue to be pervasive because of the many benefits they provide to perpetrators. Hoax attacks generate widespread media attention and heightened alarm and disruption, even if they fail to inflict lethal or other physical damage.

It's also important to anticipate new types of hoax weapons and devices being used in terrorist attacks. That includes the potential use of drones that appear to be weaponised but aren't. In December 2018, a major incident involving a non-weaponised drone at Gatwick Airport in the UK caused world-wide disruption when around 1,000 flights had to be cancelled or delayed. While that turned out to be an insider attack, with no terrorism nexus, it highlights the impact of hoax terrorist threats.[15]

Terrorist adversaries are always seeking to exploit their targeted authorities' vulnerabilities by employing real and hoax weapons and devices to spread as much panic and anxiety as possible, both in the immediate vicinity and throughout wider society. Emerging types of hoax weapons and devices, and approaches to deal with them, need to be anticipated by law makers and national security agencies.

Notes

1. Ben Hubbard, Palko Karasz, Stanley Reed, 'Two major Saudi Oil installations hit by drone strike, and US blames Iran', *New York Times*, 15 September 2019, online.
2. Glen Johnson, Nabih Bulos, 'Islamic State claims it killed American working at air base in Turkey', *Los Angeles Times*, 16 June 2016, online.
3. 'Flight 93 hijacker: "Shall we finish it off?"', *CNN*, 23 July 2004, online.
4. 'EgyptAir plane hijacked, "unstable" man arrested', *CBS News*, 29 March 2016, online.
5. 'US-Israeli teen convicted of threats against Jewish centres', *BBC News*, 28 June 2018, online.
6. 'US-Israeli teen convicted of threats against Jewish centres'.
7. 'London attack: Seven killed in vehicle and stabbing incidents', *BBC News*, 4 June 2017, online.
8. 'Barcelona and Cambrils attacks: what we know so far', *BBC News*, 27 August 2017, online.
9. Jamiles Lartey, Amanda Holpuch, Joanna Walters, Jon Swaine, 'Eight people killed in New York "act of terror" after truck drives on to bike path', *The Guardian*, 1 November 2017, online.
10. 'Man who mailed white powder to Trump's sons gets probation', *Reuters*, 20 April 2019, online.
11. 'Convicted terrorist Usman Khan kills two civilians, injures three in London Bridge attack', *The New Daily*, 30 November 2019, online.
12. Alexander Robertson, "Streatham attacker Sudesh Amman is latest terrorist to wear fake bomb vest so he can die from 'suicide by cop' and become a 'martyr'," *Mail Online*, 3 February, 2020, online.
13. Kate Connolly, Philip Oltermann, 'Vienna attack: arrests made after four killed in "Islamist terror" shooting', *The Guardian*, 4 November 2020, online.
14. Yonette Joseph, 'London Bridge attack: the implements of terror', *New York Times*, 11 June 2017, online.
15. Justin Rowlett, 'Gatwick drone attack possible inside job, say police', *BBC News*, 14 April 2019, online.

Terrorist financing: global policy challenges and initiatives in 2020

DR GORDON HOOK
Executive Secretary, Asia/Pacific Group on Money-Laundering
Sydney, Australia

Terrorist financing in itself, and as a predicate crime to money laundering,[1] challenges national, regional and global security,[2] threatens financial integrity[3] and distorts economies.[4] During the 2019 'No Money for Terror' ministerial conference in Melbourne, Minister for Home Affairs Peter Dutton remarked that the economic impact of terrorism globally was US$52 billion in 2017, according to the Global Terrorism Index. The following year, the same index cited a 38% decline, to US$33 billion. On the basis of the numbers alone, it appears that some successes may have been achieved in mitigating the global threat posed by terrorists, including their financing, but is that the correct inference?

The UN Secretary-General recently observed, in the midst of the Covid-19 pandemic, that 'terrorist and violent extremist groups see the uncertainty created by the pandemic as a tactical advantage.'[5] Those comments are supported by a recent Financial Action Task Force (FATF) publication on the risks of money laundering and terrorism financing associated with Covid-19. The pandemic has led to the implementation, globally, of a range of financial assistance packages, including social assistance and tax relief, which may represent new avenues for criminal exploitation.[6] On that basis, FATF urged that 'governments should emphasise the importance of implementing the risk-based approach when mitigating the risk of funds being diverted to support terrorists and terrorist groups.[7]

How are countries responding to their obligations to implement counterterrorism financing (CTF) obligations and what are some of the more significant issues to be concerned with? Before those questions are answered, it's worthwhile to revisit, if only briefly, the international CTF standards and some of the key responses by the FATF.

In summary, according to the UN, terrorism financing occurs when a person provides or collects funds intending or knowing that they'll be used, in full or in part, to carry out a terrorist offence or cause death or serious injury or to compel a government or international organisation to do or to abstain from doing anything.[8] While the UN requires a link between the financing of terrorism and an act or acts of terrorism, the FATF standards go beyond that and require countries to criminalise the financing of terrorist organisations and individual terrorists without a link to a specific acts, consistent with UN Security Council resolutions in which countries are required to prohibit nationals or any persons and entities within their territories from making funds, financial assets or economic resources available to terrorists or terrorist organisations.[9] Unlike money launderers, who seek primarily to profit from their behaviour, terrorist financiers seek to support terrorists or terrorist activities without a profit motive.

Terrorist groups rely on a variety of fundraising and fund-movement methods to achieve their objectives, ranging from extortion, kidnapping for ransom and drug trafficking to less violent or less serious measures, including taxation of legitimate trade, abuse of not-for-profits (including sham charities), online crowdfunding, migrant smuggling and trade in oil, other natural resources and illicit antiquities.[10]

In the last category, the funds generated from the sale of oil by Islamic State (IS) to support its campaign in 2015 were staggering: '80,000 and 120,000 barrels per day, generating USD $2–$4 million in daily profits. IS brought in USD $500 million from oil and gas sales in 2015 alone.'[11] In addition, the IS trade in antiquities to raise funds for IS-related attacks in Syria and Iraq saw the world respond with shock, not only to the abuse of historic art and archaeological antiquities but to the scale of funds raised.[12]

In late 2020, the FATF reported that the fundraising activities of IS continue to pose a serious global threat involving numerous revenue sources, including real estate investments, offshore investments in 'secrecy' tax havens and the counterfeiting of medical drugs during the Covid-19 pandemic, even though, at the same time, IS has had to draw on its own financial reserves numbering in the low hundreds of millions of dollars.

Global compliance with FATF standards

The requirement to criminalise terrorist financing was added to the FATF standards at a special plenary session of the FATF in the months following the 11 September 2001 attacks in the US. However, global compliance with those requirements in the period between 2003 and 2012 was very low. More than half of more than 160 countries assessed in that period failed to implement, to any satisfactory degree, the required provisions in domestic law, and even fewer countries displayed effective implementation of their CTF laws, including investigating and prosecuting offenders. From 2015 to 2016, the FATF undertook a global assessment of countries, referred to as the 'Terrorist Financing Fact Finding Initiative'. That review determined that, out of 194 countries, 13 (including many considered at high risk of terrorist financing) still had 'fundamental' gaps' in their legal CTF frameworks, while many other countries still had some serious gaps, albeit not 'fundamental'. Those gaps meant failure by many countries to fully address and effectively target their terrorism financing risks, including those that may be related to IS. On that point, relatively few of the 194 countries had obtained convictions for terrorist financing.[13] In 2020, effective compliance with the CTF standards is still a global concern.

The 'Panama Papers' revelations in 2016 and then the 'Paradise Papers' in 2018 raised even more concerns in the global community about the extent to which terrorism financing was occurring through products offered by offshore financial centres, and so-called tax havens, to hide and move illicit funds. One report put the estimate of funds in offshore havens at 10% of global GDP or US$7.5 trillion.[14]

Partly in response to those revelations, the FATF commissioned studies into the risks posed by poor implementation of the beneficial ownership standards[15] and found that there were significant risks of terrorism financing in countries (including offshore havens) that fail to implement beneficial ownership requirements.

Emerging terrorism financing issues

Subsequent to raising funds, terrorists are faced with the question of how to move their money. It has been observed that 'terrorists seem to choose methods of moving funds that take into account issues of: volume, risk, convenience, simplicity, costs, and speed.'[16] However, there are two points to note.

As law enforcement authorities tighten the noose on established and previously 'reliable' methods to raise and move terrorist funds, novel methods emerge to address vulnerability-closure, including investments in the food, farming, clothing and construction industries. However, there are concerning levels of understanding by many countries across the globe of their own terrorism financing risks. The FATF standards require countries to identify, assess and understand their own risks, yet many countries, including those that are considered by the FATF and other bodies as being at 'very high risk' of terrorist financing, fail to appreciate the risks within their own borders and within their regional context that affect their domestic risk environment.

With those points in mind, a number of areas present serious and ongoing concerns in relation to terrorism financing and are currently the focus of the FATF and other bodies. They're also areas where decision- and policymakers could focus their efforts further.

Social media and terrorism financing

As one academic has observed, terrorist structures, which are traditionally built of loose-knit cells, divisions and subgroups, are ideally suited for soliciting funds on the internet.[17] A recent joint typologies report on crowdfunding and terrorist financing estimated that 'by 2021, 3.02 billion people will be using some form of social media service.'[18] Those services are easy to use, expand the reach of organisations to a global scale and provide terrorists and terrorist organisations with a valuable channel to generate large amounts of money in a short period from very small amounts per donor.

A number of cases in the joint report illustrate funding relevant to financing foreign terrorist fighters' travel expenses to conflict zones, sending funds offshore to support local terrorist activities in other jurisdictions, and the purchase of propaganda materials such as flags and other symbols. Vulnerabilities involving social media platforms include anonymity and encryption. However, even though law enforcement authorities have spent considerable time addressing the use of social media for content and propaganda, it's been remarked that 'comparatively little attention has been given to its potential role in countering terrorist financing.'[19] More needs to be invested in this area, especially to identify users who act on behalf of others to raise funds.

Virtual currencies and terrorism financing

Virtual currencies (cryptocurrencies or digital currencies) are decentralised units of value untied to fiat currency and without supervisory oversight. 'They possess their own unit of account … while the respective value is determined by supply and demand and trust in the system.'[20]

According to the RAND Corporation, virtual currencies are fast becoming a concern as new sources of financing for terrorist activities.[21] Unlike currency notes, virtual currencies 'do not leave a paper trail for law enforcement to follow and in the case of decentralised digital currencies, records of transaction are not maintained by an intermediary'.[22] That makes it difficult to construct prosecution briefs should investigations undercover people or groups raising funds for the purposes of terrorism-related acts or organisational purposes such as propaganda and recruitment. It also makes it difficult to undertake tracing and freezing of virtual assets involved in the funding of organisations or their activities. Establishing robust supervisory structures to regulate the use, and exchange, of virtual currencies is an important step in addressing terrorism financing risks associated with these products.

As commented by the director of the US Financial Crimes Enforcement Network:

> As new technologies emerge to serve the financial industry, FinCEN recognizes the need for sustained industry cooperation and a flexible legal and regulatory architecture that encourages innovation while allowing appropriate regulatory engagement and effective AML/CFT oversight.[23]

In October 2019, in response to that call and others from the international community, the FATF amended its suite of recommendations to include new measures designed to address the risks of serious financial crime relating to virtual currencies and service providers. Recommendation 15 was significantly expanded to require countries to formally assess their risks in this area and requiring service providers to be licensed and registered, which means they must be supervised for compliance with anti-money-laundering / counter-terrorism-financing obligations across a range of measures in the FATF standards, not just those relevant to virtual currencies.

It's early days in the FATF assessment process but, of those countries that have so far been assessed for compliance with the new standard, many aren't achieving a satisfactory level of compliance, thereby posing an ongoing terrorism financing risk.

Illicit arms trafficking and terrorist financing

In a 2017 report published by the Royal United Services Institute in the UK, the links between legal and illegal acquisition of firearms linked to terrorist financing was examined. The report noted that:

> the use of firearms (particularly automatic weapons) has resulted in casualties on a far greater scale. As such, increased focus should be placed on identifying and disrupting financial flows [for terrorist financing] related to the trade in illicit firearms.[24]

The report also referenced Australia's 'grey market', which was said to comprise an estimated 250,000 unregistered guns owned by individuals for recreational purposes. This potential weapons source was highlighted as a risk for acquisition by 'lone wolves' or terrorist groups at low cost. In highlighting this, the report referred to the 2014 Lindt Cafe siege in Sydney, in which an unregistered sawn-off shotgun was used.

In June and October 2020, partly in response to the report and partly as a result of the accumulation of FATF member case studies, including from Australia, the FATF agreed on a new terrorist financing research project on the links between arms trafficking and terrorism financing. In proposing the project, the FATF identified some key areas of vulnerability and risks involving legal and illegal sales of firearms and ammunition. For legal sales, there's concern that arms purchased have made and will continue to make their way into the black market and to terrorists. For illegal sales, the project will look at the acquisition of illegally produced and marketed firearms for the purpose of supplying them to lone-wolf terrorists and terrorist groups.

Some of the issues to be considered and addressed in the new project will be the identification regulatory gaps and how to address them; arms supply sources, including national stockpiles and the chain leading from those sources; and the use of cash to acquire illegal firearms on the black market, to name just a few. The project is expected to report back to the FATF in 2021 with case studies and recommendations.

Conclusion and recommendations

Terrorism financing isn't abating. As long as terrorists and terrorist organisations seek to progress their agenda through the commission of violent acts and the recruitment of individuals to their cause, funds will be necessary. As one avenue of fundraising is identified by policymakers and measures are put in place to address vulnerabilities, other avenues open. Countries therefore need to continually undertake assessments of their terrorism financing risks, not just on a periodic basis but as circumstances change, and to align their policies and resources to those new and emerging risks.

More needs to be done to address the financing challenges associated with social media and with virtual currencies, as well as to identify gaps in national legislation that result in the trade in firearms for terrorist purposes. It will be interesting to review the outcomes of the new FATF project on the links between terrorist financing and arms trafficking.

Hence, in answer to the questions posed at the beginning of this paper, the fall in only one year of global funds generated for terrorism and terrorist support doesn't necessarily translate into long-term successes. Complacency is a vulnerability easily exploited by terrorists. As governments play catch-up with legislative responses or fail to close gaps due to their poor understanding of their own risks, terrorists are many steps ahead, looking for new vulnerabilities and gaps to exploit.

Notes

1 The FATF requires the inclusion of terrorism financing as a predicate crime to money laundering. FATF glossary definition of 'designated categories of offences.'

2 For instance, in Australia the National Counter-Terrorism Plan includes terrorism financing as a significant and growing national security threat; Australia New Zealand Counter-Terrorism Committee, *National Counter-Terrorism Plan*, 4th edition, 2017, online.

3 General Assembly resolution S20-2, *Political Declaration and Action Plan against Money Laundering*, A/RES/S-20/2, 21 October 1998: 'countering the world drug problem together … the problem of laundering of money … has expanded internationally to become a global threat to the integrity, reliability and stability of financial and trade systems and even government structures', UN, New York, 10 June 1998.

4 F Schneider, D Enste, D. (2002), *Hiding in the shadows: the growth of the underground economy*, Economic Issues series, International Monetary Fund, March 2002, online; 'The fight against money laundering', *Economic Perspectives: An Electronic Journal of the US Department of State*, May 2001, 6(2), online.

5 'Secretary-General's remarks to the Security Council on the COVID-19 pandemic', UN, New York, 2 July 2020, online.

6 Financial Action Task Force (FATF), *COVID-19-related money laundering and terrorist financing: risks and policy responses*, FATF, Paris, France, 2020, 5, online.

7 FATF, *COVID-19-related money laundering and terrorist financing: risks and policy responses*, 10.

8 General Assembly resolution 54/109, *United Nations Convention for the Suppression of Terrorist Financing*, A/RES/54/109, UN, New York, 9 December 1999, Article 2.

9 Criminalising terrorism financing solely on the basis of aiding and abetting, attempt, or conspiracy is insufficient to meet this additional requirement.

10 Other techniques include sham charities designed to exploit the good intentions of donors and simply asking for money or other assets (which, surprisingly, works in some cases).

11 Homeland Security Committee, *Cash to chaos: dismantling Isis' financial infrastructure*, majority staff report, US Congress, Washington DC, 2016.

12 See, for instance, Amr Al-Azm, Katie A Paul, *Facebook's black market in antiquities trafficking, terrorism, and war crimes*, Athar Research Project, June 2019, online.

13 FATF, *Annual report 2015–16*.

14 Annette Alstadsæter, Niels Johannesen, Gabriel Zucman, *Who owns the wealth in tax havens? Macro evidence and implications for global inequality*, working paper 23805, National Bureau of Economic Research, Cambridge, Massachusetts, September 2017, online.

15 FATF — Egmont Group, *Concealment of beneficial ownership*, FATF, Paris, France, 2018, online.

16 Michael Freeman, Moyara Ruehsen, 'Terrorism financing methods: an overview', *Perspectives on Terrorism*, 2013, 7(4).

17 Gabriel Weiman, *Terrorism in cyberspace: the next generation*, Columbia University, New York, 2015.

18 *Social media and terrorism financing*, Asia/Pacific Group on Money Laundering & Middle East and North Africa Financial Action Task Force, Sydney, Australia, 2019, online.

19 *Social media and terrorist financing: what are the vulnerabilities and how could public and private sectors collaborate better?*, Royal United Services Institute, London, 2019, online.

20 C Brenig, R Accorsi, G Müller, 'Economic analysis of cryptocurrency backed money laundering', paper 20, *ECIS 2015*, 6.

21 Rand Corporation (2019), *Terrorist use of cryptocurrencies: technical and organisational barriers and future threats*, online.

22 Stephen Platt, *Criminal capital: how the finance industry facilitates crime*, Palgrave Macmillan, UK, 2015, 50.

23 Jennifer Calvary, 'Stopping terror finance: a coordinated government effort', testimony to the US House of Representatives Committee on Financial Services Task Force to Investigate Terrorism Financing (FinCEN), 24 May 2016, online.

24 *Lone-actor and small cell terrorist attacks: a new front in counter-terrorist finance?*, Royal United Services Institute, 2017, online.

Countering terrorist financing: strengthening Indonesia–Australia collaboration

SYLVIA LAKSMI
PhD Candidate, Australian National University
Canberra, Australia

The degradation of the capabilities of Islamic State (IS), including the territory that enabled it to claim a 'caliphate', financial assets and revenue by multinational military coalitions in 2017,[1] and the death of Abu Bakr al-Baghdadi,[2] were huge blows to the group and its associates. What does it mean for life after the so-called caliphate? History has shown that the death of Osama bin Laden in 2011 didn't lead to the end of al-Qaeda; likewise, the IS caliphate wasn't just territorial but also a caliphate of the mind, as envisioned by the group's leaders.[3] The existence of and support for this type of caliphate has remained a persistent challenge for the world. Governments have particularly focused efforts on terrorism financing to disrupt the viability of the caliphate.

Whatever other lines of action can be used to degrade the power of concepts such as IS's caliphate or other extremist propaganda and to reduce extremists' ability to commit violence, governments must maintain a focus on disrupting and reducing terrorist groups' financing. The work of Indonesia and Australia provides powerful examples.

This paper outlines four key points regarding the bilateral partnership between Indonesia and Australia in developing counter-terrorism-financing (CTF) measures. I discuss a comparative analysis between the two countries' initiatives, the current tactical relationship and the challenges posed in the contemporary regional CTF context. Finally, I propose several recommendations to improve comprehensive strategic partnerships to diminish terrorist money flows.

CTF strategic policing in Indonesia and Australia

The bombing attack in Bali in October 2002 was the first sign of violent Islamist extremism becoming a sharper issue in the Asia–Pacific region. The fight against terrorism became prominent for local authorities, particularly dealing with terrorist funding. CTF policymaking in Indonesia and Australia refers to compliance with international standards imposed by the Financial Action Task Force (FATF), which is an intergovernmental body founded in 1989 to develop policies on money laundering and associated crimes.[4]

The Indonesian and Australian CTF strategy framework can be divided into two major components.

First, both Indonesia and Australia established a robust legal groundwork for CTF.[5] In 2002, Indonesia established a financial intelligence unit[6] called the Indonesian Financial Transaction Reports and Analysis Center (INTRAC), which works administratively with financial regulators to supervise industries.[7] Australia used its existing Australian Transaction Reports and Analysis Centre (AUSTRAC), formed in 1991,[8] for this purpose. AUSTRAC works not only as an administrative body but also as an industry regulator that promotes the compliance of reporting parties by applying values of education, persuasion, consistency, proportionality and accountability.[9]

Second, both countries emphasise the domestic implementation of targeted financial sanctions relating to terrorism and terrorist financing pursuant to UN Security Council resolutions 1267 (1999)[10] and 1373 (2001).[11] Indonesia and Australia continue to improve the 'freezing without delay'[12] mechanism that applies to property associated with terrorism financing offences.[13] However, along with those useful countermeasures, it's also necessary to reduce the ability of terrorists to legitimise their sources of funds and their ability to funnel funds into various other activities, such as for military training, propaganda, business activities and support to terrorist families, all of which enable terrorist groups' capabilities to commit violence.[14]

Current best practices of cooperation in the region

Indonesia and Australia have been expanding their cooperation on CTF through intelligence information exchanges, regional risk assessments and public–private partnerships.

Since 2017, INTRAC and AUSTRAC have cemented a strategic partnership by establishing intelligence information exchange working groups in collaboration with Southeast Asian and New Zealand financial intelligence units (FIUs). The groups are focused on the identification of IS-affiliated organisations in the Asia–Pacific region, the formulation of red flag indicators of terrorist financing risks and capacity-building programs. The programs consist of the establishment of the multilateral analyst exchange program,[15] Analyst Hubbing, and the regional Financial Intelligence Analysis Course, which have been developed to enhance understanding, analysis, capabilities and sharing of intelligence information and expertise held by Southeast Asian countries and close partner FIUs such as those in Australia and New Zealand.[16] To facilitate this collaboration, INTRAC, AUSTRAC and FIUs in Southeast Asia and New Zealand have been developing a secure online regional information-sharing platform since 2019. The Terrorist Financing Information Sharing Platform will be used as a medium for exchanging intelligence among FIUs, including to provide quick responses following terrorist incidents, and to generate watchlists of persons and financial transactions.

INTRAC and AUSTRAC have also initiated an innovative regional risk assessment that examines trends in trends and risks of terrorism funding. The objective is to strengthen legal, regulatory and operational frameworks in identifying, interrupting and prosecuting terrorist financiers, including foreign terrorist fighters.[17]

INTRAC and AUSTRAC actively promote the practice of public–private partnerships pursuant to the FATF norms. A robust relationship among public and private organisations is essential in tracking terrorists' money trails, including extending access to information on targets. For instance, AUSTRAC launched the Fintel Alliance in 2017 as a public–private partnership that involves 29 government and private-sector members (domestic and international), in working together to fight against money laundering, terrorism financing and other serious crime. The alliance incorporates law enforcement and security agencies, and also members from private organisations such as major banks, money remittance businesses and gambling operators.[18]

However, there are some barriers to cooperation between the two countries, such as legal framework limitations on information sharing and confidentiality and differing levels of capability in handling terrorism financing cases. Examples include the use of technology to support the analysis process, the capabilities and skills of their analysts, varying levels of cooperation with their respective intelligence and law enforcement agencies, and access to bank records from financial industries.

Contemporary challenges in disrupting terrorism funding

Notwithstanding that Indonesia and Australia have been developing CTF initiatives over many years, the threat environment grows increasingly complex. There are four main challenges in disrupting funds to terrorists in the region.

First, crowdfunding through social media platforms is one of the evolving risks of fundraising in the region.[19] Crowdfunding is vulnerable to exploitation by terrorists through not-for-profit organisations and humanitarian activities.[20] Recently, the Covid-19 pandemic has presented another obstacle to the war against terrorism financing. There are concerns that terrorist groups have used the crisis to raise and move funds to finance their malicious operations[21] under the guise of humanitarian aid through legitimate charities or not-for-profits[22] and use the internet to facilitate crowdfunding activities.

Second, it's been noted that some returning foreign fighters may support the resurgent Jemaah Islamiyah (JI) terrorist group, which sent recruits to Syria.[23] The re-emergence of JI has been identified as a current threat to regional security. Para Wijayanto, a businessman running palm oil plantations,[24] who was believed to be JI's new leader and was arrested in 2019,[25] admitted that the organisation had regrouped and restructured using his personal funds.[26] The term 'neo-JI' is used as a rebranding strategy to promote new activities and to attempt to change perspectives on the group from clandestine and underground to a legitimate 'legal above-ground economic and social organisation'.[27] The group refocused its mission to a 'soft approach' through preaching programs (*dakwah*), Islamic boarding schools, entrepreneurship training and social programs to improve family welfare for its members and the broader community.[28]

Third, territorial loss has become a push factor for IS militants and foreign fighters to move from Syria and Iraq to the Philippines,[29] Khorasan[30] and Jammu and Kashmir.[31] Some Indonesian nationals have relocated to Khorasan[32] or attempted to join the Islamic State Jammu and Kashmir group.[33]

An emblematic example of this shift is the Indonesian couple who, after failing to travel to Syria, carried out the Jolo Cathedral bombing in January 2019, killing 20 people.[34] The Australian Government has also noted a heightened likelihood of Australian foreign fighters relocating to the Philippines in order to join terrorist groups there. For example, Australian nationals Robert Cerantonio[35] and Abu Adam al-Australi appeared in an IS propaganda video and urged Muslims to join the jihad in the Philippines.[36] Therefore, the increasing threat of violent extremism in Southeast Asia, and particularly in the Philippines, has strong implications for security policymaking.[37] Indonesia[38] and Australia[39] also face problems in handling foreign fighter returnees who request repatriation.

Finally, another challenge is represented by the advancing technology of financial payment systems. Innovation in financial technologies brings positive opportunities to developing countries,[40] but those opportunities also pose substantial risks, such as the misuse of cryptocurrencies by terrorists.[41] Terrorists might use those platforms not only to facilitate fundraising for terrorist attacks but also for other suspicious transactions not directed to attacks but which enable terrorist organisations to operate and retain or build support, such as actively recruiting members, supporting foreign fighters' travels, social welfare for terrorists' widows and children and support for terrorist inmates' wives.[42]

Framing a mutual alliance

In the face of these challenges, while there have been some notable achievements and successes in the longstanding and productive CTF cooperation between Indonesia and Australia, there's still a lot of work to be done to address the hurdles. That's to be expected, because just as terrorist groups are adaptive so countermeasures should be. A range of considerations and factors will influence the effectiveness of policy responses. This section proposes several recommendations for potential policy options.

First, there's a greater need to enhance cooperation on information exchange. The Terrorist Financing Information Sharing Platform – secure joint online information-sharing platform – will be an effective tool to be used among FIUs for providing timely responses to prevent future attacks, thus mitigating the risks of misusing the financial system for terrorism purposes. Furthermore, Indonesia and Australia could unlock more opportunities by improving the public–private partnership program and continuing to enhance information sharing in the region against the threats of extremism and terrorist fighters.

Second, the two countries should strengthen practical cooperation in addressing the challenges posed by online communication and digital payment systems. Because those platforms are susceptible to misuse by terrorist groups, governments should enhance the standards of their respective and joint transaction monitoring and supervisory frameworks by applying four strategies:

- Establish or improve a central oversight body for supervising and monitoring online charities-based crowdfunding activities.
- In response to occasional online transactions, implement mechanisms to identify, validate and verify the digital identities of customers.
- Newly sophisticated technologies in financial systems, including virtual assets and new payment methods, pose risks and threats requiring mitigation by authorities.
- Law enforcement efforts and legal sanctions for noncompliant providers should be improved and remain responsive to the changing environment.

Furthermore, considering the prospect of abuse of donation funds to charities by terrorists, governments should remain vigilant and implement regulations on crowdfunding and not-for-profit organisations.

Notes

1 Mohammed Nuruzzaman, 'The Islamic State is on its knees, but its legacy will long haunt the Middle East', *The Conversation*, 17 July 2017, online.

2 Rukmini Callimachi, Falih Hassan, 'Abu Bakr al-Baghdadi, ISIS leader known for his brutality, is dead at 48', *New York Times*, 27 October 2019, online.

3 Patrick B Johnston, Mona Alami, Colin P Clarke, Howard J Shatz, *Return and expand? The finances and prospects of the Islamic State after the caliphate*, RAND Corporation, Santa Monica, 2019, online.

4 Financial Action Task Force (FATF), *International standards on combating money laundering and the financing of terrorism & proliferation: the FATF recommendations*, June 2019, online.

5 In criminalising terrorist financing, Indonesia enacted Law No. 8 of 2010 concerning Money Laundering and Anti-Terrorist Financing Law Number 9 of 2013 (Undang-Undang tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme, UU no. 9 year 2013. LN No. 50 Year 2013, TLN No. 5406), and Australia passed the *Suppression of the Financing of Terrorism Act 2002* (Cwlth).

6 A financial intelligence unit (FIU) works on collecting, analysing and disseminating intelligence information to the stakeholders.

7 International Monetary Fund, *Financial intelligence units: an overview*, 2004, online.

8 AUSTRAC was named as the Cash Transaction Report Agency in 1989 and renamed in 1991; Neil Jensen, 'Creating an environment in Australia hostile to money laundering and terrorism financing: a changing role for AUSTRAC', *Macquarie Journal of Business Law*, 2008, 93–112, online.

9 Jensen, 'Creating an environment in Australia hostile to money laundering and terrorism financing: a changing role for AUSTRAC'.

10 This resolution is related with imposed sanctions to any person or entity either 'designated by, or under the authority of, the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, including in accordance with the Al-Qaida/Taliban sanctions regimes'; UN, Resolution 1267, 1999, online.

11 UN, Resolution 1373, 2001, online.

12 'The Glossary of the FATF Recommendations defines without delay, with respect to the Al-Qaida/Taliban sanctions regimes, as ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, or the 1988 Committee). For the purposes of resolution 1373(2001), the term without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation.' FATF, *International best practices: targeted financial sanctions related to terrorism and terrorist financing (Recommendation 6)*, June 2013, 9, online.

13 Asia/Pacific Group on Money Laundering (APG), *Anti-money laundering and counter-terrorist financing measures: Indonesia mutual evaluation report*, September 2018, online.

14 APG, *Anti-money laundering and counter-terrorist financing measures: Australia mutual evaluation report*, April 2015, online.

15 The Nusa Dua Statement was adopted and published at the 2nd Counter-Terrorist Financing Summit in Bali, Indonesia, 2016, online.

16 The Bangkok Communiqué document was adopted and published at the 4th Regional Counter-Terrorism Financing Summit in Bangkok, Thailand, 2018, online.

17 AUSTRAC, *The regional risk assessment on terrorist financing*, 2016.

18 AUSTRAC, *Fintel Alliance*, online.

19 Agus Santoso, Sylvia W Laksmi, 'Regional terrorism financing risk assessment framework: Southeast Asia and Australia, Counter Terrorist Trends and Analyses, October 2016, 8(10), online.

20 FATF, *Emerging terrorist financing risks*, October 2015, online.

21 FATF, *COVID-19-related money laundering and terrorist financing: risks and policy responses*, May 2020, online.

22 FATF, *Emerging terrorist financing risks*.

23 Daveed Gartenstein-Ross, Colin P Clarke, Samuel Hodgson, *Foreign terrorist fighters from Southeast Asia: what happens next?*, International Counter-Terrorism Centre, The Hague, 17 February 2020, online.

24 Wahyudi Soeriaatmadja, 'Indonesia uncovers neo-JI terror group that runs oil palm plantation business for funding', *The Straits Times*, 2 July 2019, online.

25 AP, 'Indonesia arrests alleged Jemaah Islamiah terrorist network leader Para Wijayanto', *ABC News*, 2 July 2019, online.

26 Supreme Court of Indonesia, *Verdict of Para Wijayanto No. 308/Pid.Sus/2020/PN Jkt.Tim*, 2020.

27 Alif Satria, 'The Neo-JI threat: Jema'ah Islamiyah's resurgence in Indonesia follows an old playbook', *New Mandala*, 16 August 2019, online.

28 Supreme Court of Indonesia, *Verdict of Para Wijayanto No. 308/Pid.Sus/2020/PN Jkt.Tim*.

29 Zachary Abuza, Colin P Clarke, 'The Islamic State meets Southeast Asia: ISIS seeks new outposts across the Indian Ocean', *Foreign Affairs*, 16 September 2019, online.

30 Ahmad Syamsudin, Tia Asmara, Muzliza Mustafa, 'UN: Islamic State recruitment of Southeast Asians shifts to Afghanistan', *Benar News*, 7 February 2020, online.

31 Amira Jadoon, *An idea or a threat? Islamic State Jammu & Kashmir*, Combating Terrorism Center at West Point, 9 February 2018, online.

32 Petir Garda Bhawa, 'JAD Terrorism Fund Comes from Many Countries, Police Say', *Tempo.Co*, 24 July 2019, online.

33 Supreme Court of Indonesia, *Verdict of Farid Ramadhan No. 377/Pid.Sus/2020/PN Jkt.Tim*, 2020.

34 Ana P Santos, 'Who were the Indonesian husband and wife behind Jolo bombing?', *Rappler*, 27 December 2019, online.

35 Reuters, 'Robert Cerantonio, leader of Australia's "tinnie terror" plot jailed for seven years', *South China Morning Post*, 3 May 2019, online.

36 Kate Hodal, 'Australian Islamic preacher arrested in Philippines over alleged Isis links', *The Guardian*, 12 July 2014, online.

37 Clive Williams, 'Marawi battle has implications for Australians', *The Interpreter*, 24 October 2017, online.

38 Cameron Sumpter, 'Returning Indonesian extremists: unclear intentions and unprepared responses', policy brief, International Centre for Counter-Terrorism, The Hague, July 2018, online.

39 Marcus Tantau, 'Australia addresses the growing threat of returning foreign fighters', *The Diplomat*, 31 July 2019, online.

40 Department of Home Affairs, *Chair's Statement, 2019 'No Money for Terror' Ministerial Conference on Counter-Terrorism Financing*, Australian Government, November 2019, online.

41 V Arianti, Kenneth Yeo Yaoren, 'How terrorists use cryptocurrency in Southeast Asia', *The Diplomat*, 30 June 2020, online.

42 Sylvia W Laksmi, 'Nexus between charities and terrorist financing in Indonesia', *Counter Terrorist Trends and Analyses*, September 2019, 11(7), online.

Demystifying the terror–crime nexus in Australia

DR JOHN COYNE

Head of Strategic Policing and Law Enforcement.
Head of the North and Australia's Security, ASPI

Canberra, Australia

Nobel Prize-winning Polish American poet, writer and diplomat Czeslaw Miloz, reflecting on Stalinist Eastern Europe, once argued that 'the true enemy of man [humankind] is generalisation'.[1] While Stalin is long gone, and the language is now dated, the quote aptly reflects the pitfalls of adopting overly generalised approaches to the analysis of any nexus between terror and crime.

There ought to be little doubt that there are connections of varying degrees between organised crime and terrorism across the globe.[2] Nevertheless, further generalisations and the inevitable sweeping statements that so often follow them regarding the terror–crime nexus in Australia, as well as that observed in our near region, aren't very helpful to policymakers. In some cases, policy developed based on such generalisations runs the risk of worsening the problem.[3]

In this chapter, I explore the challenge of the terror–crime nexus, primarily in Australia, as well as its essential characteristics. I then consider the additional challenges of the nexus in Australia's near region.

A problem of definitions

It's clear to even the most casual observer that, globally, there have been connections between terrorism and crime for several decades, if not longer. The all too familiar link between the Irish Republican Army and organised criminal activities during the Northern Ireland troubles, which led to the movement of many members into a life of crime, illustrates this well.[4] Similarly, Hezbollah's ongoing involvement in the global cocaine and illicit tobacco markets raises questions about where and when a terrorist group becomes a criminal group with extremist views.[5]

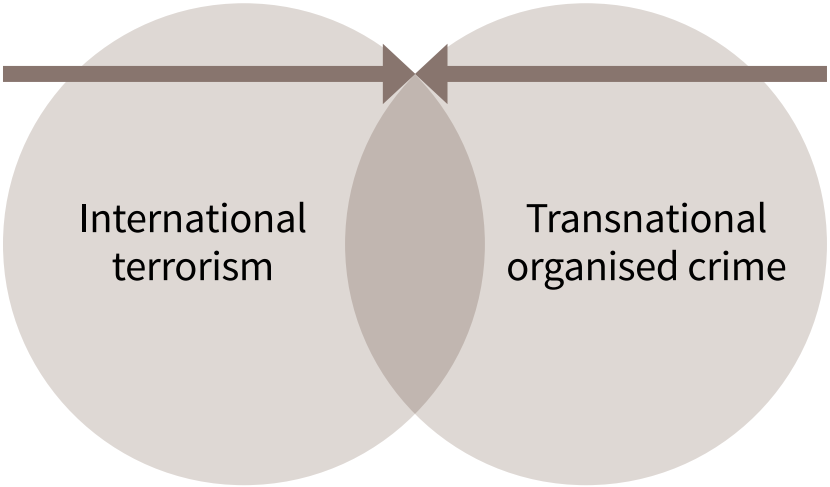
The rise of narco-terrorism in central America, particularly that involving Mexican organised crime groups, illustrates how criminal groups can take on terrorist characteristics.[6]

Academic Klaus von Lampe has identified more than 200 different definitions of 'organised crime',[7] and by 2011 Joseph Eason and Alex Schmid had already collected more than 250 academic, government and intergovernmental definitions of 'terrorism'.[8] Schmid argues that these definitions provide academic theorists with 50,000 possible combinations.[9] While many a media outlet would like it, no simple Venn diagram (see Figure 4) of terror–crime relationships that conveys anything beyond superficial meaning is possible, not even for Australia. The exact nature of these connections and relationships makes them complex, and extracting much meaning from simple diagrams becomes problematic.

Where are we now?

Old and new terrorist groups alike use crime to fund their nefarious activities.[10] Globally, evidence has emerged to suggest that the decline in state sponsorship of terrorism has driven groups such as Hezbollah, the Taliban, al-Shabaab and Islamic State to engage in a range of serious and transnational crimes.[11] From kidnap and ransom to piracy and drug distribution, terrorist groups are using crime to support their causes financially. In doing so, they're inevitably working more closely, out of necessity, with criminal groups. And there are more than a few criminal groups that are willing to work with anyone to turn a profit.

Figure 4: The simplified terror–crime nexus



For many terrorist groups, crime is a necessary means to an end, not to mention an act of political defiance. For some individuals, though, the extremist cause is simply a convenient justification for crimes, and the balance of motivation can shift from extremism to simple criminality for both organisations and individuals through time. Criminal motivation certainly seems to be the case for many of the Hezbollah members involved in the global cocaine trade.[12]

In Australia's case, there's no clear evidence of a general convergence between terrorism and transnational organised crime. There has been, however, an emergence of religious and political ideology among some organised crime groups. The New South Wales 'Brothers 4 Life' street gang has consistently demonstrated how a fusion of religious extremism with criminal activities produces a new dynamic in organised crime.[13] The same groups have shown how connectivity between convicted terrorists, even in maximum-security prisons, can result in the radicalisation of others. It's still not clear whether the use of religion and politics in such groups is opportunism among a small number of charismatic individuals or part of a broader trend.

In the region, terrorism or ethnic conflicts with a crime nexus have always been the prevailing narrative. For example, many of the activities by the Abu Sayyaf and Maute groups in the southern Philippines have appeared to be often more about crime and profit than ideology.[14] Similarly, rent-taking by ethnic armed groups in Myanmar's Shan State, in their part of the regional synthetic drug manufacturing and smuggling networks, is criminal. Of course, the ethnic groups are using the funds to continue to support their specific ideological causes, but there appears to be a genuine possibility that ideology isn't the sole driver.

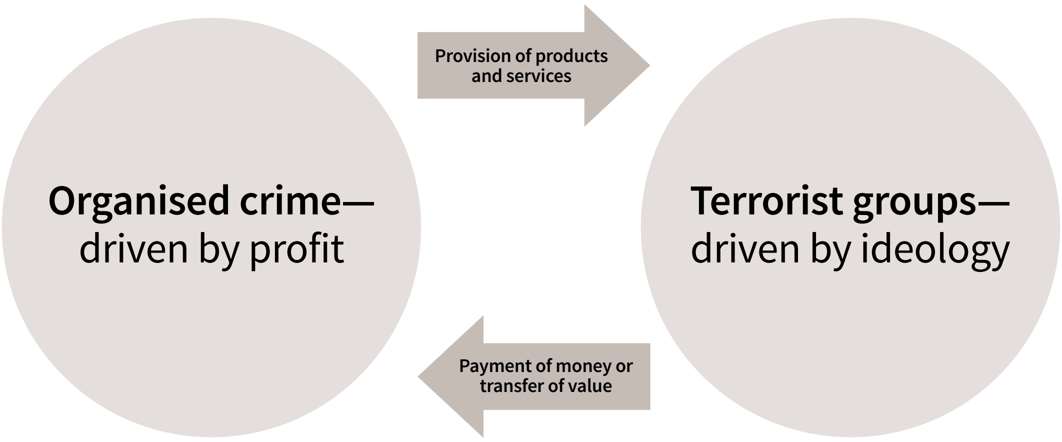
A transactional terror–crime nexus?

As much as the generalised terror–crime nexus convergence model doesn't work in Australia, let alone universally, neither does a simplified transactional crime model (Figure 5) do justice to the policy challenges.

In the Australian national and regional terrorism contexts, criminal facilitators continue to play critical roles in enabling terrorist attacks and fundraising, even with the rise of lone-actor terrorism. There are individuals within, and connected with, criminal organisations who provide links between terrorist groups, with varying degrees of visibility of their motivation, to other criminals who provide illicit services (for example, money laundering) and products (for instance, access to chemicals). In the broader criminal environment, there are also key crime enablers who provide specialist criminal capabilities not otherwise readily available. They include professionals such as accountants and lawyers.

The 2015 murder of NSW Police civilian worker Curtis Chang by terrorist Farhard Khalil Mohammad Jabar illustrates this point. Talal Alameddine was found guilty of selling the pistol that Jabar used to execute Chang. Nonetheless, the community, religious and cultural dimensions of the circumstances before and after the attack are somewhat opaque. This observation isn't a suggestion that terrorist groups *don't* engage with organised crime groups as key facilitators for the provision of goods or services. Instead, it's an argument that a simplified transactional model doesn't adequately describe the complexity of this nexus within Australia or across the region.

Figure 5: The transactional terror–crime nexus

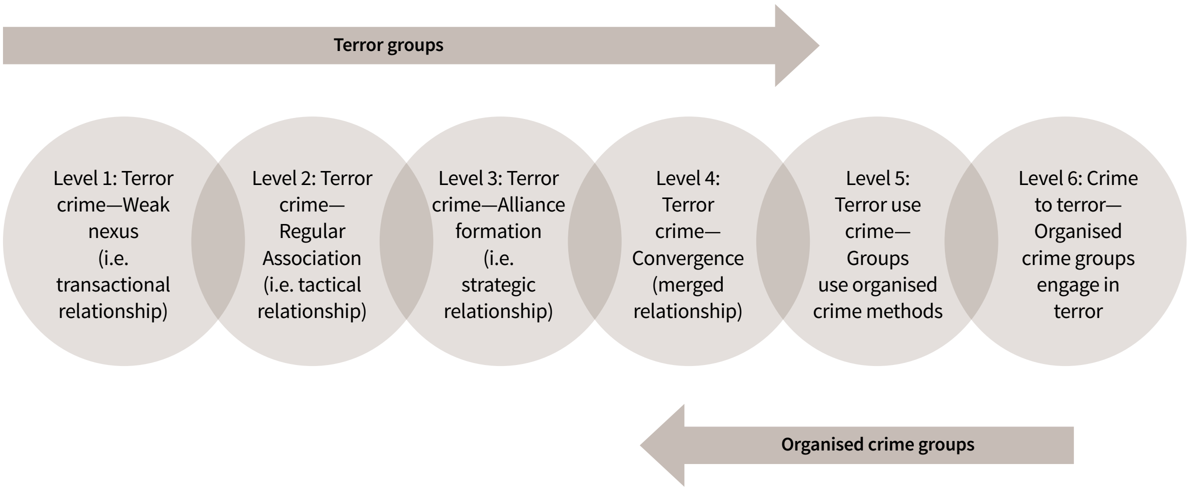

Provision of products and services
Organised crime—driven by profit
Terrorist groups—driven by ideology
Payment of money or transfer of value

A terror–crime nexus paradigm

This chapter uses a terror–crime nexus paradigm based on Schmid's levels of link intensity between organised crime and terrorist groups (Figure 6).[15] The first four levels illustrate a transition of terror groups from transactional interaction with organised crime through to full convergence. This paradigm reverses Schmid's original levels 5 and 6. Level 5 is now concerned with terror groups that use organised crime methods, not strictly as an evolution from convergence as much as a new strategy for a group. Level 6 is now concerned with organised crime groups that have remained criminal but become terrorist outfits, too, and are now engaging in terror.

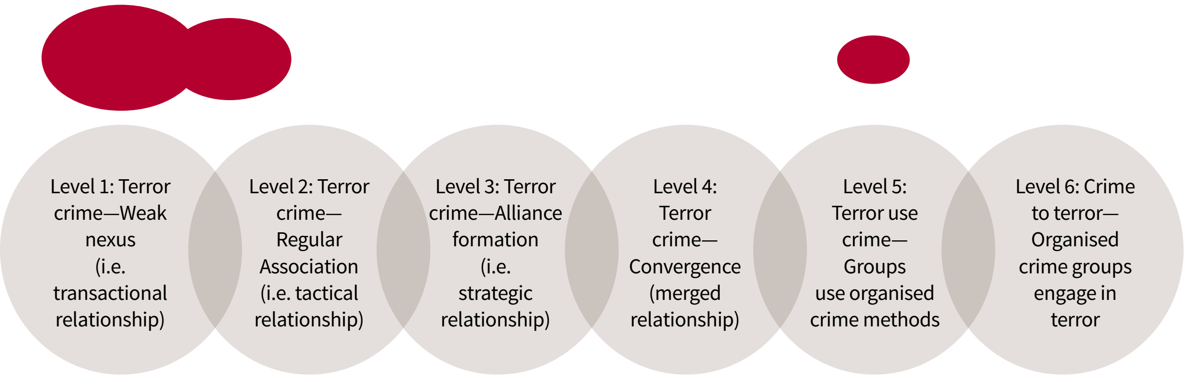
This paradigm, while not without empirical weaknesses, provides the intellectual granularity needed by policymakers. The paradigm can be used to contextualise the state of Australia's and the region's terror–crime nexus. A single overall 'score' or 'assessment level' shouldn't be generated from this model or analysis resulting from it. Instead, groups of activity can be mapped across the paradigm, as has been done for Australia in Figure 7.

Figure 6: The terror–crime nexus link paradigm


Terror groups
Level 1: Terror crime—Weak nexus (i.e. transactional relationship)
Level 2: Terror crime—Regular Association (i.e. tactical relationship)
Level 3: Terror crime—Alliance formation (i.e. strategic relationship)
Level 4: Terror crime—Convergence (merged relationship)
Level 5: Terror use crime—Groups use organised crime methods
Level 6: Crime to terror—Organised crime groups engage in terror
Organised crime groups

Source: A. Schmid, 'Revisiting the relationship between international terrorism and transnational organised crime 22 years later', ICCT v Research Paper, August 2018.

Figure 7: The terror–crime nexus in Australia


Level 1: Terror crime—Weak nexus (i.e. transactional relationship)
Level 2: Terror crime—Regular Association (i.e. tactical relationship)
Level 3: Terror crime—Alliance formation (i.e. strategic relationship)
Level 4: Terror crime—Convergence (merged relationship)
Level 5: Terror use crime—Groups use organised crime methods
Level 6: Crime to terror—Organised crime groups engage in terror

● Denotes an assessment of the scope of the Australian terror–crime nexus mapped against Schmids' paradigm.

Source: A. Schmid, 'Revisiting the relationship between international terrorism and transnational organised crime 22 years later', ICCT v Research Paper, August 2018.

The red ovals map particular groups onto the level that their activities and relationships demonstrate, instead of attempting a holistic 'terror–crime nexus' assessment for Australia.

Arguably, for the most part, the terror–crime nexus in Australia oscillates between levels 1 and 2. There's sufficient evidence, especially from recent publicly available information, of a transactional relationship, such as the purchase of weapons and, at times, tactical cooperation, especially for money laundering and the international movement of terrorist funding.[16] There's also sufficient evidence to suggest a relationship between criminality and extremism in some criminal groups in Sydney and Melbourne.[17] But, as highlighted separately by Jacinta Carroll and Rodger Shanahan, there remains no strong causal link between criminality and terrorism in Australia.[18]

Interestingly, there's evidence from groups such as Brothers 4 Life in NSW that organised crime groups, or at least street gangs, are taking on some of the characteristics of extremist groups. The same thing could be said for some right-wing extremist groups, which use ideology to unify youth at risk of or involved in criminal activities; the 2005 Cronulla riots serve as a good example of this dynamic (the red oval on Level 5 in Figure 8).

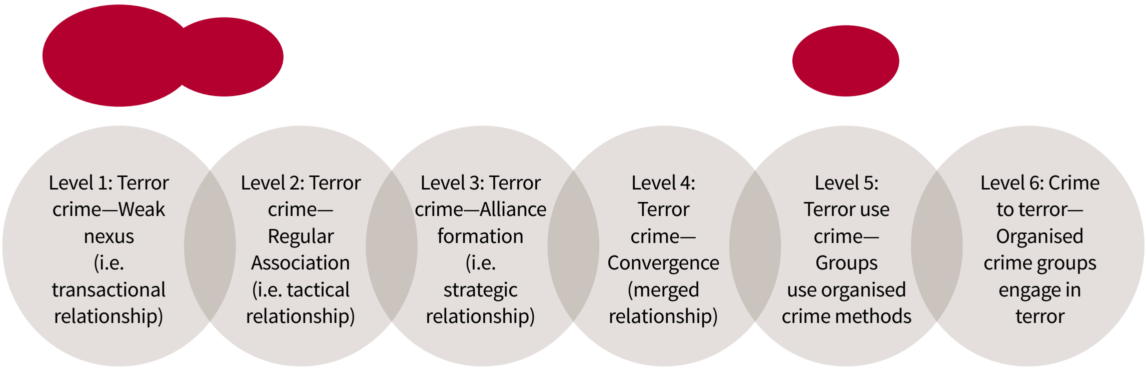
Commentary from ASPI's *Counterterrorism yearbook 2020* suggests that there's a more pronounced terror–crime nexus in the ASEAN region (Figure 5). There's clear evidence that there's an intensified transnational relationship between terrorists and criminals. In Indonesia, the long-term incarceration of terrorist offenders has allowed terrorists and terrorist groups to develop extensive criminal contacts. This higher level connection has led to significant ongoing relationships, providing direct access to key facilitators and illegal professional services that means the scale of the transactional and tactical relationships is greater than in Australia. There's also been a clear long-term trend across the archipelagic region of ASEAN, including the Philippines and Indonesia, of terrorist groups such as the Abu Sayyaf Group and Jemaah Islamiyah using organised crime methods.

Policy responses

In responding to Australia's domestic terror–crime nexus policy challenge, care must be exercised to ensure that policy interventions don't derail other critical long-term policy efforts, especially those focused on social cohesion. Proportional policy efforts need to focus on denying terrorist groups and individuals access to criminal facilitators who can enable fundraising or access to capabilities such as explosives and guns. Nonetheless, those policy measures need to be done so that they aren't easily manipulated by extremist narratives as examples of injustice, which eventually fosters discrimination and social division.

In 2020, with young Australians bearing the social and economic brunt of Covid-19, social cohesion efforts are critical. Policy measures need to consider how to prevent young Australians from entering the justice system, mainly through preferencing alternative intervention options

Figure 8: The terror–crime nexus in the ASEAN region


Level 1: Terror crime—Weak nexus (i.e. transactional relationship)
Level 2: Terror crime—Regular Association (i.e. tactical relationship)
Level 3: Terror crime—Alliance formation (i.e. strategic relationship)
Level 4: Terror crime—Convergence (merged relationship)
Level 5: Terror use crime—Groups use organised crime methods
Level 6: Crime to terror—Organised crime groups engage in terror

● Denotes an assessment of the scope of the Australian terror–crime nexus mapped against Schmids' paradigm.

Source: A. Schmid, 'Revisiting the relationship between international terrorism and transnational organised crime 22 years later', ICCT v Research Paper, August 2018.

over incarceration. The central aim for all Australian governments should be to continue preventing jihadist and far-right extremists from recruiting or radicalising in Australian communities, so it would be a mistake to have social and economic policies that respond to the pandemic adding more young people to the prison population, who are then vulnerable to radicalisation.

A second priority must be to deny terror groups access to professional criminal facilitators. To do that, the Australian Government must implement tranche 2 of its anti-money-laundering / counter-terrorism-financing legislation.[19] The amendments will force lawyers, accountants and real estate agents to report their clients if those clients are involved in suspicious financial transactions.

A third priority needs to be a double down on efforts to prevent right-wing and religious extremists from radicalising prisoners in Australian jails. Of course, substantial policy efforts are already underway in those environments. However, as future Covid-19-related austerity measures arise, there's likely to be a temptation to reduce the budgets for programmatic efforts where success is more difficult to measure quantitatively. That would be a mistake.

Finally, the federal, state and territory governments need to continue their work with communities and their leaders to prevent the religious or right-wing radicalisation of criminal groups, be they outlaw motorcycle gangs or street gangs. Such efforts need to be dually focused. First, community leaders and families need assistance with knowing when and how to challenge those who would seek to link political or religious concepts with criminality. Second, efforts should be focused on giving disgruntled and disengaged young Australians voice to express their concerns. This effort needs to deny charismatic carpetbaggers the opportunity to leverage Covid's profound social impacts.

Australia's terror–crime nexus is significantly different from that found in Central America, Europe or South Asia, but it's no less vexing for policymakers. Although groups such as Brothers 4 Life could change this situation quickly, for the time being Australia's challenge remains one of prevention.

Notes

1 J Borges, J Lawrence (eds), *Testimony to the invisible: essays on Sedenborg*, Chrysalis Books, 1995.

2 RG Smith (ed.), *Organised crime research in Australia 2018*, research report 10, Australian Institute of Criminology, 2018, online.

3 H van der Wilt, C Paulussen, 'The role of international criminal law in responding to the crime–terror nexus', *European Journal of Criminology*, 25 February 2019.

4 J Jupp, M Garrod, 'Legacies of the troubles: the links between organised crime and terrorism in Northern Ireland', *Studies in Conflict & Terrorism*, 4 November 2019.

5 CB Realuyo, 'The terror–crime nexus: Hezbollah's global facilitators', *Prism*, 2014, 5(1):116–131, online.

6 J Coyne, *'Santa Muerte,' are the Mexican cartels really coming?*, ASPI, Canberra, 11 July 2017, online.

7 Klaus von Lampe, 'Definitions of organized crime', *Organised Crime Research*, 4 November 2020, online.

8 J Easson, AP Schmid. 2011. 'Appendix 2.1: 250+ academic, governmental and intergovernmental definitions of terrorism', in AP Schmid (ed.), *The Routledge Handbook of Terrorism Research*, Routledge, Abingdon, 2012, 99–157.

9 A Schmid, Revisiting the relationship between international terrorism and transnational organised crime 22 years later, International Centre for Counter-Terrorism, The Hague, August 2018, online.

10 CP Clarke, 'Crime and terror in Europe: where the nexus is alive and well', *The RAND Blog*, 15 December 2016, online.

11 P Wang, 'The crime–terror nexus: transformation, alliance, convergence', *Asian Social Science*, 2010, 6(6).

12 Realuyo, 'The terror–crime nexus: Hezbollah's global facilitators'.

13 L Ferri, 'Notorious Brothers 4 Life founder Bassam Hamzy and a convicted terrorist appear in court after "getting into a violent brawl at Australia's most dangerous prison"', *Daily Mail*, 13 February 2019, online.

14 Garret Atkinson, *ASG: The father of the swordsman*, American Security Project, March 2012, online.

15 Schmid, 'Revisiting the relationship between international terrorism and transnational organised crime 22 years later'.

16 J Carroll, *Migration, crime and terrorism: correct figures but wrong message*, ASPI, Canberra, 23 November 2016, online.

17 Carroll, *Migration, crime and terrorism: correct figures but wrong message*.

18 R Shanahan, *Typology of terror—the backgrounds of Australian jihadis*, Lowy Institute, Sydney, 21 November 2019, online.

19 'Anti-money laundering', *Policy Agenda*, Law Council of Australia, no date, online.

Fighting organised crime, preventing terrorism: the Italian case

DARIA IMPIOMBATO

Researcher, International Cyber Policy Centre, ASPI

Canberra, Australia

In March 2020, Italy emerged as an epicentre of one of the world's worst coronavirus outbreaks. The severe economic and social costs of the pandemic reverberate to this day as the country struggles to contain the spread of the virus. A major consequence of the pandemic for Italy is the way organised crime groups have benefited from the economic and social downturn affecting the country. While Italy is making efforts to exit a period of protracted economic crisis, those factors are also likely to drive an increase in radicalisation.

Links between Italian organised crime and terrorism have been highlighted in the past.[1] However, the Covid-19 pandemic is likely to bring about new and intertwined challenges for law enforcement. Italy presents an interesting case for several reasons: its geographical position at the heart of the Mediterranean, its prominent role in EU institutions, the power of its mafia cartels, and its sophisticated law enforcement system, which has been developed over a number of years and delivered much success in the fight against terrorism.

This chapter explores the successful mechanisms used by Italian law enforcement, guided by the Dipartimento di Pubblica Sicurezza (Public Security Department) under the Interior Minister and investigative coordination by the judicial authorities, in addressing the terrorist threat at both the national and international levels. This provides insight into what other Western democracies such as Australia can learn from the Italian model. I also explore the ramifications of having the highest per capita police presence in Europe, and the limitations of an aggressive approach that at times justifies an excessive use of power or force and results in discrimination and the erosion of human rights.

Italian exceptionalism in the history of terror

As of January 2021, Italy has been immune from major terrorist attacks linked to international terrorist groups since 11 September 2001. However, during the so-called *Anni di Piombo* (Years of Lead) period between 1969 and 1982, Italy was subject to some of the worst domestic terrorist attacks in Europe. That experience of intense terrorist activity makes for a compelling case study, allowing for the analysis of national and transnational terrorist practices, but also to find improved countermeasures applicable at the international level.[2]

During the Years of Lead, one of the darkest and bloodiest periods in postwar Italy, several domestic terrorist groups across the political spectrum inflicted considerable human, economic and social costs. The better structured organisations were those on the extreme left, such as the communist Red Brigades, and the extreme right, headed by neo-fascist groups. Smaller groups were also active, including anarchist, separatist and transnational groups.

Meanwhile, powerful Italian organised crime groups such as the Sicilian Cosa Nostra and the Calabrian 'Ndrangheta continued their criminal activities and exerted territorial powers over southern regions of the country. The 1990s were the peak of *terrorismo di mafia* (mafia terror), characterised by the use of terrorist tactics by mafia syndicates to pursue their purposes, which culminated with the assassinations of anti-mafia judges Giovanni Falcone and Paolo Borsellino. The intensification of terrorist activity by Cosa Nostra, in particular, was followed by greater law enforcement action that seriously undermined the groups' economic, political and association capabilities.[3]

During that time, Italy adopted new legislation that granted mafia witnesses (also known as *pentiti*—repentants) sanctioning and penitentiary benefits as well as state protection, representing a turning point for anti-mafia prosecutions. Those and other legislative and institutional changes, such as the creation of the Direzione Investigativa Antimafia,[4] set the basis for the anti-mafia law enforcement successes of the 1990s and early 2000s, when there were numerous high-profile arrests and convictions of mafia bosses, and significant confiscations of capital and possessions.[5]

The terror–crime nexus in present-day Italy

Although there's no tangible evidence of direct links between transnational terrorist groups and Italian mafias, several confidential investigations into this matter are under way. According to Italian prosecutors, many mafia cartels see associating themselves with Islamist radicals as a risky business because the Islamists attract the authorities' attention. That assessment, however, excludes neither tangential business relations nor future prospects of collaboration with other terrorist groups or individuals.[6]

The terror–crime nexus nowadays is different from previous decades. Cosa Nostra and the 'Ndrangheta are far less likely to engage in terrorist activity, as they restructured and took a more underground approach following the crackdown by the authorities in the 1990s. Currently, most collaborations take the form of business transactions.

Most recently, in July 2020, 84 million Captagon pills, known as the 'Jihad drug' because the Islamic State has reportedly become one of its main producers in Syria,[7] were seized by the Guardia di Finanza (financial crime police)[8] in Salerno. Authorities linked them to the Lebanese terrorist group Hezbollah and the Neapolitan mafia group Camorra.[9] There are many further examples of illicit deals between the Camorra and the 'Ndrangheta and groups such as Hezbollah, the Irish Republican Army, the Basque group ETA, and the Revolutionary Armed Forces of Colombia.[10] However, experts have assessed that the risk of terrorists within Italian borders being sponsored by or receiving arms from organised crime cartels remains low. The territorial nature of the cartels' operations makes it difficult for outsiders to access the illicit arms market.

Currently, the terror–crime nexus is more visible in the authorities' response and organisational structure. For example, in 2015 law enforcement institutions assigned counterterrorism duties to the judicial body formerly dedicated to countering organised crime, which was renamed 'Direzione Nazionale Antimafia e Antiterrorismo' (National Anti-mafia and Antiterrorism Bureau).

The Public Security Department is led by the head of the police and includes all law enforcement agencies. A fundamental organ in this space is the Direzione Centrale Polizia di Prevenzione (Prevention Police Central Directorate), which manages all the different aspects of counterterrorism, including prevention and investigation. Among the different divisions is the Nucleo Operativo Centrale di Sicurezza (Security Central Operative Unit), which is dedicated to operative interventions for serious crimes, including terrorism and organised crime, and is a flagship of Italian law enforcement.

The Carabinieri, a militarised police force, also has a special operations group, known as the Raggruppamento Operativo Speciale, that deals with investigations related to organised crime and terrorism. The group was originally formed to fight domestic terrorism during the Years of Lead. Following its success in defeating the Red Brigades, it was given more responsibilities in dealing with Cosa Nostra during the 1990s, especially high-risk operations involving the infiltration of gangs.

The increasing power and sophistication of Italian mafias' criminal activities, which have infiltrated virtually every sector of Italian society and expanded across the globe, have required the authorities to implement constant changes. Consequently, the state has granted authorities extraordinary powers, resources and funding. This is considered the main driver for the creation of what is, according to many, 'the most advanced anti-mafia laws in the world'.[11] As the new wave of international terrorism started to claim victims, Italy had already developed an efficient law enforcement structure.

It's important to note that the jihadist terrorist threat is comparatively low in Italy. That's mainly due to social factors, such as a lower level of earlier immigration from Muslim countries, and different obstacles posed by social integration compared to neighbouring France. In a written response to a request for comment from ASPI, the Carabinieri have highlighted that the phenomenon of religious radicalisation is weaker, demonstrated by the lower numbers of Italian foreign fighters (currently 146) compared to those from other European countries that have experienced terrorist activity—especially France and Belgium. Despite the low-level threat posed by jihadist terrorism, experts have argued that this exceptionalism will soon be over for Italy if it doesn't solve deeply rooted issues of integration, racism and irregular migration management.[12]

Pros and cons of the Italian approach

For the purposes of this chapter, I submitted a series of questions to the Italian Polizia di Stato (state police) and Arma dei Carabinieri (gendarmerie).[13] Their responses reflect the argument that, due to past experiences and difficulties in dealing with domestic terrorism and organised crime, Italian authorities are now better prepared than most when dealing with international terrorism, especially through the activities conducted by the Direzione Centrale Polizia di Prevenzione.

The Italian counterterrorism system is based on two pillars: legislative updates, which provide police forces and the judiciary with effective instruments to ensure a sharp response in the face of evolving terrorist threats; and an integrated approach, which ensures the rapid circulation of relevant information and prioritises collaboration between investigative and intelligence apparatuses through activities led by the Comitato di Analisi Strategica Antiterrorismo (CASA, Committee for Counterterrorism Strategic Analysis).

The CASA is made up of representatives from all law enforcement and intelligence services and acts as an instrument for the Interior Minister to manage information channels, evaluate terrorist threats and respond to social-order and public-security emergencies. It's a key feature of Italy's antiterrorism strategy, as a common platform where security forces share information about terrorist groups, intelligence, individuals and threats, and brings together the expertise of the Polizia di Stato, the Carabinieri, the Guardia di Finanza, the Penitentiary Police and other intelligence organs, such as the Agency for Internal Information and Security and the Agency for External Information and Security. The efficacy of CASA is a direct consequence of its non-bureaucratic structure and its capacity to work extremely fast in accordance with the estimated risk level.

Like many other legislative systems, the Italian legislature has been mainly reactive in terms of counterterrorism laws. The first definition of terrorism was introduced in the Italian Criminal Code in 1978, after the abduction and murder of statesman Aldo Moro by the Red Brigades.[14] However, state police believe that it's the preventive measures present across the entire territory, not the reactive ones, that differentiate the Italian system from others.

Due to its particular history, Italy now has the legislative instruments it needs to rapidly adapt to different types of threats. In fact, 'not only can Italian security forces conduct lengthy surveillance operations, preemptive raids, and expulsions of foreign suspects, but since 2005, administrative deportations have also become a cornerstone of Italy's counterterrorism strategy.'[15] A legal decree adopted in 2018 has established a new position on the possibility of revoking Italian citizenship. This applies in cases in which naturalised foreign citizens present a threat to national security by committing serious crimes. The provision applies in the case of a definitive sentencing for crimes committed with terrorist aims or the intention of subverting the constitutional order. Initiated by the Interior Minister, the withdrawal of Italian citizenship occurs within three years of sentencing by decree from the President of the Republic.

Despite the enthusiasm of law enforcement agencies for those practices, the negative implications can't be ignored. Human rights and civil society groups have highlighted how such overarching powers of the Interior Minister might present issues of abuse of power as well as discrimination.[16] In 2009, the European Human Rights Court found that Italy's expulsion of a Tunisian citizen, for instance, violated international human rights law.[17] The opacity of these sweeping measures and the veil of secrecy that surrounds most terrorist-related cases make it hard to assess the fairness of such prescriptions.

That attitude has also contributed to a climate of fear and racism against immigrants, especially those crossing the Mediterranean from Africa. In 2018, that culminated in the passing of two of the most controversial laws in Italian history. Referred to as *porti chiusi* (closed ports), the laws prevented disembarkation from boats that sought to bring rescued people to Italian shores. Such laws have been widely criticised for violating human rights and are still facing international scrutiny.[18] There's no objective data on the systematic use of illegal immigration by Italian terrorist groups, so a direct connection between immigration and terrorism is not only factually inaccurate, but also dangerous and potentially conducive to the radicalisation of those who become marginalised within Italian society.

Covid-19, implications for Australia and recommendations

Since the start of the Covid-19 pandemic, Italian mafias have taken advantage of the state's struggle to support local communities. It has been widely reported that criminal groups have been distributing food and other goods to families in need, filling the void that institutions left behind and strengthening their grip over the population.[19] Nicola Gratteri, Italy's most prominent 'Ndrangheta expert and prosecutor, said that 'the bosses know very well that in order to govern, they need to take care of the people in their territory. And they do it by exploiting the situation to their advantage.'[20] Additionally, profits from the 'Ndrangheta's infiltration into Italy's healthcare system have boomed.[21]

The strengthening of Italian organised crime groups is dangerous for Australia, since they have extensive ties to the country, particularly the 'Ndrangheta.[22] Similarly, the potential for increased collusion with terrorist groups should alarm Australian law enforcement agencies. In the light of the peculiarities of the phenomena summarised in this chapter, Australian authorities should:

- further study the potential for intersectionality between counterterrorism and anti-mafia legislation and measures in Australia, which can be done by following key elements of the Italian example, as well as investigating trends and practices of terrorist and organised crime groups and the potential intersections in their operations
- improve collaboration with countries such as Italy in order to share anti-mafia and counterterrorism techniques and information
- push for the improvement of international counterterrorism, anti-mafia and broader anti-organised crime standards.

Meanwhile, to address the issues highlighted in this chapter, Italy should:

- promote a cross-border approach and better collaboration between police forces across the EU to advance more unified and coordinated action on both the organised crime and the terrorism fronts
- ensure that human rights are respected during counterterrorism operations, and continue to investigate and prosecute discrimination and human rights violations carried out by law enforcement agencies in their counterterrorism activities
- sharpen and rebalance procedures of expulsion and citizenship revocation in order to ensure that they're transparent and fairly applied.

In summary, organised criminal groups remain powerful and the terrorist threat is ever present in Italy, despite the advancement of law enforcement measures. This is particularly due to the deepening crisis the country has experienced since the beginning of the Covid-19 pandemic. This is also likely to result in an uptick in radicalisation in Italy and around the world, heightening the risk of intersecting activities between criminal gangs and terrorists, and therefore presenting major security concerns.

Notes

1 *Europe's crime-terror nexus: links between terrorists and organized crime groups in the European Union*, European Parliament, October 2012, online.

2 Committee on the Judiciary, *Terrorism and security: the Italian experience*, US Senate, November 1984, online.

3 Letizia Paoli, 'Mafia and organised crime in Italy: the unacknowledged successes of law enforcement', *West European Politics*, September 2007, online.

4 A direct translation of this is 'Anti-Mafia Investigative Directorate'.

5 Paoli, 'Mafia and organised crime in Italy: the unacknowledged successes of law enforcement'.

6 Francesco Strazzari, Francesca Zampagni, *Between organised crime and terrorism: illicit firearms actors and market dynamics in Italy*, Flemish Peace Institute, 2018, online.

7 Michael Walsh, 'What is the drug Captagon and how is it linked to the Islamic State group and a drug bust in Italy?', *ABC News*, 2 July 2020, online.

8 The Guardia di Finanza is a militarised police body responsible for investigating financial crimes, drugs and smuggling. It operates under the Ministry of Economy and Finance and is part of the Public Security Department, which coordinates the four police branches. The four branches are independently administered, but coexist under the operative coordination of the department and the General Director.

9 Francesco Bongarrà, 'Italian police: record-breaking drugs bust could have Hezbollah link', *Arab News*, 26 December 2020, online.

10 Gabriele Carrer, 'Droga, armi e 'ndrangheta. Ecco l'Hezbollah-connection in Italia', *Formiche.net*, 27 September 2020, online; Strazzari & Zampagni, *Between organised crime and terrorism: Illicit firearms actors and market dynamics in Italy*.

11 Strazzari & Zampagni, *Between organised crime and terrorism: Illicit firearms actors and market dynamics in Italy*.

12 Michele Groppi, *The terror threat to Italy: how Italian exceptionalism is rapidly diminishing*, Combating Terrorism Center at West Point, May 2017, online.

13 In Italy, the state police is the main civil police body, responsible for routine policing duties. The Carabinieri, on the other hand, is the country's national gendarmerie, a militarised police force whose main practices fall under the Defence Ministry's authority. In practice, several overlaps exist between the two law enforcement bodies.

14 Committee on the Judiciary, Terrorism and security: the Italian experience.

15 Andrea Beccaro, Stefano Bonino, 'Terrorism and counterterrorism: Italian exceptionalism and its limits', *Studies in Conflict & Terrorism*, 9 December 2019, online.

16 Robin Simcox, 'Is Italy immune from terrorism?', *Foreign Policy*, 18 July 2018, online.

17 *Italia: L'espulsione di un tunisino viola la Convenzione Europea dei Diritti dell'Uomo*, Human Rights Watch, 5 August 2009, online.

18 *Italy: Revoke abusive anti-asylum decrees*, Human Rights Watch, 31 January 2020, online.

19 Salvo Palazzolo, 'Palermo, il fratello del boss della droga fa la spesa per lo Zen', *La Repubblica,* 8 April 2020, online.

20 Lorenzo Tondo, 'Mafia distributes food to Italy's struggling residents', *The Guardian*, 10 April 2020, online.

21 Miles Johnson, 'How the nafia infiltrated Italy's hospitals and laundered the profits globally', *Financial Times*, 9 July 2020, online.

22 Anna Sergi, 'The 'Ndrangheta down under: constructing the Italian mafia in Australia', *European Review of Organised Crime*, 2019, online.

Revisiting the terror–crime nexus in Latin America: militant proto-state governance and challenges to state security

DR ALEXANDRA PHELAN
Deputy Director, Gender Peace and Security Centre, Monash University
Melbourne, Australia

The conventional view of the terror–crime nexus emphasises the interplay between organised crime and terrorism, closely examining the links between illicit economic activities and militant non-state actors. Specifically, the term has most commonly been applied to the use of crime by terrorist organisations as a source of funding and also relates to the formation of alliances between criminal and terrorist organisations.[1] Traditionally, the terror–crime nexus has best been understood as a continuum, converging when criminal groups begin displaying political motivations and terrorist groups use their political ideology as either a facade or a justification for their criminal objectives.[2] Where there's evidence of collusion between organised crime groups and terrorist organisations, they tend to be within weak states where black markets and illicit economies are largely or completely controlled by existing cartels or organised crime groups or newer transnational organised crime groups and terrorists.[3]

Yet, in the context of Latin America, the terror–crime nexus can't be understood purely in terms of alliances, tactics, gains from illicit economies and the real or fabricated political justifications of those factors. Economic regulation and protection are fundamentally political activities carried out by states, regardless of whether or not they successfully generate political support or opposition.[4] In many respects, the terror–crime nexus has become closely linked with proto-state governance, as guerrillas, cartels and organised crime groups alike also integrate illegal economies into their areas of control and influence and often redirect proceeds from them back into communities where they operate. This is designed not only to maintain authority over both territory and lucrative turf, but also to persuade and enhance perceptions of their organisational legitimacy over that of their opponents.

In 2020, the Covid-19 pandemic illustrated the degree to which non-state armed groups throughout Latin America (such as in Mexico, El Salvador, Brazil and Colombia) wield control or influence over territories and further demonstrated the complexities of the terror–crime nexus when integrated and consolidated into militant governance. The effects of Covid presented both opportunities and challenges for guerrillas and organised crime groups, some of which leveraged the crisis to strategically reposition, expand their presence and enforce arbitrary rule to the detriment of populations living within their spheres of influence, as I will demonstrate in the cases of Colombia and Brazil. This has significant security implications for the state and its efforts to counter the expansion of both insurgents and organised crime groups, particularly in areas where the government has been unable—or unwilling—to fully re-exert authority and the rule-of-law vis-a-vis such militant groups.

Colombia

Although the 2016 Colombian peace agreement resulted in the formal demobilisation of the Revolutionary Armed Forces of Colombia (FARC) and facilitated its transition into a formal political party, the Colombian conflict continues to be marked by a general realignment of militant non-state actors. This includes the ongoing presence of the National Liberation Army (ELN), FARC dissident factions and criminal gangs otherwise known as *bandas criminales*—or BACRIM—that continue to vie over power vacuums left after FARC's demobilisation.

Since FARC disarmed in 2017, the ELN has increasingly consolidated as a 'bi-national insurgency'[5]—a term recently used to describe the guerrilla organisation's traditional foothold in Colombia and rapid expansion into Venezuela. The ELN formed as a guerrilla organisation in 1964 in Colombia and began to consolidate its presence in Venezuela from the early 2000s. However, it has recently tightened its authority and influence in Venezuela, particularly in the states of Apure, Táchira, Zulia, Bolívar and Amazonas.[6] Concerningly, this has included taking control of illegal mines and has allowed the guerrillas to use the acquisition of gold, coltan and diamond deposits not only to fund their organisations, but also to pressure the Venezuelan regime.[7] In Táchira, Amazonas and Apure, the ELN has strengthened its governance, imposing curfews, administering both justice and punishment in its areas of proto-state authority and conducting recruitment campaigns of minors in schools, among other illegal activities.[8] Furthermore, there's general consensus that the ELN has recently been distributing state-subsidised food boxes from the Venezuelan local storage and production committees (*comités locales de abastecimiento y producción*).

On 29 August 2019, former FARC secretariat member Iván Márquez announced a return to arms alongside former top leaders Jesús Santrich and Henry Castellanos Garzón, also known as 'El Paisa' and 'Romaña', calling for a 'new phase of armed struggle' in response to the Colombian state's 'betrayal of the Havana peace agreement'.[9] Over the past 12 months, it's believed that FARC dissidents were able to double their membership from approximately 2,600 to almost 4,600, with a presence in 138 municipalities throughout Colombia.[10] In addition to the group's involvement in drug trafficking, smuggling and extortion, similarly to the ELN, FARC dissidents have been heavily involved in the illegal mining of gold and other minerals, which has become a critical source of revenue for the organisation. It's believed that both FARC dissidents and the ELN make more than half of their income from mining in Colombia and Venezuela.[11]

The Covid-19 pandemic has further demonstrated how both guerrillas and organised crime groups have exerted proto-state authority by enforcing lockdown measures throughout Colombia after a national quarantine was decreed on 24 March 2020. Colombia's Ombudsman's Office warned that BACRIM, ELN and FARC dissidents were taking advantage of the pandemic's lockdown period to strengthen their military advantage and impose control orders on populations throughout the country. This included regulating commercial and leisure establishments, blocking land and waterways and controlling medical and food supplies to the point of restricting their arrival. At least 10 documented homicides were allegedly committed because the victims had violated the measures imposed by militant groups.[12]
The groups demonstrate clear examples of the terror–crime nexus, yet they also serve as examples of how such illicit activities have boosted the groups' resources to the degree that they're able to exert authority in Colombia and transnationally into Venezuela.

Brazil

Brazil's two largest gangs—the First Capital Command (*Primeiro Comando da Capital*, PCC), traditionally based in São Paulo, and the Red Command (*Comando Vermelho*, CV), traditionally based in Rio de Janeiro—also serve as examples of the terror–crime nexus's complexity, and both have continued to pose challenges to the Brazilian state's ability to exert control over various *favelas* (slums) throughout the country. In some *favela* neighbourhoods, it's common that such gangs and drug-trafficking organisations exert more authority and influence than the police. The PCC and CV worked closely with each other until their longstanding alliance broke down in 2016, contributing to the PCC forming alliances with criminal organisations such as Amigos dos Amigos in order to attempt to exert control over turf in Rio de Janeiro.[13] Both groups use violence and synchronised attacks, shut down businesses, destroy public transport and attack both public buildings and police stations, often deliberately targeting police in retaliation for gang arrests or crackdowns. The PCC has used violence, protest and disruption both strategically and politically, employing them as punishment for statements and acts of political officials and as bargaining chips in relation to Brazil's organised crime policies, including incarceration policies.[14]

Both the PCC and the CV, along with other gangs exerting control throughout Brazil, imposed social control in response to Covid-19 by way of curfews, restrictions on movement and the implementation of specific measures to limit the spread of the virus. Although President Bolsonaro dismissed Covid as 'sniffles', comparing the virus to the flu, in April Brazil's former Health Minister, Luiz Hendrique Mandetta, suggested that the government may have to coordinate with drug traffickers in the *favelas* over the enforcement of curfew and other management plans to stop the spread of Covid.[15] Many *favela* communities have been abandoned by the state in the fight against Covid and as a result have organised their own responses to stop the spread. For example, in Paraisopolis in São Paulo—a *favela* in which the PCC is alleged to act as the *de facto* authority—a resident association hired its own medical team for the community out of distrust of the government response.[16] In Rio de Janeiro, the CV imposed curfews and restricted movement after 8 pm in Cidade de Deus. Gangs in other *favelas*, such as Rocinha, Rio das Pedras and Muzema, issued control orders that were circulated via messaging apps, stating that *baile funk* parties were cancelled, that bars were ordered to close (take-away permitted) and that residents must stay home.[17] In addition to enforcing rules, gangs also handed out welfare and hand soap and displayed signs asking those who entered to wash their hands[18]—active attempts to fill the void of ongoing government neglect of those communities.

Recommendations

The convergence of the terror–crime nexus with proto-state governance poses significant challenges to the state, particularly when such organisations can't be considered as solely 'terrorist' or 'criminal' and policy approaches can't be purely defined in line with either taxonomy. The two cases of Colombia and Brazil demonstrate that both guerrillas using crime and drug trafficking gangs using violence politically can further defy a state's authority when their activities result in their control of territory and social order. This is particularly challenging when illicit economic activities are firmly integrated into their areas of control. Furthermore, crises such as the current pandemic can be used by such groups to enhance their own power, legitimacy and local support where states fail to respond effectively.

In order to frustrate the control of such organisations, ‘good governance’ through an increase in state presence and the effectiveness of state institutions become key in countering the terror–crime nexus, particularly in Latin America. In both Colombia and Brazil, armed non-state actors have succeeded in wielding control where state presence has been minimal, security hasn’t been consolidated and ineffective application of the rule of law has failed to maintain order. However, previous attempts at military campaigns (in Colombia) and pacification programs (in Brazil) have demonstrated that government policies aimed at territorial reclamation *must* be overlaid onto legitimacy building. In both contexts, impoverished and isolated communities continue to bear the brunt of both government and non-state actor violence and experience the arbitrary enforcement of ‘order’ as a daily reality. Those communities have developed varying degrees of mistrust of the state born out of decades of insufficient social welfare and resources and, in some areas, outright neglect. Therefore, policies that emphasise meaningful investments in both social and economic opportunity, combined with adequate consolidation of security and stability, serve best to confront such militant actors.

Notes

1 Tamara Makarenko, ‘The crime-terror continuum: tracing the interplay between transnational organised crime and terrorism’, *Global Crime*, 2004, 6(1), 130.

2 Makarenko, ‘The crime-terror continuum: tracing the interplay between transnational organised crime and terrorism’, 135.

3 Steven Hutchinson, Pat O’Malley. ‘A crime–terror nexus? Thinking on some of the links between terrorism and criminality’, *Studies in Conflict & Terrorism*, 2007, 30(12):1105–1107.

4 See D Gutiérrez, José Antonio, Frances Thomson, ‘Rebels-turned-narcos? The FARC-EP’s political involvement in Colombia’s cocaine economy’, *Studies in Conflict & Terrorism*, 2020, 44(1):26–51, 7.

5 See Karen Arteaga Garzón, Gwen Burnyeat, Andrei Gómez-Suárez, Germán Otálora Gallego, ‘Trump, Venezuela and the ELN: the geopolitics of peace in Colombia’, *America’s Quarterly*, 1 July 2020, online.

6 FundaRedes, *FundaRedes 2019 Informa Anual*, 2020, 35, online.

7 See ‘ELN in Venezuela’, *InSight Crime*, 28 January 2020, online.

8 FundaRedes, *FundaRedes 2019 Informa Anual*.

9 See Noticias Caracol, ‘Iván Márquez, Jesús Santrich, el Paisa y Romaña retoman las armas’, *YouTube*, 29 August 2019), online.

10 Alexandra Phelan, John P Sullivan, Robert Bunker, ‘Third generation gangs strategic note no. 26: COVID-19, revolutionaries and BACRIM in Colombia’, *Small Wars Journal*, 2 June 2020, online.

11 International Crisis Group, *A glut of arms: curbing the threat to Venezuela from violent groups*, Latin America report no. 78, 20 February 2020, 9.

12 ‘Grupos armados se expanden durante la emergencia por coronavirus en Colombia’, *El Universo*, 18 May 2020, online.

13 See ‘Red Command’, *InSight Crime*, 18 May 2018, online, for an overview of the CV and ‘First Capital Command’, *InSight Crime*, 9 July 2018, online, for an overview of the PCC.

14 See Ryan C Berg, *Breaking out: Brazil’s First Capital Command and the emerging prison-based threat*, American Enterprise Institute, March 2020, 8, 10.

15 ‘Coronavírus: Mandetta dialoga com facções e irrita bolsonaristas’, *Metrópoles*, 14 April 2020, online.

16 ‘Mistrustful of the state, Brazil slum hires own doctors to fight virus’, *Reuters*, 3 April 2020, online.

17 ‘Coronavírus: tráfico e milícia ordenen toque de recolher em favelas do Rio’, *Agência O Globo*, 24 March 2020, online.

18 ‘Brazil gangs impose strict curfews to slow coronavirus spread’, *The Guardian*, 26 March 2020.

An evolution of terrorism: the intersection of cybercrime and terrorist activity

DR ANNE ALY MP

Federal member for Cowan, Western Australia, House of Representatives, Parliament of Australia

Perth, Australia

It's now almost two decades since the September 11 attacks heralded a seismic shift in international and national security. Much has been said about how those attacks changed the world—how they brought about a new era, in which both terrorism and acts of terror by non-state actors have become par for the course in security assessments.

As we move into a remodelled era in which states—North Korea, China and Russia—are growing their role as key players in international security, we could be easily misled into suggesting that we're returning to an international security landscape reminiscent of the Cold War. Indeed, in 2006, the dominant mission of the US Department of Defense in international security was its 'long war' against international terrorism. Now, it seems, the long war is coming to an end, and a new war has begun. The 2018 US National Defense Strategy affirms that:

> The central challenge to U.S. prosperity and security is the *reemergence of long-term, strategic competition* by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.[1]

It would be imprudent to jump too quickly to a conclusion that terrorism no longer presents a confronting threat to national and international security. Equally imprudent would be the assumption that a Cold-War-like duality is now the definitive issue for international security. Even as we watch the retreat of the Islamic State of Iraq and Syria (ISIS), the reclaiming of 65,000 square kilometres of land and the much-heralded defeat of ISIS forces in Syria and Iraq, at least seven counterinsurgency conflicts still rage across the Middle East and North Africa. In October 2020, amid a global pandemic, deadly attacks in France and Austria reminded the world that ISIS-inspired lone actors were not only operational, but capable of carrying out terrorism. In November, ISIS claimed responsibility for an attack on Kabul University that killed at least 32 people.

Almost two decades of combating violent jihadism reveals a pattern in which the decentralisation of the threat from one theatre of violence sees the spreading and revival of the threat in another theatre. Dedicated foreign fighters are likely to be nomadic, migrating from one conflict zone to the next. The most important lesson from this is that military strikes can destroy terrorist training camps and their capabilities but they will not kill terrorism; that is, the underlying ideas, ideology and narrative and their regenerative capacity to attract adherents who are willing to fight, kill and die. Behind all forms of terrorism, be it violent jihadism or far-right violent extremism, is an ideology that frames the world in an 'us versus them' binary and, in the minds of its adherents, justifies a violent response to perceived oppression and injustice. Moreover, that ideology has a lingering appeal that may recede or surge in response to global or regional incidents and conflicts.

Terrorism typologies

The risk of terrorism, like the risk of most criminal activities, can be evaluated as a combination of opportunity, capability and intent. Legislative measures that allow for the arrest, detention and incarceration of people who are found to be planning an attack and laws that make it illegal to travel to certain conflict zones to join terrorist groups address opportunity. Targeting terrorism financing, recruitment and training addresses capability. But in a contemporary, low-tech terrorist environment—where a terrorist attack can be carried out by a single person with a simple weapon such as a knife, gun or vehicle with little or no planning, no financial investment and no special training—opportunity and capability are much more difficult to detect and prevent.

Indeed, the greatest dilemma for modern counterterrorism is intent. In a world where intent evolves in the dark spaces of the internet, where individuals draw inspiration from YouTube videos, social media posts and anonymous chatrooms, we desperately need a comprehensive approach to counterterrorism that incorporates prevention and early intervention strategies.

Disposition to violence

In the 1990s, Helmut Willems studied the development of xenophobic violence and the social and biographical traits of perpetrators, including their criminal histories and disposition to violence.[2] He found that up to 10% of perpetrators had prior records for politically motivated crimes and that up to 35% had prior records for other crimes. Willems distinguished four perpetrator types, which differed in political–ideological orientation and propensity to violence: right-wing activists, ethnocentric youth, criminal youth and fellow travellers. Three of those types had some history of criminal activity: right-wing activists typically had prior records for multiple political crimes; ethnocentric youth for juvenile crime; and criminal youth for multiple criminal activities. Willems's model posits that the right-wing activists are ideologically driven, while xenophobic youth tend to be driven by perceived grievances.

Of particular interest is the finding that criminal youth with a history of violence didn't appear to have marked right-wing ideological leanings or political interests:

> In terms of the propensity to violence, this is a markedly action-oriented, aggressive, and violently disposed type. Here violence is seen not as a means of political conflict, but as a normal element of daily life and conflict resolution which needs no specific legitimation.

Criminal youth tend to come from unstable family backgrounds and have lower education attainment levels. Their violence isn't an expression of ideological or political identity, but a factor of their personal experiences and their own aggressive impulses. In comparison, right-wing activists tend to come from relatively stable backgrounds and have higher education levels; their propensity for violence is politically motivated and legitimised by their strongly held ideologies.

This suggests that there's an important distinction to be made between perpetrators for whom violence is legitimised as a means to an end for an ideological cause and perpetrators for whom violence is detached from any ideological identity. The latter are also high-trait aggressive personalities with a history of violent or aggressive behaviour. Though they may hold certain attitudes or feelings that align with a particular ideology, they're not cognitively radicalised to the extent that they identify completely with that ideology.

The contemporary threat in the domestic arena is characterised by low-tech attacks carried out by single individuals using guns, knives and vehicle ramming (or a combination of those). These kinds of attacks are relatively easy and cheap to carry out and require no planning, and hence can circumvent many security measures. They're also by no means new or innovative—for example, vehicle ramming has been used as a tactic of terror for at least two decades. The Counter Extremism Project has documented at least 53 vehicular terrorist attacks over that period, collectively resulting in the deaths of at least 202 people and the injury of at least 1,123 others.[3]

These attacks are the most challenging for law enforcement agencies. In these cases, proactive identification using traditional forms of intelligence gathering, such as human sources or surveillance, is particularly difficult, and, as a result, law enforcement is placed at a disadvantage.

Behavioural indicators

As the world moves to social media for everything from news to entertainment to quotidian social interaction, so too has terrorism. For example, the attacker who ploughed a van into pedestrians in Toronto in 2018, who was part of an alarming 'incel' subculture, used Facebook to declare his attack.

Public declarations on social media of intent to carry out an attack are more common than we realise and are often a reliable indicator of an impending attack. This means that it's possible to track and trace online behaviours on social media to proactively identify potential violent attackers.[4]

That behaviour starts with a search:

- The *seeker* is primarily motivated to acquire any information about an extremist ideology or idea and is likely to be cognitively open to receiving new information.
- The *lurker* has already narrowed their information sources and has started to rigidify their mindset around extremism, while their social media associations start to gravitate towards ideological themes.
- The *inquirer* uses political aggression in their posts as they begin making connections between a perceived obstruction to their own life goals and the actions of their out-group. Their likes and associations may be skewing towards certain extremist or extremist-sympathising pages.
- The *advocate* adopts a confrontational and declarative posting style. Their profile and cover photos contain symbols associated with an extremist ideology, images associated with conflict, or both. Their likes and associations overtly support an ideology.
- Finally, the *activator* is either activating, or about to activate, their extremist ideologies offline in the commission of a violent extremist act.

Within this framework of online behavioural profiles, there are certain markers—thematic, emotional and behavioural—that can be used to build a more comprehensive profile of a potential suspect. They are detectable on the average user's social media profile. Thematic markers include allegiance to radical groups or figures, in-group ideology and pride, out-group derogation, and identification as a 'soldier' or 'warrior', as expressed through symbols, likes, associations, images and subscriptions. Key emotional markers are anger and contempt for and disgust at the out-group. Behavioural markers include fixation (an increasingly pathological preoccupation with a person or cause); identification (a desire to be or identify as an agent for a cause); and leakage (the communication of the intent to carry out violence).

Policymakers and counterterrorism practitioners can use online behaviour profiles, such as those detailed in this paper, to identify and disrupt possible terrorist operatives who also have a social media presence. In the development of the behaviour profile detailed here, my research team was able to identify a number of persons of concern. The Counter Narratives to Interrupt Online Radicalisation (CNIOR) program, headed by me, developed the Interrupting Online Radicalisation Toolkit, which provides guidelines and instructions for law enforcement and counterterrorism practitioners on how to use behavioural indicators to identify and disrupt potential terrorists.

Technology and terrorism

One of the most compelling reasons to assess threat and capability continuously is that terrorists and criminals always find new ways to do harm. Just as terrorism has pervaded our lives in ways that turn everyday items into weapons and everyday activities into platforms for recruitment and influence, we must also meet the new challenges of security by turning our expertise to the internet and information and communications technology. In response to law enforcement's increasing awareness of terrorists' use of social media, and measures to mitigate any continued threat, terrorists and criminal groups have migrated to the Dark Web and encryption services, wherein they can operate in obscurity.

Terrorists have been using the 'darknet' in the same way as they have been using the surface web—to recruit, radicalise and influence, as well as to finance and coordinate attacks. Since 2015, there has been a significant increase in the use of Telegram (an encrypted instant messaging platform) by terrorist actors. Telegram has now become the preferred online platform for ISIS supporters to distribute propaganda, coordinate and communicate, replacing social media applications such as Twitter and Facebook. Telegram was used to coordinate attacks inspired or directed by the Islamic State in Paris (2015), Brussels (2016), Berlin (2016) and Istanbul (2017).[5]

In 2017, a crackdown on popular darknet markets AlphaBay and Hansa was a response to serious concerns about the use of those platforms to facilitate communication between terrorist actors. That followed the take-down of the Silk Road in 2013 and another operation in 2014 that seized around half a dozen darknet sites. Each time, the darknet has bounced back. The latest crackdown drove cybercriminals to migrate to messaging apps such as WhatsApp, Facebook Messenger and Telegram in order to trade stolen credit cards, account information, malware and drugs.[6]

What we're seeing is a more coordinated integration of cybercrime and terrorism. In January 2015, evidence emerged of a terror cell using bitcoin to fund operations. In another instance, an Indonesia-based group collected bitcoin donations on the darknet and hacked a trading website using a stolen identity. The group collected around US$600,000 via a series of cybercrimes.[7] In Australia, recent high-profile breaches of anti-money-laundering and counter-terrorism-financing (AML/CTF) provisions by two major banks and casino operators have shone light on systemic gaps in our provisions. The Commonwealth Bank of Australia was recently found to be in breach of AML-CTF laws in 52,700 instances and was fined $700 million for failing to report multiple deposits made for money-laundering purposes through its ATMs. In September 2020, Westpac was fined $1.3 billion for breaching AML/CTF laws 23 million times.[8]

In the past, cyber terrorism has been a contested concept, with no agreed-upon definition. It's now generally accepted that cyber terrorism involves the use of computers to create a severe disruption to critical infrastructure, causing death or the spreading of fear. But the use of digital and online technologies to enable terrorism, whether by providing a platform to inspire, recruit, communicate and coordinate or to raise illegal funds, has not really been considered in that definition.

Conclusion and recommendations

The interface of cybercrime and terrorism gives us a more practical way to conceptualise cyber terrorism in the modern context, and a more concrete target for focusing our efforts. To that end, I suggest a definition of cyber terrorism as 'the use of cyberspace to enable, inspire, influence or direct a terrorist attack or to raise funds to facilitate such attacks'.

This approach to cyber terrorism would allow law enforcement practitioners and legislators to target online activities used in support of a terrorism. For this reason, Australia needs to ensure that our AML/CTF laws are up to the task of preventing criminal syndicates and terrorist actors from exploiting our financial systems.

Australia also needs more trained experts in early detection, with more resources devoted to monitoring online behaviours that precede violent action. University courses that equip graduates with the understanding and skills to tackle cyber-enabled criminal activity of all types (including terrorism) need to be more widely available.

It's imperative that our future law enforcement practitioners have a strong understanding of how the internet, in all its pervasiveness, has become a tool for opportunists who seek to exploit it for criminal purposes. Our future counterterrorism preparedness depends on it.

Notes

1 Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, US Government, January 2018, online.

2 H Willems, 'Development, patterns and causes of violence against foreigners in Germany: social and biographical characteristics of perpetrators and the process of escalation', *Terrorism and Political Violence*, 1995, 7(1):162–181.

3 *Vehicles as weapons of terror*, Counter Extremism Project, December 2020, online.

4 The online behavioural profile presented in this chapter is based on my work as Director of the Countering Online Violent Extremism research program based at Curtin University, Western Australia. That work has been published elsewhere.

5 C Bennett, '"Trucks, knives, bombs, whatever": exploring pro-Islamic State instructional material on Telegram', *CTC Sentinel*, 2018, 11(5):23–29.

6 Samuel Gibbs, Lois Beckett, 'Dark web marketplaces AlphaBay and Hansa shut down', *The Guardian*, 21 July 2017, online; 'AlphaBay: Global authorities shut down dark net market 10 times the size of 2013's Silk Road', *ABC News*, 21 July 2017, online; Chris Baraniuk, 'AlphaBay and Hansa dark web markets shut down', *BBC News*, 20 July 2017, online.

7 Resty Woro Yuniar, 'Bitcoin, PayPal used to finance terrorism, Indonesian agency says', *Wall Street Journal*, 10 January 2017, online.

8 James Eyers, 'Westpac settles AUSTRAC case for $1.3b', *Australian Financial Review*, 24 September 2020, online.

The evolution of resilience to violent extremism

PROFESSOR MICHELE GROSSMAN
Research Chair in Diversity and Community Resilience, Alfred Deakin Institute for Citizenship and Globalisation, Deakin University

Melbourne, Australia

‘Resilience’ has been a byword in preventing and countering violent extremism (P/CVE) approaches for at least a decade.[1] But what does resilience to violent extremism mean, how has it evolved over time, what gaps persist, and how responsive are current resilience-based policies and programming in a complex contemporary threat landscape?

Overview

Resilience has become embedded in P/CVE thinking to the extent that many now consider it a ‘key ingredient to effectively manage terrorism’.[2] A wide range of national, international and multilateral policy frameworks and bodies have at some point explicitly framed ‘resilience’ as a core element of their resourcing and programming approach.[3]

Debate continues about how best to define resilience, ranging from seeing it as an individual or collective trait that enables ‘bouncing back’ from crises or challenges[4] to more nuanced approaches that understand resilience as multidimensional social processes.[5] One point of agreement, however, even when concepts or definitions vary, is that adversity or challenge must be present for resilience to emerge. Violent extremism and terrorism are key examples of adversities in which resilience may surface and be tested at various points of risk and impact.

In response to calls for greater clarity about how the concept of resilience can successfully inform P/CVE models,[6] resilience as *resistance*, resilience as *prevention*, resilience as *adaptation*, or resilience as *recovery* variously appear in a wide range of articles, policies, programs and strategies, sometimes deploying different concepts within the same framework: for example, within different components of the UK’s CONTEST strategy, resilience is respectively defined as community *recovery from a crisis or disaster* but also as *community resistance to terrorist ideology*.[7] However, the most common concept of resilience in P/CVE contexts is linked to *prevention of* and *resistance to* violent extremism.

For the most part, this understanding is grounded in the social-ecological model of resilience.[8] This model conceptualises resilience as a *social process*, rather than simply an individual trait or characteristic. It sees resilience as the ability to thrive in contexts of adversity through positive, prosocial adaptation and transformation; emphasises the importance of identifying and mobilising protective factors that can offset risks and vulnerabilities; and highlights the capacity to access, navigate towards and draw on resilience resources that support coping with and overcoming hardship in culturally meaningful and socially just ways.

This formulation of resilience recognises that our ability to *prevent* violent extremism from taking hold of vulnerable individuals and groups, and our capacity to *resist* the messaging and narratives promoted by violent extremists as solutions to problems or grievances, is in large part dependent on how resilient we are at different scales—individual, family, community or society. It also considers the resilience of the many different, interacting systems that support or undermine our individual and collective wellbeing—health, education, cultural, legal, economic, environmental, and so on.

Individual and community resilience

At the level of individual resilience to violent extremism, researchers have identified psychosocial protective factors linked to empathy;[9] self-regulation/self-control and value complexity;[10] self-esteem and assertiveness;[11] intercultural tolerance of diversity;[12] and the ability to recover from a terrorist attack or reject extremist narratives.[13] Alongside these are more social ecology-oriented models that link individual resilience capacity to interactions with social contexts and systems such as families, schools, workplaces and the broader community.[14] Protective factors in these more socially dynamic models emphasise features such as social coping skills through anger management and conflict resolution; democratic citizenship; counternarratives; internet safeguarding measures; social and civic participation; a supportive and warm family environment; autonomy, self-esteem and sense of agency; and social and emotional wellbeing and life skills.[15] Neither the presence nor the absence of these factors is predictive of who may or may not radicalise to violence, but they do identify the multiple forms of social capital that can enable resilience to violence to develop and thrive.[16]

Yet the dominant trend has evolved to concentrate primarily on building community rather than individual resilience to violent extremism. This reflects three trends in the way that the field has evolved in its thinking about resilience over time. First, such thinking relies on an understanding of violent extremism itself as comprising social ecologies of group-level rather than individual-level processes, based on an understanding of radicalised individuals as embedded within and influenced by group-level processes and networks. Second, it has been shaped by the pragmatic needs of governments that have sought to extend and simplify their policy reach as much as possible in relation to violent extremism by focusing resources and efforts on primary, ‘whole of society’ prevention efforts through encouraging the non-violent resolution of grievances and addressing the underlying adversities that have seeded those grievances. Third, and most problematically, it has relied on a tendency to attribute violent extremist ideologies and behaviours to *communal identity* structures (such as religion, race and gender) rather than to *communal ideological or belief* structures (for example, violent jihadist, white supremacist, incel).

The ‘community’ in community resilience to violent extremism

‘Community’ in the context of resilience to violent extremism can sometimes denote either (or both) a *spatial concept of community*, such as a geographical or physical place, or a *relational concept of community* based on sense of belonging, solidarity, support, acceptance or similarity.[17] As a result, policy approaches have often centred on an understanding of community resilience to violent extremism that stresses the relationship between resilience and social capital.[18] If the drivers of violent extremism are bound up with socially based dynamics and adversities, then the solutions that seek to protect against those drivers must also be socially based and enacted (by addressing economic disadvantage, social marginalisation and exclusion, or the sense of political disenfranchisement in particular communities, for example).[19] Yet, regardless of whether ‘community’ is defined spatially, relationally, or both, policy risks can emerge when complex communities are treated as homogeneous entities, rather than as social formations involving contested or multilayered views, positions and forms of power and influence within them. One example of these risks is the tendency to favour policy-focused dialogue with male community leaders in ways that ignore or minimise the effectiveness of women’s influence and contributions in developing community-level solutions and interventions.[20]

At its best, this has enabled a move away from more securitised approaches based on ‘risk society’[21] assumptions that target particular communities as suspect, vulnerable or deficient,[22] instead emphasising the positive resilience capital[23] that communities bring to the challenges of preventing or resisting violent extremism.

Persisting gaps and new challenges in resilience to violent extremism

Yet gaps in how P/CVE frameworks conceptualise and operationalise resilience to violent extremism persist. One gap is the tendency to see resilience as stopping at the threshold of individuals and communities, without considering the need for comparable resilience—marked by features such as openness to experimentation and learning, the capacity to adapt and transform, and both redundancy and participation across multiple, interdependent systems[24]—at the levels of policy and governance, for example, by being more willing to genuinely share power with communities when designing government–community partnerships, or enhancing multiple reporting channels for community concerns about violent extremism across states and territories. Such a stance fails to account for the range of co-occurring systems that make up the P/CVE resilience matrix.

A second gap is the failure of much P/CVE policy and programming to engage systematically with the resilience of violent extremist groups and movements themselves. Multisystemic resilience, for example, includes features such as openness to new information, the capacity to integrate environmental shocks and the ability to pivot towards new behavioural regimes. This can easily be applied to various terrorist or violent extremist movements themselves, which have demonstrated their capacity over time to integrate environmental shocks (such as financial or territorial losses), initiate new behavioural regimes (for example, shifting from large-scale, high-tech to small-scale, low-tech domestic attacks), and transform in response to various stressors (such as internal leadership competition or digital take-downs). They have also proved adept at negotiating new resources by decentralising resource bases to create local franchises or diversify digital platforms and strategies. Recognising and addressing these resilient features of terrorist movements is an essential part of our own resilient response when we’re designing and trialling interventions.

Finally, a new challenge is whether the focus on building broad, community-level resilience responds sufficiently to the current threat landscape. Community resilience to violent extremism assumes that we’re trying to reach, support and strengthen the resources of vulnerable people through the systems in which they're embedded, including the family, education, the workplace or broader social messaging. Yet the rise of lone-actor terrorism and the emergent threats of right-wing violent extremism arguably present a more complicated landscape than that of the past 10 years—one in which 'community' is often digital in nature, based on social connectivity through amplified grievances rather than prosocial support, and also one in which vulnerable people are frequently disconnected from, disenchanted by or mistrustful of established systems that might otherwise support them. This raises the question of whether we need to reconfigure our approach to building community resilience to violent extremism by attending further not only to individual resilience capacity, but also to more generalised community resilience that can help restore confidence and connection with the social resources needed to help people cope with multiple challenges, including loss of trust in the public sphere, lack of economic security and the perception of being socially devalued or 'left behind'. Such generalised community resilience also needs to address and, where possible, positively exploit the shifting ecology of online communications and the centrality of digital literacy and consciousness that's now reshaping our cultures and societies in many ways and at many levels.

The evolution within the P/CVE field on the importance of building systems that go beyond an immediate concern with social or political violence towards protective factors such as social capital and connectedness, economic and social support and development systems, and education, health, social welfare and human rights has been a welcome development.

Building resilience to violent extremism means developing not just a 'whole of community' but a 'whole of systems' approach that encompasses all the actors involved in the P/CVE matrix, including governments and terrorist movements alike. We also need to engage in continuous assessment of whether the policy and program settings for resilience to violent extremism developed over the past decade are now responsive to the current domestic and transnational threat landscape.

Notes

1 A Dalgaard-Nielsen, P Schack, 'Community resilience to militant Islamism: who and what? An explorative study of resilience in three Danish communities', *Democracy and Security*, 2016, 12(4):309–327, online; M Grossman, M Peucker, D Smith, H Dellal, *Stocktake Research Project: a systematic literature and selected program review on social cohesion, community resilience and violent extremism 2011–2015*, Victoria University and Australian Multicultural Foundation, Melbourne, 2016; PH Longstaff, NJ Armstrong, K Perrin, WM Parker, MA Hidek, 'Building resilient communities: a preliminary framework for assessment', *Homeland Security Affairs*, 2010, V1(3), article 6, online; B Spalek, L Davies, 'Mentoring in relation to violent extremism: a study of role, purpose, and outcomes', *Studies in Conflict & Terrorism*, 2012, 35(5):354–368, online; M Grossman, K Hadfield, P Jefferies, V Gerrand, M Ungar, 'Youth resilience to violent extremism: development and validation of the BRAVE measure', *Terrorism and Political Violence*, 30 January 2020, online; S Weine, S Henderson, S Shanfield, R Legha, J Post, 'Building community resilience to counter violent extremism', *Democracy and Security*, 2013, 9(4):327–333, online.

2 M Dechesne, 'The concept of resilience in the context of counterterrorism', in U Kumar (ed.), *The Routledge international handbook of psychosocial resilience*, Routledge, London and New York, 2017, 414–423.

3 This includes Public Safety Canada's *Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy* (2013), the Council of Australian Governments' *Australia's Counter-Terrorism Strategy: Strengthening our Resilience* (2015), the US's Strategic Implementation Plan for *Empowering Local Partners to Prevent Violent Extremism in the United States* (2011), and components of the UK's Prepare and Prevent streams within its anti-terrorism CONTEST strategy (2011). Internationally, building resilience to violent extremism also features strongly in the policy and practice frameworks of multilateral bodies such as the European Commission's Radicalisation Awareness Network, the Global Community Engagement and Resilience Fund and the Global Counter-Terrorism Forum.

4 S Mohaupt, 'Review article: Resilience and social exclusion', *Social Policy and Society*, 2009, 8:63–71. Longstaff et al., 'Building resilient communities: a preliminary framework for assessment'.

5 M Ungar, 'Practitioner review: diagnosing childhood resilience—a systemic approach to the diagnosis of adaptation in adverse social and physical ecologies', *The Journal of Child Psychology and Psychiatry*, 2015, 6(1):4–17. online; M Ungar, 'Systemic resilience: principles and processes for a science of change in contexts of adversity', *Ecology and Society*, 2018, 23(4):34, online; AS Masten, 'Resilience in developing systems: the promise of integrated approaches', *European Journal of Developmental Psychology*, 2016, 13(3):297–312, online.

6 Longstaff et al., 'Building resilient communities: a preliminary framework for assessment'; M Grossman, H Tahiri, P Stephenson, *Harnessing resilience capital: an investigation of resilience and cultural diversity in countering violent extremism*, Australia – New Zealand Counter-terrorism Committee, Canberra, 2014; M Grossman, 'Resilience to violent extremism and terrorism: a multisystemic analysis', in M Ungar (ed.), *Multisystemic resilience: adaptation and transformation in changing contexts*, Oxford University Press, Oxford, 2021.

7 K Hardy, 'Resilience in UK counter-terrorism', *Theoretical Criminology*, 2015, 19(1):77–94.

8 C Hunter, 'Is resilience still a useful concept when working with children and young people?', *Journal of the Home Economics Institute of Australia*, 2012, 19(1):45–52; L Liebenberg, M Ungar, F Van de Vijver, 'Validation of the child and youth resilience measure-28 (CYRM-28) among Canadian youth', *Research on Social Work Practice*, 2011, 22(2):219–226, online; AS Masten, 'Global perspectives on resilience in children and youth', *Child Development*, 2014, 85(1):6–20, online; D Stokols, RP Lejano, J Hipp, 'Enhancing the resilience of human–environment systems: a social–ecological perspective', *Ecology and Society*, 2013, 18(1):7, online; M Ungar, 'Resilience across cultures', *British Journal of Social Work*, 2008, 38:218–235, online; M Ungar, 'The social ecology of resilience: addressing contextual and cultural ambiguity of a nascent construct', *American Journal of Orthopsychiatry*, 2011, 81(1):1–17, online; Ungar, 'Practitioner review: diagnosing childhood resilience—a systemic approach to the diagnosis of adaptation in adverse social and physical ecologies'; M Ungar, 'Systemic resilience: principles and processes for a science of change in contexts of adversity', *Ecology and Society*, 2018, 23(4):34, online; TM Yates, AS Masten, 'Fostering the future: resilience theory and the practice of positive psychology', in PA Linley, S Joseph (eds), *Positive psychology in practice*, John Wiley & Sons, Hoboken, 2004, 521–539.

9 A Aly, E Taylor, S Karnovsky, 'Moral disengagement and building resilience to violent extremism: an education intervention', *Studies in Conflict & Terrorism*, 2014, 37(4):369–385, online; BOUNCE, *Resilience training, network and evaluation STRESAVIORA II (Strengthening Resilience against Violent Radicalisation 2015–2018*, European Commission with the Egmont Institute, Brussels, 2018; F Lösel, S King, D Bender, I Jugl, 'Protective factors against extremism and violent radicalization: a systematic review of research', *International Journal of Developmental Sciences*, 2018, 12(9):1–14, online; W Stephens, S Sieckelinck, H Boutellier, 'Preventing violent extremism: A review of the literature', *Studies in Conflict & Terrorism*, 2 January 2019, online; EL Taylor, PC Taylor, S Karnovsky, A Aly, N Taylor, '"Beyond Bali": a transformative education approach for developing community resilience to violent extremism', *Asia Pacific Journal of Education*, 2017, 37(2):193–204, online; B Van Brunt, M Murphy, A Zedginidze, 'An exploration of the risk, protective, and mobilization factors related to violent extremism in college populations', *Violence and Gender*, 2017, 4(3), online; S Sieckelinck, AJ Gielen, *Protective and promotive factors building resilience against violent radicalisation*, RAN issue paper. European Commission, 2017.

10 Lösel et al., 'Protective factors against extremism and violent radicalization: a systematic review of research'.

11 BOUNCE, *Resilience training, network and evaluation STRESAVIORA II (Strengthening Resilience against Violent Radicalisation 2015–2018*.

12 HB Ellis, S Abdi, 'Building community resilience to violent extremism through genuine partnerships', *American Psychologist*, 2017, 72(3):289–300, online.

13 Radicalisation Awareness Network (RAN), 'Ex post paper, research seminar', 17 October, RAN, Amsterdam, 17 October 2018, online.

14 U Bronfenbrenner, PA Morris, 'The bioecological model of human development', in RM Lerner, W Damon (eds), *Handbook of child psychology: theoretical models of human development*, John Wiley & Sons, New York, 2006, 793–828.

15 S Sieckelinck, AJ Gielen, *Protective and promotive factors building resilience against violent radicalisation*, RAN issue paper, European Commission, 2017.

16 Grossman et al., 'Youth resilience to violent extremism: development and validation of the BRAVE measure', 2.

17 Ellis & Abdi, 'Building community resilience to violent extremism through genuine partnerships', 291.

18 Dalgaard-Nielsen & Schack, Community resilience to militant Islamism: who and what? An explorative study of resilience in three Danish communities'; Ellis & Abdi, 'Building community resilience to violent extremism through genuine partnerships'; Grossman et al., *Harnessing resilience capital: an investigation of resilience and cultural diversity in countering violent extremism*; Grossman et al., 'Youth resilience to violent extremism: development and validation of the BRAVE measure'.

19 J Day, S Kleinmann, 'Combating the cult of ISIS: A social approach to countering violent extremism', *The Review of Faith & International Affairs*, 2017, 15(3): 14-23, online.

20 M Grossman, S Carland, H Tahiri, A Zammit, *Roles of Women in Supporting and Opposing Violent Extremism: The Australian Landscape*, Australia-New Zealand Counter-Terrorism Committee, Canberra, 2018, online.

21 U Beck, *Risk society: towards a new modernity*, trans. Mark Ritter, Sage Publications, London, 1992; A Giddens, 'Risk and responsibility', *Modern Law Review*, 1999, 62(1):1–10; D Lupton, *Risk*, Routledge (Psychology Press), London, 1999.

22 A Kundnani, 'Radicalisation: the journey of a concept', *Race and Class*, 2012, 54(2):3–25, online; B Spalek, 'Community policing, trust and Muslim communities in relation to "new terrorism" politics and policy', *Politics and Policy*, 2010, 38(4):789–815; online; F Vermeulen, 'Suspect communities—targeting violent extremism at the local level: policies of engagement in Amsterdam, Berlin, and London', *Terrorism and Political Violence*, 2014, 26(2):286–306, online.

23 Grossman et al., *Harnessing resilience capital: an investigation of resilience and cultural diversity in countering violent extremism*.

24 Ungar, 'Systemic resilience: principles and processes for a science of change in contexts of adversity'.

Operational perspectives on terrorism and managing the risk

COMMANDER SANDRA BOOTH
Australian Federal Police
Canberra, Australia

ASSOCIATE PROFESSOR DR NATALIE DAVIS
Australian Federal Police
Canberra, Australia

Overview

Over the past decade, the numbers of terrorist investigations and people charged with terrorism-related offences in Australia have continued to rise. As a result, the number of convicted terrorism offenders released from prison has also increased and will continue to do so. In the changing landscape of terrorism and investigations, law enforcement and its partners must increasingly share information and respond collaboratively to all threats to the community from ideologically driven attacks. In addition to the ongoing risk of violent Islamic extremism, that landscape includes growing threats from right-wing extremists using the internet to promote their ideology.

Operational perspectives on terrorism affecting Australia

Since September 2014, when the national threat level was raised to 'probable', 128 people have been charged as a result of 59 counterterrorism-related operations around Australia.[1] The landscape for terrorist activity is dynamic and evolving, and, although Islamic extremism continues to cause the highest workload for government agencies, Australian Federal Police Deputy Commissioner Ian McCartney has identified an increase in investigations associated with other ideologies.[2] Far-right extremism is now seen as an increasing concern for law enforcement. Australian Security Intelligence Organisation (ASIO) Director-General Mike Burgess has also acknowledged those rising concerns and has estimated that ASIO's workload dealing with far-right extremists has increased to 30%–40%, up from 10%–15% before 2016.[3] Burgess has stated that right-wing extremists are more organised, sophisticated, ideological and active than in previous years.

Since the outbreak of the Covid-19 pandemic in 2020, the UN Security Council, along with law enforcement and intelligence agencies, has acknowledged increasing concern for at-risk individuals who are vulnerable to extremist ideologies that promote violence.[4] Young people being aggressively radicalised both on- and offline has been highlighted as an ongoing threat to Australia.[5] Burgess expanded on those concerns, stating that the novel coronavirus had reinforced conspiracy theories, and that the pandemic is being used by radicals online as 'proof' that democratic societies are at risk of collapse and that a race war is inevitable.[6] Although the narrative used by those groups might not be convincing to most people, that message could work with people vulnerable to the rhetoric, which might result in increasing support for the use of violence to achieve political goals.

Counterterrorism strategies to deal with high-risk terrorism offenders

From 2019, about 70 individuals have been or are due for release from prison, having served their sentences for terrorism-related offences. Questions have been raised about the risk posed to the community by the release of those offenders. While some international recidivism rates are reportedly as low as 0%,[7] those figures have been affected by the attacks by Usman Khan and Sudesh Amman, who were released terrorism offenders, in the UK in 2019 and 2020, respectively. The low rate of recidivism in a single jurisdiction is in contrast to relatively high rates of criminal and terrorist recidivism elsewhere.[8]

However, law enforcement agencies have encountered difficulties in assessing recidivism internationally because of a number of factors. Those factors include differences in the definition of recidivism, which might involve the commission of subsequent terrorism offences after a term of imprisonment or engaging in other criminal acts, or cases in which no one was charged (such as when someone has died as a result of their own actions). Further difficulties lie in the low base rate of terrorist offences and in the lengthy prison terms imposed, both of which make it difficult to establish empirical evidence of recidivism. For example, one terrorist offender in Australia isn't due for release until 2060, so it's difficult to determine her risk of future violent extremist activity or support for violent activity after her release.

Finally, the notion that offenders disengage from terrorism while in prison is now being reconsidered. While an offender might display positive behaviour in custody, they may have merely 'gone grey' while incarcerated. There is danger in placing too much emphasis on an offender's good behaviour in custody. Many terrorist offenders commit their offences when their behaviour is otherwise prosocial, and evidence suggests that they behave well while in custody.[9]

Legislative options

Through the *Criminal Code Act 1995*, a court may determine that a convicted terrorist offender may pose an unacceptable risk of violent extremism if they were to be released from prison. The court can make orders for the person to be placed on an interim control order, identifying controls to mitigate the risk they may pose to the community. Such controls can include curfews and bans on access to certain websites or associates. The conditions must be specific to the violent extremism risk posed by the individual. Although not a requirement under the legislation, consideration may also be given to their likelihood of successful reintegration into the community and their social networks, which may mitigate the risk of future ideologically driven violent behaviour.

Risk assessment and mitigation

The release of a terrorism offender at the completion of their sentence when there are still concerns about the risk they pose to the community is a vexing problem for decision-makers. It's vexing partly because the core concept of our justice system is that offenders should be returned into society once they have served their sentenced terms.

The control order regime was established to ensure the physical safety of the community by mitigating the risks of individuals participating in future violent extremist activities. Although not required as part of a control order, there's also a focus on assisting each individual to reintegrate into the community on release.

Risk is difficult to quantify, but risk assessments are more useful, robust and defensible when they consider all factors that affect the individual offender and the likelihood that they'll cause harm to the community.

A violent extremism risk assessment shouldn't be completed in isolation. A comprehensive picture of the individual can be gained from additional information about them, such as a psychometric assessment, their history, their social networks and protective factors that might mitigate the risk and inform a more comprehensive risk assessment. Although risk can never be entirely eliminated (or it wouldn't be risk), effective risk management can minimise and mitigate risks that have been clearly identified.

The factors that affect a risk assessment can include both *static* and *dynamic* factors. Static factors (for example, a childhood history of family dysfunction) are unchangeable over time, whereas dynamic factors (such as access to weapons, the person's social networks and support, and external environmental factors such as foreign policy) are changeable. While static factors are important considerations, dynamic risk factors can be more telling in a context of violent extremism. Risk assessments need to be repeated in an ongoing process sensitive to triggers (such as changes in the person's family) and the emergence of new forms of threat (for example, a new social network of supporters of violent extremism). The assessment needs to be based on a risk model that identifies those factors that are most influential in changing the level of risk. That, in turn, assists in prioritising resources and approaches relevant to the specific risk.[10]

When assessing a person's risk of future violent extremism, it's important to assess their behaviour and cognition. Some assessors have placed weight on the reported responses of convicted terrorists to questions about their intentions, motivations and experiences. However, due to issues such as recall bias and political bias, care should be taken when interpreting a person's account of why they joined a group.[11] There are also possible problems involving self-censorship, as convicted interviewees may adjust their accounts to fit a broader political narrative.

Risk assessments are regularly conducted on offenders to determine their risk of reoffending in the future. Risk assessment instruments for future sexual offending (such as Static-99R or RSVP) or violent offending (such as HCR-20) can help to identify factors that may increase the likelihood of the person reoffending. Empirical data supports the use of certain instruments to assess the risk of sexual and violent offending, but not for violent extremist offending. This means that the hazard in question isn't common compared to other forms of behaviour, and a violence risk assessment instrument might not identify the risk for violent *extremism*; for example, such instruments don't seek information on violent extremist ideology.[12] In the terrorism arena, the base rate for offending, compared to the numbers of sexual and violent offenders, is low and is likely to remain low. As an example, the base rate for homicide in the US in 2018 was 5.3 cases per 100,000 people.[13] In comparison, the rate for major cardiovascular disease was 163.6 cases per 100,000 people in the same year.[14] In terrorist cases, the rate is even more problematic: in 2018, 45 people were killed by terrorist acts in the US,[15] which leads to an estimated death rate due to terrorism of 0.014 cases per 100,000 people. Therefore, although the base rate for terrorist events is extremely low and the recidivism risk is difficult to quantify, the consequences of such an event can be a catastrophic death toll and psychological damage to the population in general.

Recommendations to counter terrorist threats and funding support to terrorist groups

The future for the investigation, management and mitigation of the risk of violent extremists to the Australian community will continue to be a vexing problem for government and non-government agencies. No longer does law enforcement focus solely on the arrest, charging and sentencing of offenders to reduce the risk of violent extremism to public safety. Law enforcement must be dynamic, malleable and agile to respond to emerging issues and the changing terrorism landscape. Those employed to counter terrorism need to stretch themselves and collaborate with non-traditional partners to develop new and innovative strategies to address the issue. That will continue to require a shared and collaborative response by government and non-government agencies, along with communities, who are often best placed to identify an individual's increasing support for violent extremism, to report concerning behaviour, to help redirect the individual away from violent radicalisation and to reintegrate them into the community through intervention programs.

Policy and legislation

Policymakers in government are essential in working alongside law enforcement to develop options for the mitigation of the risk posed by those who support violence to achieve their goals and propagate their beliefs. This has been demonstrated, for example, by the Australian Federal Police engaging with the Department of Home Affairs to develop policies and strategies to address violent extremism in Australia, including by addressing legislative gaps as we continue to learn about the evolving terrorist environment. That work has included social cohesion and community engagement activities to integrate those vulnerable to radicalisation and support for violence into a pluralistic and multicultural society.

Human sciences and practitioners

There's an increasing recognition of the need for social science researchers to collaborate with law enforcement practitioners to develop theories on new and emerging issues and to identify opportunities to mitigate terrorism risks. Research helps inform decision-making based on evidence about the motivations, intent and ideological drivers of violent extremists.

To make it more likely that people at risk of violent extremism will be identified early and risks to the community will be reduced, we need to identify typical behaviours of supporters of extremism, consider the whole of their life cycle when they come to the attention of authorities, and address concerning behaviours through mitigation strategies. Although it isn't possible to predict precisely who will go on to commit violent extremist acts, the identification of potential indicators of violent extremism and the professional judgement and experience of human science practitioners support law enforcement decisions that are often made in real time and during critical stages of an investigation.

Government and non-government collaboration

Law enforcement, intelligence and non-government agencies should continue and enhance their collaboration to establish procedures and processes to address the ongoing risk posed by individuals and groups who want to harm the community. It's only through shared responsibility and collaboration that we'll be able to understand the enduring risk posed by violent extremists intending to destabilise democratic and multicultural societies and to identify, assess and mitigate that risk.

Notes

1 Correct at 27 January 2021.

2 Senate Estimates, 20 October 2020.

3 'Neo-Nazis among Australia's most challenging security threats, ASIO boss Mike Burgess warns', *ABC News*, 24 February 2020, online.

4 Counter-Terrorism Committee Executive Directorate (CTED), *Member states concerned by the growing and increasingly transnational threat of extreme right-wing terrorism*, CTED trends alert, UN, July 2020, online.

5 Senate Estimates, 20 October 2020.

6 'Neo-Nazis among Australia's most challenging security threats, ASIO boss Mike Burgess warns'.

7 A Silke, J Morrison, *Re-offending by released terrorist prisoners: separating hype from reality*, International Centre for Counter-Terrorism, The Hague, 2020.

8 MB Altier, E Leonard Boyle, JG Horgan, 'Returning to the fight: an empirical analysis of terrorist reengagement and recidivism', *Terrorism and Political Violence*, 18 November 2019, online. See also B Hasisi, C Tomer, D Weisburd, M Wolfowicz, 'Crime and terror: examining criminal risk factors for terrorist recidivism', *Journal of Quantitative Criminology*, 2020, 36:449–472.

9 J Hall, *Terrorist risk offenders: independent review of statutory multi-agency public protection arrangements*, UK Government, 2020, online.

10 K Roberts, J Horgan, 'Risk assessment and the terrorist', *Perspectives on Terrorism*, 2008, 2(6).

11 T Schmutz, '"Lone soldiers" in the Israeli military—a research note on the conceptualization of foreign fighters', *Terrorism and Political Violence*, 23 October 2020, online.

12 RTI International, *Countering violent extremism: the application of risk assessment tools in the criminal justice and rehabilitation process*, US Department of Homeland Security, 2018, online.

13 Federal Bureau of Investigation, *Crime in the United States, 2018*, US Government, 2018 online.

14 *Number of deaths due to diseases of the heart per 100,000 population. Timeframe: 2018*, KFF, 2019, online.

15 START: National Consortium for the Study of Terrorism and Responses to Terrorism, *Trends in global terrorism: Islamic State's decline in Iraq and expanding global impact; fewer mass casualty attacks in Western Europe; number of attacks in the United States highest since 1980s*, University of Maryland, October 2019, online.

Understanding transitions to violence and the role of practitioner–academic partnerships

DEPUTY COMMISSIONER ROSS GUENTHER
Public Safety and Security, Victoria Police

Melbourne, Australia

ASSOCIATE PROFESSOR DEBRA SMITH
Principal Research Fellow, Institute for Sustainable Industries & Liveable Cities, Victoria University

Melbourne Australia

Since the establishment by the Islamic State of Iraq and the Levant (ISIL) of its so-called caliphate in June 2014, the Australian domestic terrorist threat environment has undergone significant change. In Victoria, and for the rest of Australia, this transformation was marked by Numan Haider's attack on two members of Melbourne's Joint Counter Terrorism Team in September 2014. Arguably the first attack of its type anywhere in the Western world in response to ISIL's call for domestic acts of violence,[1] that incident had many of the hallmarks that would come to characterise future actual and planned attacks in other parts of Melbourne and Australia.

The operational implications for counterterrorism (CT) policing have been both complex and profound as a result of the elevation to a new level of the threat of lone-actor, low-capability terrorism. The direct operational effects of overseas events and propaganda, the increasing influence of mental health issues and the truncation in some instances of terrorists' decision-making and planning processes have complicated matters further. In fact, the appeal of ISIL's ideological message achieved a level of motivational resonance previously unseen in Australia, no doubt bolstered by the idea of the purported caliphate itself. The result has been a significant proliferation of CT persons of interest (POIs).

In more recent times, the growth in right-wing extremism has added to the challenges of managing a rising, and increasingly diverse, POI cohort. The ability of police to identify and prioritise risk so that resources can be allocated where they're needed most is therefore a key prerequisite for effective POI management. Critically, this includes the capacity to make distinctions, sometimes quite subtle, between individuals who are sympathetic to a terrorist cause and those who are more susceptible to using violence based upon their beliefs.

The need to make that important distinction, and the challenges inherent in being able to do so, were revealed in a recent UK Government report that examines terrorist recidivism. The report asks its readers to consider the case of an individual released from prison after serving a short prison term for downloading suspicious material likely to be useful to a terrorist. It goes on to ask, 'What is the likelihood that they will go on to carry out a violent attack on members of the public? What is the likelihood that they are merely fixated on extreme material readily available on the Internet?'[2] Those questions are more than just an exercise in intellectual curiosity.[3] They have significant real-world implications for operational CT policing because they directly inform priorities and the allocation of intelligence and investigative resources. While it isn't possible to predict with certainty whether an individual will engage in terrorist violence, the ability to make nuanced judgements about how people make the critical transition to violence has several implications for a range of CT activities, including in the following areas:

- *High-risk terrorism offenders (HRTOs):* In recent years, a number of terrorism offenders have been released from prison, and it's expected that this number will continue to grow. The management of these individuals is resource intensive and highly complex, while community expectations might even dictate a need to manage HRTOs for years. To a significant extent, therefore, their status as individuals who represent a risk of terrorist violence is determined by their previous offending. While that's clearly an important consideration, ultimately HRTOs' medium- to long-term management should largely be determined by the extent to which they represent an unacceptable risk to community safety. That requires the development of indicators that are sensitive to tipping points, because not everyone who's radicalised will engage in violence.[4] This, of course, also needs to be balanced against other types of risk, in the understanding that terrorist offending can take various forms, not all of which necessarily involve direct engagement in violence.
- *Residual or ongoing risk:* Events over the past several years, both in Australia and overseas, indicate that individuals who were formerly the subject of a CT investigation may re-emerge, months or years later, as significant terrorist risks. Indeed, some have chosen to engage in attacks that resulted in injury and the loss of life.[5] Those incidents have forced police to reconsider how they manage this 'residual' risk. The challenges associated with doing so, however, are significant. Finite resources clearly dictate that the focus of operational CT policing should be on those individuals who represent the most significant and imminent risk. However, we also know that risk isn't static. Police therefore need the confidence to downgrade the priority of POIs where the available intelligence and professional judgement dictate. The capacity to confidently make such evaluations, however, in no small part depends on the ability of police to possess and then contextualise new intelligence on those POIs as part of an ongoing risk assessment process. Establishing a nuanced, contemporary and empirically based understanding of the diverse circumstances under which individuals can transition to violence is a key foundation upon which this process rests.
- *Countering violent extremism (CVE):* Within Victoria Police, CVE has for the past 10 years been a critical component of the force's diverse CT arrangements. The very nature of this work involves working closely with community-based partners who, with the support of police, are taking on increasing responsibility for the management of CVE participants. Providing those partners with information to enhance their understanding of behaviours indicative of imminent terrorist activity can aid their decision-making on when a client may better be managed by police. The mutual identification and acceptance of critical thresholds of escalating risk, and the processes that they

might trigger, are fundamental to effective POI management and the maintenance of trust and transparent police–community relationships.

Given the operational importance of identifying individuals who are mobilising towards violence, Victoria Police's Counter Terrorism Command undertook internal research to identify specific circumstances that might contribute to an individual escalating from support for an ideology towards some form of terrorist action. Based on an in-depth examination of Victorian case studies, the research resulted in the development of a framework focused on four distinct circumstances that may correlate with an escalation towards committing a violent attack in Australia or participating in a foreign incursion. Those four circumstances were:

- a confluence of events generating intense emotions and/or grievance
- exposure to means and opportunity capable of recalibrating perceived chances of success
- costs associated with action are lowered and the costs of not acting are raised
- the intensification of perceived pressure to act.

The research further developed 19 corresponding observable behavioural indicators related to those four circumstances. Therefore, the framework that originated from this knowledge was an important step towards generating new hypotheses and better distinguishing individuals who may be mobilising towards violence from those who demonstrate broader support for the ideology without intending to act. Victoria Police subsequently sought to test those hypotheses, working with academics at Victoria University to develop a systematic and scientific method that enabled the integration of open and closed data sources to expand and deepen the police research.

From a research perspective, the project represented an opportunity to work with highly targeted data that focused specifically on mobilisation to extremist violence, rather than the broader and more contentious concept of radicalisation. Indeed, research on radicalisation has been widely criticised for contributing to the creation of 'suspect communities', partly through a lack of focus on how to identify the few people who are inclined to act violently on extreme views.[6] The lack of research focusing specifically on mobilisation is in part a result of the difficulties involved in accessing information on individuals in the lead-up to engaging in violence.

The combined Victoria University and Victoria Police research team adopted a comparative case study approach, drawing on 12 cases of people who had engaged in or attempted to engage in violent extremism and six cases of people who expressed support for violent extremism but stopped short of transitioning to violence. The supporters who didn't transition to violence acted as a control group. Including a control group is methodologically important to understand what factors distinguish between radicalisation and an individual's mobilisation to violence, yet they're remarkably rare in studies of violent extremists.[7] The Victoria University researchers gathered data from various open sources, and Victoria Police added data from restricted sources where it was available.

The project found empirical support for a number of the variables examined. The most strongly supported of the four circumstances highlighted by Victoria Police's internal research was the third (*costs associated with action are lowered and the costs of not acting are raised*), in which four of the six associated variables were present. We also established support for two of the seven variables associated with the first circumstance (*confluence of events to generate intense emotions and/or grievance*), as well as one of the variables associated with both other circumstances (*intensification of perceived pressure or need to act and exposure to means and opportunity capable of recalibrating perceived chances of success*).

The results of the study pointed to the importance of collaborative research between law enforcement and academia to enable the generation of fine-grained insights into mobilisation from supporter to active participant in violent extremism, which are so operationally important. Generating data points from closed sources enriched the evidence base and significantly contributed to the ability to develop control cases and make useful comparison points.

From the perspective of operational CT policing, the research outcomes have formed the foundation for the contemporisation of tools used by investigators and analysts to prioritise POIs. Importantly, this has led to a focusing on risk factors and behavioural indicators previously not formally included in the POI assessment process, particularly those grounded in individuals' emotional states. Moreover, the research identified some risk factors considered counterintuitive, the presence of which may previously have led to a downgrading or moderation of a POI's risk profile. Ultimately, these new insights reflect the mutable nature of the terrorist threat and therefore the need to regularly revisit our contemporary understandings and assumptions of how and why individuals are radicalised to violence.

Beyond the project outcomes, several other benefits arose from the collaborative, co-production approach. For the police personnel, being physically embedded in the academic research team with adjunct status provided greater insight into the processes underpinning scientific inquiry, enhancing transferable skills that can be used in their core roles in policing. It also generated greater transparency and practitioner confidence in the outcomes and applicability of the research. For the academics, working alongside the police personnel provided rare insight into how terrorism research is applied operationally, while also providing an opportunity to nuance their understanding of violent extremism in ways that will shape and influence their further studies. It also helped them understand the limits of open-source data, providing insight into how that data can most effectively be used, as well as some of its limitations.

For both partners, the importance of developing a research relationship that extends beyond a specific short-term project became clear. While there are several models for conducting joint police–academic research, the benefits of co-production through a program of iterative research, building each stage on previous knowledge, provides a strong model for combining the resources, skills and expertise of the different organisations to achieve more targeted and operationally applicable results. While this does sometimes result in demands on each party as they navigate their different working cultures and expectations, each party becomes more adapted to their role in the applied research process as the relationship matures and carries that forward into new areas of inquiry.

Notes

1 ISIL spokesman Abu Mohammad al-Adnani made the speech ‘Your Lord is ever watchful’, which called for domestic acts of violence, on 20 September 2014. Haider’s attack was on 23 September 2014.

2 Jonathan Hall, *Terrorist risk offenders: Independent Review of Statutory Multi-Agency Protection Arrangements*, UK Government, 2020, 7, online.

3 Recent attacks in the UK, including those perpetrated by individuals who participated in terrorist rehabilitation and reintegration programs, demonstrate the risk of terrorist recidivism. For example, Sudesh Mamoor Faraz Amman and Usman Khan were responsible for attacks in London in 2020 and 2019, respectively.

4 Jamie Bartlett, Carl Miller, ‘The edge of violence: towards telling the difference between violent and non-violent radicalization’, *Terrorism and Political Violence*, 2012, 24(1).

5 See, for example, Dominic Grieve, *The 2017 attacks: What needs to change? Westminster, Manchester Arena, London Bridge, Finsbury Park, Parsons Green*, Intelligence and Security Committee of Parliament, UK, November 2018, online.

6 Michele Grossman, Mario Peucker, Debra Smith, Hass Dellal, *Stocktake Research Project: A systematic literature and selected program review on social cohesion, community resilience and violent extremism 2011–2015*, Department of Premier and Cabinet, Victorian Government, 2016; Kristina Murphy, Adrian Cherney, Julie Barkworth, *Avoiding community backlash in the fight against terrorism: research report*, Australian Research Council (grant no. DP130100392), 2015; Arun Kundnani, ‘Radicalisation: the journey of a concept’, *Race & Class*, 2012, 54(1).

7 Bartlett & Miller, ‘The edge of violence’; Michael Jensen, Gary LaFree, Patrick A James, Anita Atwell-Seate, Daniela Pisoiu, John Stevenson, Herbert Tinsley, *Empirical assessment of domestic radicalization (EADR)*, final report to the National Institute of Justice, Office of Justice Programs, US Department of Justice, Washington DC, 2016, online.

Countering violent extremism: the New South Wales approach

PIA VAN DE ZANDT
Director, Office of Community Safety and Cohesion,
New South Wales Department of Communities and Justice

Sydney, Australia

AFTAB MALIK
Research and Community Engagement Manager, Office of Community Safety
and Cohesion, New South Wales Department of Communities and Justice

Sydney, Australia

MADELEINE COOREY
Senior Policy Officer, Office of Community Safety and Cohesion,
New South Wales Department of Communities and Justice

Sydney, Australia

In New South Wales, our countering violent extremism (CVE) efforts are distinct from but complementary to our counterterrorism programs.[1] While counterterrorism is led by law enforcement and security agencies, CVE programs are primarily led by social policy agencies, working closely with NSW communities. Our CVE strategy encompasses programs that focus on prevention and early intervention, such as support and wellbeing programs in schools, a community helpline, and efforts with the NSW Police Force to combat bias crimes.[2] NSW agencies also deliver more targeted interventions, such as mental health support for fixated people who pose a threat, interventions for young people in youth justice and case management for those at risk of violent extremism, including families of foreign fighters returning to NSW. Because we, as a society, all share responsibility for countering hate and extremism, the NSW Government engages with community leaders, business and local government. We also work closely with academics and experts to commission research to ensure that we have the capability to respond to emerging issues. Our CVE efforts seek to build resilience and cohesion and protect, divert and disengage individuals from violent extremism. Underpinning that approach is an emphasis on evidence, trust and transparency.

Community as a source of strength

Engagement with communities is fundamental to the NSW approach to CVE.[3] We view our diverse communities as a source of strength, not suspicion. CVE is framed as 'a social issue with security implications'—not a security issue with social implications.[4] In NSW, we've found that consultation with, and providing feedback to, communities builds trust and transparency.[5] Recognising that both global events and domestic political rhetoric can affect social dynamics, the NSW Government engaged with community stakeholders—even those sceptical of the process—to co-design a strategic communications plan for use by our political leaders in the event of a terror attack. Likewise, we developed a community awareness-raising campaign about new laws designed to protect people from public threats of violence, based on their race or religious affiliation, with Keep NSW Safe, which is a coalition of 31 individuals and community groups.[6]

The NSW CVE approach encourages community autonomy, supporting communities to find solutions to our social cohesion challenges. The Community Partnership Action grants program (or COMPACT), led by Multicultural NSW, is one such example.[7] COMPACT is made up of an alliance of more than 60 grassroots community organisations, including charities, NGOs, sporting associations, private sector partners, schools and universities. In its first two years, COMPACT reached more than 20,000 young people, and 66% of participants reported that they had developed a greater level of acceptance of and respect for others.[8] COMPACT programs are locally designed, managed and implemented in the community.[9] By facilitating relationships within communities ('social bonding'), between communities ('social bridging') and between communities and institutions ('social linking'), we ensure that everyone who wants a role in preventing violent extremism has one.[10]

To ensure that we engage with and hear from new voices, we held a series of in-depth dialogues with Muslim youth leaders, women and religious leaders during 2019. Those roundtables helped us to engage with Muslims from diverse religious practices, ethnicities and cultures and understand barriers that may exist to engaging with existing CVE initiatives. We also gained insights from the community into possible new approaches to CVE.

Recurring criticisms that arose across our engagements included confusion about CVE and its intersection with counterterrorism; the persistent view that CVE focuses upon and securitises Muslims; and the perception that political rhetoric and media representations of Islam and Muslims play a role in creating societal divisions. We also learned that Muslim communities are willing to engage with CVE programs if the conditions are right; that there's an opportunity for governments to better communicate what CVE is and the role law enforcement plays; and that communities are seeking agency and autonomy, to be empowered to tell their own stories, including that of an 'Australian Islam'—an expression of Islam that's culturally relevant and, importantly, deeply connected with Australia's past.[11] Cognisant of such issues, the NSW Government is investing $12.3 million in CVE in 2020–21, with a focus on community-based programs. This may allow space for communities to challenge stereotypes and misconceptions about faith and tell their own stories. Opportunities to build on the trust already established with community leaders by NSW Police in CVE were also evident. While we acknowledge the inherent tensions of police involvement in CVE, we work closely with NSW Police to manage those tensions with communities so that critical partnerships can be sustained.[12] Importantly, by pursuing a broad-based CVE strategy, we may allay the apprehensions and fears held by Muslim communities and enhance their engagement with our CVE programs.[13]

While Islamist terrorism remains the most prominent threat,[14] we can't ignore the threat posed by other extremist ideologies—most notably far-right extremism.[15] We commissioned Macquarie University researchers to investigate the online narratives of far-right extremists. They found that those narratives highlighted the theme of a 'white identity' under threat, which is also evident among far-right extremist organisations in North America and Europe.[16]

The research raised awareness for government and civil society about the revolutionary and antisocial agenda of far-right extremist organisations. The project revealed a risk of a 'creeping threat' to liberal democracy when the activities of far-right extremists seek to widen the range of acceptable social and political discourse in our society (the 'Overton window') by using narratives that challenge Australian liberal democracy.[17]

The need for better metrics and evaluation

Since 2015, the NSW Government's investment in CVE has sought to increase the capacities of communities and government to respond to violent extremism and mitigate its social impacts. The program has focused on improving understanding of the complexities of radicalisation across government and service providers.[18] An independent evaluation found that our efforts increased community resilience, strengthened protective factors against violent extremism in NSW and increased CVE expertise and capacity in government. Significant relationships were also built across government and with the community.[19]

As part of an emphasis on evaluation, NSW is working to ensure that all CVE projects have a strong program logic to ensure that there's a coherent set of objectives and supporting activities to achieve the stated outcomes. This includes a robust data collection and evaluation plan. We aim to develop better metrics by collaborating, for example, with the Scanlon Foundation and other civil society organisations, to better understand the extent of social cohesion within NSW and the challenges and threats to our multicultural society.

Currently, we're working to align our CVE program indicators to the available evidence on 'what works' in other programs, such as youth crime prevention and youth justice programs, drawn from criminology, child protection and public health literature. We'll continue to examine whether this direction is viable and whether it can adequately measure success in diverting or disengaging individuals from extremism.

We've also developed a web-based, publicly available CVE program design and evaluation tool, funded by the Australian Government. It aims to assist CVE practitioners in government and community organisations to develop robust, evidence-based CVE programs and evaluate them.[20] Confronted by Covid-19, we've also begun to monitor the impact of the pandemic on social cohesion by analysing publicly available data to gauge public sentiment and identify pressure points that may strain social cohesion and foment violent extremism.

Next steps

We're adapting our programs to changing circumstances, such as those presented by the Covid-19 pandemic. For example, funding for COMPACT, our community grants program, has been increased. Developing global citizenship and digital intelligence will be a focus of programs for young people, and we'll seek to work more closely with local government and the private sector to reduce hate and extremism.

A key challenge for the future of our CVE program is its positioning in relation to counterterrorism. There are risks that confidence and trust can be undermined by the 'securitising' of programs, participants and communities. Over time, as agencies' programs continue to mature, it makes sense to make CVE 'business as usual' and build it into broader, mainstream government strategies. That would also help address CVE's reputation as being simply a part of counterterrorism. For example, CVE programs in schools might best sit within broader programs targeting antisocial behaviour, while intervention programs for young people at risk of extremism might work best as part of broader crime prevention efforts. If we're ultimately successful in embedding CVE as business as usual for NSW Government departments, and overcome the trust deficit with communities, we'll nonetheless still need to be able to identify CVE activities so that their successes may be measured, and any failures scrutinised. In 'mainstreaming' CVE initiatives, whole-of-government coordination and accountability shouldn't be lost.

The NSW Government would like to build CVE expertise among a broader group of policymakers and practitioners—people working in child protection, housing, mental health and disability services and people in community-based organisations in NSW. We're investing in improvements to our intervention program to better support at-risk individuals to resist violent extremist ideologies, including through a multi-NSW-agency panel. We're implementing more rigorous screening, assessment and case management for people at risk of extremism and developing an evidence base for our interventions. Our multi-agency approach—which includes representatives from NSW Police and health and education authorities—is also used to support families returning from foreign conflict zones as they reintegrate into NSW. In the youth justice arena, we're developing an evaluation framework so that we can build a better understanding of 'what works' for young people in detention.

NSW CVE practitioners engage in a global environment and collaboration—local, national and international—as a foothold into better practice. Importantly, we'll continue to emphasise that CVE is an issue that affects all of society, so we must work with a broad range of stakeholders to ensure that our society remains resilient, strong and cohesive.

Notes

1 Such complementarity is explained by the NSW Counter Terrorism Strategy. See Department of Communities and Justice, *NSW Counter Terrorism Strategy*, NSW Government, 2020, online.

2 Bias crime is described as crime in which 'the victim is targeted because of an aspect of his or her identity, including race, ethnicity, religion or sexual orientation.' See Gail Mason, 'A picture of bias crime in New South Wales', *Cosmopolitan Civil Societies: an Interdisciplinary Journal*, 2019, 11(1), online.

3 We believe that the best defence against violent extremism is strong, resilient individuals and communities. For example, see Multicultural NSW, *COMPACT: Program and Grants Information 2020–21*, NSW Government, 2020, online.

4 Anne Aly, Anne-Marie Balbi, Carmen Jacques, 'Rethinking countering violent extremism: implementing the role of civil society', *Journal of Policing, Intelligence and Counter Terrorism*, 2015, 10(1):9. Also, a recent review of CVE literature concludes that attempts to achieve a non-securitised approach have resulted in efforts to build community and individual resilience. See William Stephens, Stijn Sieckelinck, Hans Boutellier, 'Preventing violent extremism: a review of the literature', *Studies in Conflict & Terrorism*, 2 January 2019, online.

5 As has been noted, CVE generally operates in a 'significant trust deficit'. See Brian A Jackson, Ashley L Rhoades, Jordan R Reimer, Natasha Lander, Katherine Costello, Sina Beaghley, *Practical terrorism prevention: reexamining US national approaches to addressing the threat of ideologically motivated violence*, Homeland Security Operational Analysis Center, 2019, 3. Trust can be regained a number of ways, which include empowering local communities to deliver initiatives they believe address violent extremism and forming partnerships between organisations countering far-right extremism and Islamophobia that have robust evaluation processes in place to assess the success or failure of CVE initiatives. See Nada Roude, 'Australian Muslim leaders' perspectives on countering violent extremism: towards developing a best practice model for engaging the Muslim community', PhD thesis, Charles Sturt University, 2017.

6 The campaign can be viewed at *Stop Public Threats*, online.

7 A first-of-its-kind community resilience-building initiative, COMPACT seeks to mitigate the social impacts of violent extremism. Urbis, *Evaluation of the COMPACT Program*, report prepared for NSW Department of Premier and Cabinet, 28 November 2018, online.

8 Acil Allen Consulting, *NSW Countering Violent Extremism Program evaluation*, October 2019, 28–29, online.

9 Jackson et al., *Practical terrorism prevention*, xiii.

10 Stephens et al., *Preventing violent extremism*, 8.

11 While unrelated to and independent from CVE, Sheikh Wesam Charkawi, a Sydney-based scholar, locally funded and produced a documentary that sought to empower marginalised Muslim youth with a narrative that provided them with a sense of connection with Australia's historic past. Sheikh Wesam Charkawi, *Before 1770*, Abu Hanifa Institute, online.

12 Adrian Cherney and Jason Hartley acknowledge the 'problems', 'challenges' and 'inherent tensions' of police involvement in CVE efforts, but argue that the ability of police to 'reconcile and manage' those tensions with community stakeholders will determine just how effective and sustainable such partnerships will be. Adrian Cherney, Jason Hartley, 'Community engagement to tackle terrorism and violent extremism: challenges, tensions and pitfalls', *Policing and Society*, 2017, 27(7):750–763, online.

13 NSW engages with a wide range of non-Muslim and Muslim stakeholders representing diverse communities and ethnicities. In late 2019, that engagement led us to fund the Collaborative Approaches to Counter the Extremist Right-Wing and Islamophobia Threat conference. The symposium challenged the perception that CVE is concerned only with Islamist-inspired extremism, which, in turn, generated interest and intrigue in our work from sceptics and critics alike. The conference was described by the organisers as 'the first countering violent extremism (CVE) government-funded conference in Australia and the world dedicated specifically to examining the impact of the extremist right-wing and Islamophobia on social cohesion after the 15 March 2019 terrorist attack in New Zealand'. See Derya Iner, Priscilla Brice, *Collaborative approaches to counter the extremist right-wing and Islamophobia threats: a report on the NSW conference held on 21 November 2019*, Charles Sturt University, Sydney, 2019, 2. Isaac Kfir has observed that, while Islamophobia is rising, there exists a 'fundamental misunderstanding' of what it is. See Isaac Kfir, *18 years and counting: Australian counterterrorism, threats and responses*, ASPI, Canberra, 2019), 5, 22, online. For insights into the relationship between Islamophobia and radicalism, see John L Esposito, Derya Iner (eds), *Islamophobia and radicalization: breeding intolerance and violence*, Palgrave Macmillan, Switzerland, 2019.

14 The Australian Security Intelligence Organisation (ASIO) states that the 'principal source of the terrorist threat remains Sunni Islamist extremism'. ASIO, *ASIO annual report 2018–19*, Australian Government, 2019, 19, online.

15 For example, ASIO acknowledges that the threat from the extreme right-wing in Australia has 'increased in recent years' (ASIO, *ASIO annual report 2018–19*, 20), whereas the US Government describes white supremacist violent extremism as 'one of the most potent forces driving domestic terrorism' (Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence*, US Government, 2019, 10, online). The UK Government recognises extreme right-wing terrorism as 'a growing threat' (HM Government, *CONTEST: the United Kingdom's strategy for countering terrorism*, June 2018, 8, online), and Canada recognises that the threat of violent extremism 'is constantly changing' and that 'some individuals within the far-right movement have espoused, glorified, promoted, and even engaged in violence' (Canada Centre for Community Engagement and Prevention of Violence, *National Strategy on Countering Violent Radicalization to Violence*, Canadian Government, 2018, 1, online).

16 Department of Security Studies and Criminology (DSSC), *Mapping networks and narratives of online right-wing extremists in New South Wales* (version 1.0.1), Macquarie University, 9 October 2020, online.

17 '[T]he Overton Window can both shift and expand, either increasing or shrinking the number of ideas politicians can support without unduly risking their electoral support'; Nathan J Russell, *An introduction to the Overton window of political possibilities*, Mackinac Center for Public Policy, 4 January 2006, online. The research also noted that issues for future consideration included building awareness about the civic underpinnings of representative liberal democracy and the threat of right-wing extremism, and expanding the current CVE infrastructure provided by the NSW Government to those vulnerable to this kind of extremism. The researchers noted that local government was well placed to deliver programs in some communities. See DSSC, *Mapping networks and narratives of online right-wing extremists in New South Wales*.

18 The evaluation of NSW's CVE Program demonstrated that the program achieved significant reach—nearly 1.5 million people in NSW were affected, including through engagement with communities, service providers, 130 schools, government and local councils. Acil Allen Consulting, *NSW Countering Violent Extremism Program evaluation*.

19 Acil Allen Consulting, *NSW Countering Violent Extremism Program evaluation*.

20 The tool includes examples of relevant, valid and rigorous CVE indicators and data collection methods that can be tailored and adapted to support project-level evaluations in government and non-government programs. It contains CVE evaluations from Australian and international jurisdictions and allows users to review examples of various approaches to CVE program evaluation. See Adrian Cherney, Jennifer Bell, Ellen Leslie, Lorraine Cherney, Lorraine Mazerolle, 'Countering violent extremism evaluation indicator document', *National Countering Violent Extremism Evaluation Framework and Guide*, Australian and New Zealand Counter-Terrorism Committee, 2018, online.

The new far right: construction of hatred against the Islamic community in multicultural Australia

ANGEL ADAMS

PhD candidate focusing on online and offline extremism
in Australia at Deakin University

Melbourne, Australia

The construction of a Western identity and power relations during the colonial period still permeate some Australian public discourses, creating a challenge to social cohesion in the country. Western narratives of a fear of the 'other(s)' bring disengagement to a multicultural society and can potentially lead to a more unstable environment in which hatred, exclusion and violence are legitimised and deemed necessary to combat what's perceived to be a national threat. The inflation of counterterrorism policies after 9/11 throughout Western countries contributed to an increase of fear of the 'other' and the racialisation of Muslims, leading to a significant increase in Islamophobia.[1] The fear of Islamist terrorism inspired a global 'moral panic' that fostered division and suspicion against Islam and Muslims in Western societies, fuelling narratives of exclusion by the far right. For instance, the 'Great Replacement Theory', which was adopted by Christchurch's terrorist attacker and holds Muslim migrants to be an existential threat to Western countries, led to the killing of 51 Muslim worshippers in 2019, according to the report of the New Zealand royal commission that investigated the attack.[2]

Although a majority of Australians perceive multiculturalism as positive for the country, negative feelings towards the Islamic community have increased within the past year,[3] which correlates with exclusionary discourses and their current expansion through social and mainstream media. The dissemination of extreme far-right public narratives by mainstream sources can legitimise the exclusion of minority groups depicted as outsiders, increase the risk of a perpetual cycle of radicalisation[4] and weaken democratic mechanisms and institutions. Thus, the current and persistent spread of far-right extremist groups in Australia highlights the importance of addressing, preventing and combating historical constructions of racism and exclusion embedded within liberal democracies and multicultural Western countries. Australia should focus strongly on supressing racially and ethnically motivated violent extremism and invest in research to understand the dynamics, trends, tactics and international connections of transnational nationalist and xenophobic groups, especially white supremacists, in order to prevent Christchurch-inspired attacks and the spread of hatred.

Legitimising a far-right narrative

From the late 1900s onwards, 'whiteness studies' and discussions became prominent in the US and the UK. Initially, debates focused on differences and relations with the 'other' and how blacks could merge into 'better selves'.

Race discussions occurred, but the concept of whiteness became prominent in global politics and centred the white-Anglo community as the dominant race.[5] The white race was described as homogenous, privileged and superior. That originated from the desire to dominate and impose white-centred norms over 'other' non-white individuals. Through colonisation and racialisation, the concept of the 'other' took on a global dimension.[6] During the colonialist era, ideologies, institutions and practices were focused on establishing the white empire, which created an asymmetrical relationship with the 'other' and deeply unfair power structures. Most importantly, the global context at that time in history was one of conflict against those being colonised and, above all, coloured people. Thus, 'whiteness studies' sought to intensify a global narrative of power relations between the white dominant and the coloured colonised, leading to a perception of a new white era and justifying the colonisation of 'inferior' races.

Additionally, racial identification of nations enabled geopolitical alliances based on national race identities, demonstrating the transnational character of the social construction of whiteness. For instance, when Theodore Roosevelt dispatched the US's Great White Fleet around the world, the flotilla visited Australia in 1908, where Rear Admiral Sperry greeted Australians as a 'white man to white men'.[7] Australia had assimilated the Western transnational features of ally nations, which were constituted as an Anglo and white identity.[8]

Nevertheless, the Australian 'imagined community'[9]—a nation imagined and socially constructed by people who perceive themselves as part of the same community—developed a unique set of characteristics that would distinguish Australians from people of other white-Anglo nations. The Australian sovereign state was socially constructed based on an ethnic nationalist identity, in which shared culture and ethnic origins would unite individuals.[10]

Nationalist discourses have been demonstrated, throughout history, to be centred on the exclusion of people who don't share the same national identity. Some researchers suggest that the best option for Australia would lie in a more inclusive type of nationalism,[11] in which policies and education would focus on social inclusion and institutions would embrace diversity, in order to constitute a more united multicultural nation.

An inclusive and diverse national identity could increase feelings of belonging and solidarity among citizens. Nevertheless, for Australia to truly embrace multiculturalism, it needs to accept new creations of its own national identity and to contest old ideologies that could potentially harm its diversity.[12] Australia's national identity should always seek to look towards the future in order to open itself to new social constructions of identity, which would ultimately increase feelings of belonging.

The end of the White Australia policy in the early 1970s, and the implementation of an integration policy based on multiculturalism, demonstrated a national interest aimed at increasing social justice and equal rights in a highly diverse nation. It also demonstrated a positive change towards immigration and minorities within the country.

Australia's contemporary public discourses and increasing number of new far-right (NFR) movements are stoked by global or local social, political and economic events. For instance, NFR groups have increased their online and offline activism amid concerns over globalisation, immigration and terrorism, taking a more anti-Muslim and 'patriotic' approach since the mid-2010s.

In 2016, the populist One Nation party won four seats in the Australian Senate with a political campaign focused on anti-Islam and anti-immigration. Contemporary politicians with far-right perspectives focus on the negative aspects of immigration, driving public and political opinions to justify the use of oppressive and exclusionary policies as a right of the state in order to preserve Australians' security, culture and values,[13] which helps to legitimise NFR groups in the Australian public sphere. Therefore, it's possible to identify some contemporary conservative public figures and NFR groups' discourses exploring a politics of fear, due to an exaggerated concern of replacement by the 'other' identified in Australia's ethnocentric inception. Importantly, though, Australia currently faces a less advanced far-right threat in numbers and virulence compared to other nations, such as the US and Germany. The prevalence of NFR groups appears to be driven by a global phenomenon of grievance and anxiety in various 'nationalist' and populist groups.

Identity politics in the West

The modern Australian national identity was built on a transnational white-Anglo character, providing the basis for today's far-right groups to develop a narrative of exclusion against Islam and Muslims (the 'other'). Those groups' white supremacism has influenced current racial tensions, which are rooted in the foundation of the nation-state on ethnic-nationalist ideas. The continuous presence of the far right on the fringes of Australian politics is buttressed by Australia's history of whiteness, having as a dominant characteristic the exclusion of the 'other'[14] that's embedded in an emotional connection to an idealised past and anxieties about the changing social order.

Political discourses rooted in a history of pronounced ethnic-nationalist identity can be an obstacle to inclusiveness and equality within liberal democratic and multicultural countries. They can affect a country's policies, leading to the passing of exclusionary legislation and the maintenance of a system of exclusion and racism against Indigenous people, minorities and immigrants in opposition to the 'true' nationals.

Australian NFR movements are rooted in a belief in white supremacy. They fear failing their Anglo-Saxon identity[15] and seek to protect traditional and conservative Western values in lieu of multiculturalism, globalisation, or both. Most NFR groups can be defined as sociopolitical movements with multiple far-right features and agendas that depend on the country's political landscape and current concerns about national threats. Hence, it's essential to understand the local context in order to identify those groups' volatile agendas and construction of narratives.

NFR groups have been demonstrated to be fundamentally anti-Muslim or anti-Islam and to project some form of cultural and racial superiority.[16] They deem certain peoples to pose a cultural, security, racial and ethnic threat to the nation,[17] which is a sentiment that's at the core of the strong vigilante aspect inherent in NFR groups' activism.

After the 9/11 terrorist attacks, a sociopolitical context of increased 'moral panic' and extensive media coverage heightened anti-Muslim sentiment.[18] That was evidenced by the appearance and growth of a range of NFR groups using anti-Islam and anti-Muslim rhetoric in Western countries.[19] In Australia, they have included the Patriot Defence League Australia, Aussie Angels Against Sharia, Stop the Mosque, Reclaim Australia, the political party Australian Liberty Alliance, the United Patriots Front, Antipodean Resistance, Nationalist Alternative Australia, the True Blue Crew and the Soldiers of Odin. Some of the NFR groups have assumed a perspective different from that of old-school fascists or neo-Nazi groups.[20] For example, some groups have demonstrated a level of acceptance for immigration if immigrants assimilate and accept Australia's 'true' national identity.[21]

However, studies have shown that most NFR groups have a shared belief that the Islamic community 'contaminates the nation's pristine cultural environment',[22] employing a narrative of hatred and vilification of Muslims and Islam, justified on the ideological arguments explained above. That bigotry and hatred intentionally harm inclusiveness and damage the human dignity of the Islamic community. As a result, the Australian Islamic community has been subject to hatred at a disproportionately higher rate than other minority groups, especially online.[23]

NFR groups usually appropriate populist discourse by highlighting what in their eyes is the best approach to combat what they perceive to be injustices in the public realm, and which is supported by the centuries of white history and exclusion that affirms their version of the history of Australia. Additionally, NFR groups perceive themselves as being engaged in a 'war', adopting approaches that exceed normative democratic practices and can culminate in violent extremism.

For instance, uncontrolled hatred and the white supremacist beliefs of one man resulted in the mass killing of 51 Muslims in Christchurch.

Conclusion

Australia, being one of the world's most multicultural countries, needs to continue to address, prevent and contain historical structural racism embedded in institutions and directed not only against the Islamic community but also against other minorities. That's necessary in order to increase feelings of belonging and sociopolitical justice, which would reduce the risks of political violence and radicalisation. Australia should seek a contemporary national identity that's consonant with its demographics in order to increase social cohesion. It should constantly seek to prevent hatred and violence and protect democracy.

A broad range of people from the national to local levels need the resources to directly integrate security work with social cohesion strategies. For instance, police could receive broader training to identify hate crimes' motivation and be supported to collect information into a national database, providing valuable information to different agencies and Australian researchers. Teachers also play a crucial role in promoting democratic values and practices and developing pedagogical strategies to further engage students in questioning the use of violence as a means of change. It's also important that policymakers understand the context, complexities and implications of discriminatory policies and mitigate the risks of possible counter-reactions when creating new policies.

Additionally, while giving voice to political dissent is an integral part of a democracy, allowing groups to promote fear, hate, racism and exclusion can eventually lead to irreparable wounds in the country's history, raising the risk of a backlash against democratic processes. If we don't address these issues appropriately, groups with exclusionary identities can become the norm, along with radicalisation, leading to a perpetual cycle of instability in the country.[24] Above all, Australians' pursuit of change needs to be achieved through inclusive democracy and governance and never through violence.

Notes

1 Ihsan Yilmaz, 'The nature of Islamophobia: some key features', in Douglas Pratt, Rachel Woodlock (eds), *Fear of Muslims? Boundaries of religious freedom: regulating religion in diverse societies*, Springer, Cham.

2 Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques on 15 March 2019, *Report*, online.

3 The Scanlon Foundation has found a consistently high level of endorsement of multiculturalism up to 2018, ranging from 83% to 86%. Australians have been consistent in perceiving 'multiculturalism as being good for Australia'. In 2019, there was a decrease in the level of acceptance of multiculturalism. The decrease appears to correlate with an increase in negative feelings towards Muslims and Islamic communities. In 2019, interviewer-administered surveys showed that 21%–25% of people expressed negative feelings towards Muslims. In the self-completion version of the survey, in which people tended to be more open and transparent, the rate was much higher at 39%–41%. In 2019, 85% of Australians perceived 'multiculturalism' as being suitable for the country. Andrew Markus, *Mapping social cohesion: the Scanlon Foundation surveys*, Scanlon Foundation Research Institute, 2019, online.

4 Tahir Abbas, *Islamophobia and radicalisation: a vicious cycle*, Oxford University Press, 2019.

5 Marilyn Lake, Henry Reynolds, *Drawing the global colour line: white men's countries and the question of racial equality*, Melbourne University Publishing, 2008, 1.

6 Georgia Shiells, 'Immigration history and whiteness studies: American and Australian approaches compared', *History Compass*, 2010, 790–804.

7 Lake & Reynolds, *Drawing the global colour line*, 3.

8 Leigh Boucher, 'Trans/national history and disciplinary amnesia: historicising white Australia at two *fins de siècles*', in Jane Carey, Claire McLisky (eds), *Creating white Australia*, Sydney University Press, 2009, 47.

9 An allusion to Benedict Anderson's concept of imagined community. Anderson depicts a nation as a socially constructed community, imagined by the people who perceive themselves as part of that group.

10 Danielle Every, Martha Augoustinos, 'Constructions of Australia in pro- and anti-asylum seeker political discourse', *Nations and Nationalism*, 8 July 2008, 562–580.

11 Every & Augoustinos, 'Constructions of Australia in pro- and anti-asylum seeker political discourse'.

12 Anthony Moran, 'Multiculturalism as nation-building in Australia: inclusive national identity and the embrace of diversity', *Ethnic and Racial Studies*, 2011, 34(12):2153–2172, doi: 10.1080/01419870.2011.573081.

13 Every & Augoustinos, 'Constructions of Australia in pro- and anti-asylum seeker political discourse'.

14 Boucher, 'Trans/national history and disciplinary amnesia: historicising white Australia at two *fins de siècles*', 44–48.

15 Every & Augoustinos, 'Constructions of Australia in pro- and anti-asylum seeker political discourse'.

16 Mario Peucker, Debra Smith, Muhammad Iqbal, 'Not a monolithic movement: the diverse and shifting messaging of Australia's far-right', in Mario Peucker, Debra Smith (eds), *The far-right in contemporary Australia*, Palgrave Macmillan, 2019.

17 Peucker et al., 'Not a monolithic movement: the diverse and shifting messaging of Australia's far-right'.

18 Hannah Ritchie, 'Does the news reflect what we die from?', *Our World in Data*, 2019, online.

19 Mario Peucker, Debra Smith, 'Far-right movements in contemporary Australia: an introduction', 1, doi: 10.1007/978-981-13-8351-9_1.

20 Peucker & Smith, 'Far-right movements in contemporary Australia: an introduction', 6–7.

21 Jade Hutchinson, 'The new-far-right movement in Australia', *Terrorism and Political Violence*, 15 July 2019, 1–23, doi: 10.1080/09546553.2019.1629909.

22 Peucker & Smith, 'Far-right movements in contemporary Australia: an introduction'.

23 Derya Iner, Iman Zayied, Matteo Vergani, 'Analysis of Islamophobia Register Australia data 2014–2015', in Derya Iner (ed.), Islamophobia in Australia 2014–2016, Charles Sturt University and ISRA, 2017, online.

24 Abbas, *Islamophobia and radicalisation: a vicious cycle*.

Young people and violent extremism in the Covid-19 context

PETA LOWE
Principal Consultant, Phronesis Consulting and Training
Newcastle, Australia

Young people's vulnerability to and involvement in violent extremism has been exacerbated by the global Covid-19 pandemic. Increasing experiences of social isolation, more time spent online as a result of lockdowns and school closures, growing expressions of anti-government sentiments and increasing unemployment, poverty and social inequality have all exacerbated pre-existing vulnerabilities that young people have to extremist narratives. Now, more than ever, prevention and diversion efforts are needed to identify and address the contributing push and pull factors at both the individual and community levels.

Young people and violent extremism in the current context

In a year that's been marked by uncertainty, fear and unprecedented social restrictions, it's understandable that governments, civil society and private organisations have focused their efforts and resources towards other risks and needs. But, as has been pointed out by many experts in countering violent extremism and terrorism, all levels of society need to come together to develop and deliver new and focused attention to the global prevention and countering of violent extremism, particularly to the engagement of young people in the responses.[1]

Many extremist groups—including right-wing groups from neo-Nazis and fascists, such as the Atomwaffen Division[2] and Wotansvolk,[3] to QAnon; left-wing groups, including anti-fascists and eco-terrorists, such as Global Rebellion;[4] and Islamist extremist groups, such as ISIS and al-Qaeda have been exploiting current political and social contexts, taking advantage of moderate protests or movements to spread their extremist narratives, expand their support base and recruit new members by feeding uncertainty and amplifying anti-government rhetoric and concerns.[5] Some have weaponised Covid-19, encouraging followers to spread the virus intentionally.[6] Others have hijacked anti-lockdown protests in an attempt to shape anti-government narratives and have used internet and social media platforms to spread their propaganda and recruit members. The spread of disinformation, conspiracy theories and propaganda has the potential to damage young people significantly, particularly those already marginalised, as they've been spending more time in online environments and less time in social, recreational, educational or community settings. UK Counter Terrorism Policing calls the current environment a 'perfect storm, one which we cannot predict and that we might be dealing the effects of for many years to come'.[7] In Australia, many peak youth and children's rights bodies are concerned about the impact Covid-19 is having on youth employment, housing, mental health and experiences of social isolation, all of which are factors that can contribute to radicalisation.[8]

Many of the initiatives and resources targeting violent extremism before Covid-19 have been redirected to much-needed health and social responses to the pandemic. While the medical and economic responses have supported many through the health and financial impacts of Covid-19, addressing broader radicalisation push factors such as poverty and socio-economic inequality and increased funding and resourcing for general mental health initiatives and responses have provided generic prevention interventions addressing some radicalisation pull factors or personal factors, specific diversion or detection resources have been redirected.[9] That redirection, together with the need to cease many existing preventive and diversionary initiatives or redesign them for virtual service delivery, has left vulnerable and at-risk youth without those protective interventions.

There have been many experiences of increased connection and engagement within family relationships and local communities in response to the social restrictions. The lockdowns have provided valuable time and opportunity for families to reconnect, spend time together and engage with each other without the pressures or interruptions of pre-Covid daily life. The refocusing has also had positive impacts on communities; there have been many stories of grassroots, community-driven initiatives to support people within the community remaining socially distanced but connected and increased feelings of community belonging.[10] However, while we've seen some positive impacts from Covid-19 restrictions, we've also seen many of the negative impacts: data reveals skyrocketing domestic violence rates, increased conflict and use of violence and aggression, and unprecedented demand for mental health support and services.[11]

Many young people, in particular, have been negatively affected by lockdowns and social restrictions, resulting in an absence of engagement with their usual support systems and networks of people who are outside their immediate family: peers, coaches, youth workers and teachers, who are also well placed to observe and respond to changes in a young person. That lack of engagement in support networks outside the family unit makes young people who are already feeling marginalised, or searching for identity and belonging, even more vulnerable to the messages from extremist groups seeking to provide connection and answers as to why they're feeling that way, feeding any existing grievance or frustration. Increasing concerns from children and young people about mental health, social isolation and negative impacts on family were reported during a study, co-authored by the Australian Human Rights Commission, into the impacts of Covid-19 on children and young people who contact Kids Helpline.[12] The report reflects a broad societal challenge with respect to children and young people, their mental health and their perceptions of isolation and disconnection from their communities and regular social networks in an environment contributing to potential push and pull factors for young people turning to violent extremism. Additionally, this environment reduces early opportunities for people who are well placed to observe and respond to changes in a young person's behaviour. It's often people outside the family household who notice and can respond to the early changes observable when young people become vulnerable to, or are in the process of, radicalising to violent extremism. In July 2020, the Australian Federal Police (AFP) warned that the risk of children and young people being influenced by Islamic State and right-wing extremism was increasing and supported a bill for proposed new laws that would enable the AFP and ASIO to question children as young as 14 if they're suspected of planning a politically motivated attack.[13] The AFP stated that it held growing concerns about the increased likelihood over the past six years of young people being involved in terrorist attacks, citing an increase in children and young people in Australia being targeted by overseas right-wing extremist groups. The proposed legislation and the assessment it's based on predate the effects of the pandemic on young people, which are likely to have increased those challenges. Similarly, I wrote last year about the complex factors that contribute to young people being significantly more vulnerable to influence and radicalisation to violent extremism than adults, and those factors continue to be influential—increasingly so in the current Covid-19 context.[14]

Additionally, ASIO reported to a parliamentary inquiry in September 2020 that far-right violent extremism makes up about 40% of its current counterterrorism caseload (an increase of about 15% since 2016), calling it a 'real and growing' threat.[15] And, while right-wing extremism has long been considered a real threat by those working in frontline contexts, the Christchurch attacks in 2019 heightened media and public awareness about this issue. Right-wing extremism in Australia has been called a 'creeping threat' in a recent study by Macquarie University into how right-wing extremists are using social media and online networks to further recruitment and spread propaganda and extremist narratives.[16] The study highlights how the narratives and messages of right-wing extremist groups are finding their way into political and social norms, mainstream media, social media and online platforms, particularly those frequently used by young people.

Countering and preventing violent extremism with young people

There's much focus internationally on the best practices for preventing and countering violent extremism with young people. Most efforts focus on addressing push factors and macro drivers (such as poverty, limited educational and employment opportunities and persecution or injustice) and pull factors (such as perceptions of group belonging, the influence of peers or significant leaders and the search for status and identity).

A number of recent studies in Australia have sought to highlight the specific factors contributing to youth radicalisation to violent extremism, as well as exploring the factors contributing to youth resilience to violent extremism, in order to inform best practice principles for preventing and countering specifically within the Australian context. A study into the development and validation of the Building Resilience Against Violent Extremism (BRAVE) measure for youth resilience to violent extremism found that there are five main factors that contribute to resilience:

- cultural identity and connectedness—the young person's familiarity with their own culture and their belief that their culture is accepted by the wider community
- bridging capital—having trust in and connection to others outside their own group
- linking capital—having trust in and the ability to connect to government and government organisations
- violence-related behaviours—a willingness to speak out against violence-related behaviours
- violence-related beliefs—the degree to which violence has been normalised or is seen to contribute to status and respect.[17]

While the study was based on 18–35-year-old participants, the findings reflect what are accepted as the factors that are most significant for adolescents in terms of risk, and therefore opportunity, to build resilience to violent extremism. Most importantly, it highlights the areas of risk that have been contributed to and exacerbated by the Covid-19 context, particularly having trust in the government and connection to those outside one's own group, both of which have been targeted, particularly by right-wing extremists. While the Australian state, territory and federal governments' active and successful management of the pandemic is likely to have revived broader trust in government in Australia, right-wing extremist narratives seek to portray government actions as evidence of agendas to restrict citizens' freedoms or to target particular groups and can add to the 'evidence' for those already seeking to find an answer or cause.

Another Australian study conducted by the University of Queensland reviewed open-source information about young people who had committed or been convicted of terrorism-related offences. It highlighted the need to focus on the following contributing risk factors:

- social dislocation (including educational disengagement)
- active engagement with online social media
- exposure to other radicalised networks and associates
- personal grievances and, in particular, triggering events.[18]

Despite the limitations of the study (a small sample size and the uncertain reliability of open-source information), it highlights important risk factors to be addressed in prevention and diversion interventions and adds to the existing literature underpinning the development of intervention programs and services. Of most significance, particularly in the current context, is the risk associated with social dislocation, including educational disengagement. For many young people who were already struggling to remain engaged in education before the lockdowns, this additional time away from educational settings may have only disengaged them further. Other than the pandemic, suspensions or expulsions from school also contribute to social isolation, educational and community disengagement and increased time spent online.

These studies reinforce the importance of the early identification of and intervention with young people at risk of radicalisation. They highlight the additional risks and concerns about social isolation and online social media engagement making some young people open to ideas about governments being less trustworthy because of their pandemic response actions, but also the reduced opportunity for those engaged with a young person to identify and respond to early changes in behaviour that could indicate risk or vulnerability to radicalisation to violent extremism.

Recommendations

While Covid-19 has highlighted the risk of and exacerbated concerns about young people's involvement in violent extremism, and particularly the increase in their engagement with right-wing extremism, it has also provided opportunities for the development and delivery of prevention and diversion interventions to respond to those risks and vulnerabilities. There are a number of areas for government policy and investment to focus on, including the following actions:

- *Create and use online platforms and forums as a way of effectively communicating about and countering the spread of false information and conspiracy theories.* This would be best achieved by empowering and resourcing key actors, such as community and youth leaders, to combat hate speech and the spread of false information online.
- *Develop online resilience-building initiatives and campaigns specifically designed by and for young people.* Such initiatives should target online spaces where young people connect and spend most of their time. Engaging young people in the development and implementation of such campaigns can increase the relevance of the initiatives for other young people; provide an outlet for them to express and discuss their concerns and hopes; empower them to be agents of change in their communities and society; and magnify peer-to-peer engagement and influence. These initiatives should be co-designed with young people and involve education, training and ongoing support for the young people involved.
- *Partner with current actions and investments in mental health, education, employment and resilience for young people generally across Australia.* This should include existing services, such as Kids Helpline, Youth Action, Headspace and Reach Out, to explore designing into them elements that can also assist in preventing youth radicalisation.
- *Invest in and support local communities, leaders and organisations to build and deliver locally led initiatives to support local vulnerable young people within their own communities.*
- *Develop and deliver awareness and skills development programs that focus on improving young people's media literacy and critical thinking skills.* Such programs should promote and encourage the critical analysis of information and its reliability and build young people's awareness and understanding of online platforms and spaces, such as how social media platforms use algorithms to determine what information is directed to users.

- *Engage young people in the design and development of 'safe spaces', both virtual and physical, where they can ask questions and engage in conversations about topics and issues that confuse or frustrate them.* Such spaces should use trained professionals with a strong understanding of youth and violent extremism, so that they're able to maintain dialogue with vulnerable youth.
- *Develop and deliver education and awareness sessions for young people about the process and indicators of radicalisation.* The sessions would help them to develop knowledge and skills to identify when/whether they or their peers and friends are being targeted by extremist narratives or recruiters. At the early stages of radicalisation, being able to identify seemingly small changes can have a big impact on successful diversion interventions.
- *Develop and deliver education and awareness sessions for professionals, frontline workers and volunteers engaged in youth service delivery and community organisations.* The aim should be to build their awareness and understanding of the indicators of radicalisation and opportunities for diversion for young people.

Notes

1 Eric Rosand, Khalid Koser, Lilla Schumicky-Logan, *Preventing violent extremism during and after the COVID-19 pandemic*, Brookings Institution, Washington DC, 28 April 2020, online.

2 'Atomwaffen Division', Southern Poverty Law Center (SPLC), Montgomery, Alabama, no date, online.

3 'David Lane', SPLC, no date, online; Jane Coaston, 'The New Zealand shooter's manifesto shows how white nationalist rhetoric spreads', *Vox*, 18 March 2018, online.

4 *Global Rebellion*, online.

5 UN Interregional Crime and Justice Research Institute, *Stop the virus of disinformation: the risk of malicious use of social media during COVID-19 and the technology options to fight it*, November 2020, online; Anna Patty, 'Extreme right groups exploiting virus fear and tension', *Sydney Morning Herald*, 24 March 2020, online.

6 Debbie White, 'Terrorists could use "coronavirus spreaders" in new jihadi attacks, Russian intelligence reportedly claims', *The Sun*, 30 June 2020, online; Jeff Charles, 'Threat of domestic terrorism arises amid COVID-19 pandemic', *Red State*, 19 August 2020, online.

7 Michael Steward, 'Impact of COVID-19 is creating "perfect storm" for radicalisation risk, terrorism police warn', *East Anglian Daily Times*, 20 November 2020, online.

8 Australian Human Rights Commission (AHRC), *Impacts of COVID-19 on children and young people who contact Kids Helpline (2020)*, 15 September 2020, online.

9 Counter-Terrorism Committee Executive Directorate, *The Impact of COVID-19 Pandemic on terrorism, counter-terrorism and countering violent extremism*, UN Security Council, June 2020, online.

10 'People are putting bears in their front windows to bring children joy', *SBS*, 8 April 2020, online.

11 Else Kennedy, 'The worst year: domestic violence soars in Australia during COVID-19', *The Guardian*, 1 December 2020, online; 'COVID-19 information for workplaces', Safe Work Australia, 29 April 2020, online; Liam Mannix, 'Here comes the COVID-19 mental health surge', *Sydney Morning Herald*, 14 June 2020, online.

12 AHRC, *Impacts of COVID-19 on children and young people who contact Kids Helpline (2020)*.

13 Anthony Galloway, '"Emerging issue": AFP warns children being influences by right-wing extremism', *Sydney Morning Herald*, 9 July 2020, online.

14 Peta Lowe, 'Youth and violent extremism', in Isaac Kfir, John Coyne (eds), *Counterterrorism yearbook 2020*, ASPI, Canberra, online.

15 Paul Karp, 'ASIO reveals up to 40% of its counter-terrorism cases involve far-right violent extremism', *The Guardian*, 22 September 2020, online.

16 Department of Security Studies and Criminology, *Mapping networks and narratives of online right wing extremists in New South Wales*, Macquarie University, Sydney, 2020.

17 Michele Grossman, Kristin Hadfield, Philip Jefferies, Vivian Gerrand, Michael Ungar, 'Youth resilience to violent extremism: development and validation of the BRAVE measure', *Terrorism and Political Violence*, 30 January 2020, online.

18 Adrian Cherney, Emma Belton, Siti Amirah Binte Norham, Jack Milts, 'Understanding youth radicalisation: an analysis of Australian data', *Behavioral Sciences of Terrorism and Political Aggression*, 15 September 2020, online.

The impact of natural disasters on violent extremism

LYDIA KHALIL

Research Fellow, Lowy Institute and Alfred Deakin Institute, Deakin University and member of the Centre for Resilient and Inclusive Societies (CRIS)

Melbourne, Australia

According to the UN Office for Disaster Risk Reduction and the Centre for Research on the Epidemiology of Disasters, major natural disasters such as floods, droughts and heatwaves have doubled in the past 20 years, and we should expect more of the same in the coming decades.[1] The coronavirus pandemic that swept through 2020 was a long anticipated global pandemic that resulted in necessary yet unprecedented restrictions that have frayed the social fabric and will have long-lasting societal impacts. The concurrent crises of 2020, which turned the year into a personal and collective *annus horribilis* across continents, clarified that the multilayered political, economic and environmental effects of natural disasters[2] aren't limited to the developing or conflict-prone parts of our world, but will also affect high-GDP economies and established democracies that are facing substantial challenges, such as inequality, the erosion of the acceptance of evidence-based knowledge and democratic backsliding. We're all now living in a more uncertain and insecure world that will be affected by complex emergencies and natural disasters into the future.

Alongside evidence that natural disasters are on the rise, there's been an equally unprecedented spread of misinformation, disinformation and contestation about the causes and origins of those crises.[3] In the current information environment, it has become increasingly difficult for governments and other authoritative sources to provide accurate messaging that cuts through.

Multiple emergencies and crises in a post-truth age will not only challenge government's disaster response and recovery efforts, but potentially spur antigovernment sentiment, violent extremism and even low-level civil conflict—something largely unaccounted for in the disaster and emergency management (DEM) plans of advanced economies and democracies.

The rise of the 'infodemic'

The Director-General of the World Health Organization (WHO) has stated that, alongside the Covid pandemic, we're in the midst of an 'infodemic'—the rapid spread of misleading or fabricated information that 'like the virus … is highly contagious and grows exponentially' and complicates response efforts.[4] Disinformation has become so robust that the WHO convened the first-ever 'Infodemiology' conference to define the discipline and establish a community of practice and research.[5]

During the pandemic, some of the disinformation has been generated and spread via coordinated campaigns and bots, but mostly by former US President Trump and conspiracy-theory groups, who were identified as super spreaders of disinformation via social media posts that were then amplified by coverage in the traditional media.[6]

The consequences of the mis- and disinformation crisis go beyond implications for the management of natural disasters, but they're directly relevant. Governments, particularly Western democratic governments, are no longer able to control the flow of information as they could in the pre-internet era, and that will complicate governments' messaging as they address disasters and emergencies. Therefore, the increased occurrence and scale of natural disasters and complex emergencies such as the pandemic, occurring within a contested information environment, will undoubtedly challenge governments' disaster and emergency responses in a number of ways—including by spurring violent extremism.

Natural disasters as a potential push factor towards violent extremism

What drives individuals to commit violence based on their beliefs or radicalises them towards violent extremism is an essential yet still contested question among researchers and counterterrorism practitioners alike. However, we do know that it's often a combination of *pull* factors (personal motivations and drivers) and *push* factors (broader societal, environmental and structural conditions that can be conducive to extremism and violence). Previous research findings have demonstrated that natural disasters such as bushfires, hurricanes, earthquakes and pandemics have the potential to act as push factors.

Much of the study of push factors from natural disasters or resource scarcity has been in developing and conflict-prone regions, rarely in advanced economies and consolidated democracies. Yet what research on natural disasters and the risk of violent civil conflict has been done demonstrates clear links. Studies into the effects of natural disasters on civil conflict demonstrate that disasters can have structural effects that affect the distribution of resources, income and wealth and can provide the motive, incentive and opportunity for violent action. They can also heighten grievances and provide openings for groups with pre-existing grievances to act violently against the state.[7]

Likewise, research on natural disasters and their role in provoking terrorism demonstrates a correlation. In the previous decade, researchers Claude Berrebi and Jordan Ostwald, in their study of 167 countries from 1970 to 2007, found that an increase in deaths from natural disasters resulted in an increase in terrorism-related deaths and attacks in the following two years. They hypothesised that the turmoil caused by emergencies exacerbated vulnerabilities that terrorists then exploited, and that post-disaster instability and political tensions could manifest as terrorism or violent extremism.

More recent research has shown that the increase in terrorism after disasters is not only correlated with but related to the government's *response*; it's the 'portrayal of government responses to a natural disaster that impacts subsequent terrorism rather than the natural disaster itself'.[8] Poor disaster and emergency management, or the perception of it, can act as a push factor by exacerbating existing grievances.

Findings on the effect of natural disasters on terrorism in previous decades also found that the effect was concentrated in countries with low to middle-range GDP and that countries with higher GDP didn't experience increases in terrorism following disasters or emergencies.[9] It was assumed that richer countries had more resources to effect disaster recovery and combat terrorism.

Yet, nowadays, we can no longer assume that high-GDP economies and established democracies with yawning inequality gaps and experiencing democratic backsliding are immune from violence, polarisation and extremism after natural disasters—particularly in the current information environment.

Previous examinations of the issue have focused on the correlations between natural disasters and terrorism and crime or on the effect of government responses in influencing the trajectory of the terrorism risk in the *aftermath*. Yet, in the experience of both the bushfires and the pandemic of 2020, we have seen that the response of extremist actors—particularly far-right actors—isn't exclusively dependent on an objective analysis or assessment of a government's response; nor did extremism emerge exclusively in the aftermath of the crisis.

Instead, we've observed extremist actors not only reacting to the government response but *pre-emptively* undermining it and using disasters as *opportunities* to challenge government legitimacy and spread disinformation and conspiracy theories in order to sow distrust and foment polarisation.

We've seen that extremist movements—particularly right-wing extremist movements in Western democracies—have instrumentalised and exploited recent crises to mobilise and justify and extend their narratives. During the bushfires in Australia, far-right actors pushed narratives through coordinated social media campaigns that maligned minorities and opponents on the left; for example, some posted that the fires were the work of Islamist arsonists or were caused by insufficient backburning due to Greens party or Antifa opposition, while also legitimising the use of violence against those groups.[10] A similar dynamic was in play during the US forest-fire season.

Extremist groups have also latched on to disasters as catalysts for 'accelerationism'—a theory of creative destruction proposing that any point of upheaval is an opportunity to usher in and accelerate the demise of current societal structures and governments and impose new ones.[11] Groups such as the Atomwaffen Division, The Base and the Sonnenkreig Division are all right-wing extremist groups that have promoted accelerationism.[12] The Boogaloo movement in the US has also been a proponent of the same theory—its name is a reference to what its adherents believe to be a future civil war.[13] The adoption of this philosophy by extremist actors is problematic for DEM efforts because it implies that any crisis will be an opportunity for violence and targeting, regardless of the government's emergency response.

Accelerationism also coincides with the history of and tendency towards conspiracism, millennialism[14] and apocalyptic obsessions of the extreme right. Natural disasters can play into those beliefs and mobilise individuals to action.[15]

The extreme right has a long history and association with conspiracy theorising and conspiratorial thinking,[16] and more recent research examining conspiracy beliefs and violent extremist intentions also confirms that 'a conspiracy mentality leads to increased violent extremist intentions.'[17] Extremist actors use conspiracy theories and disinformation about disasters as a delegitimation tool, putting forward the idea that government institutions have no use or value or are the hostile actors, not legitimate authorities that can help, respond or recover.[18]

Furthermore, deliberately spreading disinformation has become a form of attack in and of itself. For example, some right-wing extremist groups encouraged followers to spread disinformation about the coronavirus in order to exacerbate tensions, undermining democracy and government authority and social cohesion.[19]

Conspiracy theories connected to Covid-19 and other natural disasters and intersecting with 5G, QAnon and other conspiracies have already inspired plots and attacks,[20] but they also form part of a longer continuum towards violent extremism through what the late scholar Ehud Sprinzak termed 'transformational delegitimation' brought on by gradual disillusionment with democracy, the state and other institutions of authority.[21]

At other times, extremist narratives have *downplayed* the seriousness of an emergency as part of the delegitimation of government and authority, dismissing the threat of Covid-19 and claiming that it's a hoax or an elite conspiracy. They've also pushed narratives denying that climate change extended and exacerbated the effects of the bushfire season in Australia.[22]

The global pandemic has played into anti-globalisation and nativist attitudes among various extremists. Data extracted from Australian far-right and extremist social media has shown persistent narratives about how globalisation has contributed to the spread of Covid, that multiculturalism is a failure and that the pandemic restrictions are an opportunity to press for more permanent limitations on immigration, and extolling white supremacy.[23]

Extremist actors have also used disasters and emergencies to bolster their existing frameworks and beliefs. White supremacist groups have blamed the multicultural societal model for the pandemic and ethnic diversity for the spread of the virus—calling it the 'diversity flu'. The UN has highlighted a growth in 'Covid-19 related hate speech' targeting certain ethnic groups or foreigners, warning that it could 'trigger social unrest and intergroup violence, possibly enhancing the conditions conducive to conflict and atrocity crimes'.[24]

Indeed, extremist actors have used the crisis to make direct calls to action. Leaked US Department of Homeland Security memos have highlighted that right-wing extremists have called on adherents to purposely spread the virus among minority communities and law enforcement targets.[25] Federal Bureau of Investigation agents killed known right-wing extremist Timothy Wilson in a shootout during a sting operation because Wilson was planning to use a car bomb to blow up a hospital treating a number of Covid-19 patients.[26] American senior public health expert Dr Anthony Fauci has needed extra security because of a number of credible threats against his safety.[27] Extremists have urged followers to use homemade chemical weapons to target essential businesses that serve minority communities.[28]

There have also been anti-elite sentiment and targeting. Extremists have made unfounded claims against elite elements such as Bill Gates, the Gates Foundation and George Soros (claiming that they're using the pandemic to make money by promoting allegedly harmful vaccines[29]), while also undermining experts and institutions such as the UN, the US Centers for Disease Control and Prevention, and others. This anti-establishment, anti-institutional and anti-elite sentiment is encapsulated in the QAnon conspiracy theory, which exploded in reach and adherents during the pandemic.[30]

The evidence of this phenomenon is most prevalent in the US, but similar instances have occurred in Australia and Europe. One man was charged with sending threats to kill Victorian Premier Daniel Andrews over his government's pandemic response.[31] A Europol briefing warns of the growth of right-wing extremism and that:

> COVID-19 could further escalate some of these trends, given the potential economic and social impact of the pandemic worldwide … the propaganda of the various scenes has addressed the COVID pandemic, trying to capitalise from it and reinforce own narratives, propagate misinformation and perceived societal division.[32]

Other conspiracy theories abound, such as the belief that 'COVID-19 is a genetically engineered virus created by world banks to kill off weaker humans.'[33] During the bushfires in Australia, a conspiracy theory, expanded and spread by extremist actors and groups online, proposed that the bushfires were deliberately lit in order to clear land so that the government and the private company behind the proposed high-speed rail project wouldn't have to pay people for their land.[34]

States of emergency, in which democratic governments invoke emergency powers after natural disasters, also play into the narratives of anti-government extremists. What are necessary extensions of government authority and curtailing of individual liberties during an emergency, extremists frame as tools of social control and evidence of authoritarian tendencies, playing into the concern that temporary restrictions will become a permanent feature of life and governance. In the US, for example, there have been (disrupted) plots by anti-government extremists against the Governor of Michigan over coronavirus restrictions.[35] Earlier in the year, one man deliberately derailed a train to target a US Navy hospital ship, claiming that its presence in Los Angeles was part of a government takeover.[36] An expanded 'sovereign citizen' movement fuelled by online conspiracies in Australia has held illegal anti-government protests over restrictions,[37] leading to a number of arrests.[38] Anti lockdown protests fuelled by far right extremist elements and conspiracists and attacks against disease control centres were also prevalent in Europe.[39]

An agenda for future research

When it comes to future natural disasters and emergencies, and disinformation about them, we must recognise that those disasters will play into the hands of extremist actors. Therefore, there are several questions in need of further exploration. Can emergencies and natural disasters be drivers of violent extremism not only in conflict-prone regions but also in high-GDP countries? Do emergencies and natural disasters create new conditions for radicalisation, or exacerbate or intersect with existing conditions and drivers? What existing grievances can be exploited and what new grievances might be created in the wake of an emergency or disaster? Is there evidence that extremist narratives about natural disasters are influencing the mainstream? How should this knowledge be not only incorporated in countering violent extremism (CVE) programs, but proactively accounted for in DEM planning? How can DEM incorporate CVE? What do different experiences, both in government responses to disasters and in the effectiveness, virality and reach of extremist disinformation, in different societies tell us about managing future disaster responses and increasing public trust in government?

The events of 2020 have revealed the urgency of addressing those questions. In dealing with natural disasters, governments have focused primarily on traditional categories of DEM, such as recovery response, public health, disaster planning, border security and economic stimulus. Governments also traditionally put together strategic communications campaigns to project a sense of control and authority and to mitigate the spread of disinformation that commonly emerges during times of crisis.[40] But a key element in disaster response and recovery is maintaining not only the functioning of governments and society but also trust in the government and its systems and the cohesiveness of society.

Natural disasters can intersect with disinformation and not only produce a steady erosion of trust and the delegitimation of government authority that can lead to violent extremism but also produce other harms in the process. If CVE isn't addressed during times of crisis, that will make maintaining and recovering government legitimacy and social cohesion in the long term all the more difficult.[41]

Notes

1 Centre for Research on the Epidemiology of Disasters (CRED), UN Office of Disaster Risk Reduction, *Human cost of natural disasters: an overview of the last 20 years 2000–2019*, 2020, online.

2 Using the CRED definition of natural disasters: R Below, A Wirtz, D Guha-Sapir, *Disaster category classification and peril terminology for operational purposes*, CRED, Brussels, October 2009, online.

3 M Cinelli, W Quattrociocchi, A Galeazzi, CM Valensise, E Brugnoli, AL Schmidt, P Zola, F Zollo, A Scala, 'The COVID-19 social media infodemic', *Scientific Reports*, 2020, 10:16598, online.

4 'Director-General's remarks at the media briefing on 2019 novel coronavirus on 8 February 2020', World Health Organization (WHO), Geneva, 2020, online.

5 '1st WHO Infodemiology Conference', WHO, Geneva, 2020, online.

6 S Ali, 'Combatting against Covid-19 & misinformation: a systematic review', *Human Arenas*, 2020, online; S Evanega, M Lynas, J Adams, K Smolenyak, 'Coronavirus misinformation: quantifying sources and themes in the COVID-19 "infodemic"', *Cision Global Insights*, 2020, online. Evanega et al. found that 'media mentions of US President Donald Trump within the context of COVID-19 misinformation made up by far the largest share of the infodemic.'

7 Philip Nel, Marjolein Righarts, 'Natural disasters and the risk of violent civil conflict', *International Studies Quarterly*, March 2008, 52(1):159–185, online.

8 Daren Fisher, Laura Dugan, 'The importance of governments' response to natural disasters to reduce terrorist risk', *Justice Quarterly*, 15 November 2019, doi: 10.1080/07418825.2019.1685120.

9 Claude Berrebi, Jordan Ostwald, *Earthquakes, hurricanes and terrorism—do natural disasters incite terror?*, RAND Corporation, Santa Monica, September 2011, online.

10 Timothy Graham, 'How extremist messaging co-opts emergency events', *The Interpreter*, 21 December 2020, online.

11 Ashton Kingdon, *The gift of gab: the utilisation of COVID-19 for neo-Nazi recruitment*, Global Network on Extremism & Technology, 7 May 2020, online.

12 Daveed Gartenstein-Ross, Samuel Hodgson, Colin P Clarke, *The growing threat posed by accelerationism and accelerationist groups worldwide*, Foreign Policy Research Institute, 20 April 2020, online.

13 *The Boogaloo: extremist new slang term for coming civil war*, Anti Defamation League, 26 November 2019, online.

14 Millennialism or millenarianism is the belief in that there will be a radical or transformational changes to society after a major cataclysm, destruction or the 'end of days'.

15 Michael Barkun, *Disaster and the millennium*, Yale University Press, 1974.

16 See Seymour Martin Lipset, Earl Raab, *The politics of unreason: right-wing extremism in America, 1790–1970*, Harper & Row, New York, 1970.

17 Bettina Rottweiler, Paul Gill, 'Conspiracy beliefs and violent extremist intentions: the contingent effects of self-efficacy, self-control and law-related morality', *Terrorism and Political Violence*, 20 October 2020, doi: 10.1080/09546553.2020.1803288.

18 For an understanding of conspiracies as a delegitimation tool, see Russell Muirhead, Nancy L Rosenblum, *A lot of people are saying*, Princeton University Press, 2019.

19 Andrew Silke, *COVID-19 and terrorism: assessing the short- and long-term impacts*, Pool Re, 5 May 2020, online.

20 Silke, *COVID-19 and terrorism: assessing the short- and long-term impacts*.

21 Ehud Sprinzak, 'The process of delegitimation: towards a linkage theory of political terrorism', *Terrorism and Political Violence,* 1991, 3(1):50–68.

22 'Why wasn't there more prescribed burning and would it have helped?', *ABC News*, 6 January 2020, online.

23 Author's unpublished dataset.

24 *United Nations guidance note on addressing and countering COVID-19 related hate speech*, UN, 11 May 2020, online.

25 Department of Homeland Security, *White racially motivated violent extremists suggest spreading the coronavirus*, weekly intelligence brief, US Government, 17–21 February 2020, online.

26 Adam Goldman, 'Man suspected of planning attack on Missouri hospital is killed, officials say', *New York Times*, 25 March 2020, online.

27 Dan Diamond, 'Fauci gets security detail after receiving threats', *Politico*, 1 April 2020, online.

28 Lydia Khalil, 'COVID-19 and America's counterterrorism response,' *War on the Rocks*, 1 May 2020, online.

29 'Far-right exploitation of COVID-19', briefing note, Institute for Strategic Dialogue and BBC, 12 May 2020, online.

30 Marc Andre Argentino, 'QAnon conspiracy theories about the coronavirus are a public health threat', *The Conversation*, 9 April 2020, online.

31 Jenny Noyes, Simone Fox Koob, Fergus Hunter, 'NSW man charged with emailing threat to kill Victorian Premier Daniel Andrews', *Sydney Morning Herald,* 11 January 2021, online.

32 Europol, *Written contribution to JPSG reporting on the fight against right wing extremism and terrorism (RWE)*, unclassified briefing, EDOC# 1127986v1, 21 September 2020, online.

33 Erin Pearson, Simone Fox Koob, 'It's better to die on your feet, bailed protest planner told police', *The Age*, 11 September 2020, online.

34 Cameron Wilson, 'I can't believe I have to say this, but the bushfires were not deliberately lit to make way for high-speed rail', *Buzzfeed News,* 11 January 2020, online.

35 Hannah Allam, 'Michigan authorities charge 13 in plot to kidnap Governor Gretchen Whitmer', *NPR*, 9 October 2020, online.

36 Dakin Andone, 'Engineer accused of crashing train said he was "suspicious" of nearby coronavirus relief ship, Justice Department says', *CNN*, 2 April 2020, online.

37 Michael McGowan, 'The threads that don't connect: Covid gives Australian conspiracy theorists a common home', *The Guardian,* 2 August 2020, online.

38 Danny Tran, 'Anti-mask "sovereign citizen" granted bail after allegedly coughing on woman in Melbourne cafe', *ABC News,* 27 August 2020, online.

39 John Henley, 'Latest corona virus lockdown spark protests across Europe,' *The Guardian*, 3 November 2020, online.

40 Joshua Roose, Lydia Khalil, 'Countering extremism and conspiracies in a global pandemic', *ABC Religion and Ethics*, 11 September 2020, online.

41 Anna Patty, 'Disaster planners warn conspiracy theories pose a security threat', *Sydney Morning Herald*, 13 September 2020, online.

The importance of inter-office coordination in counterterrorism: the Israeli case study

PROFESSOR BOAZ GANOR
Ronald S Lauder Chair for Counter-Terrorism at the Interdisciplinary Center, Herzliya and founder and the Executive Director of the International Institute for Counter-Terrorism

Herzliya, Israel

On 5 September 1972, during the 20th Olympic Games in Munich, Germany, eight terrorists who were members of Black September (Fatah's foreign terrorist attack apparatus) broke into the Israeli athletes' quarters, murdered two of them and captured another nine as hostages. Later, during a rescue attempt by German security forces, the terrorists murdered all nine hostages. That attack, having garnered unprecedented media coverage by virtue of the multiple media crews covering the Olympics, is considered by many scholars to be the genesis of modern terrorism. The attack shocked the Israeli public, who demanded an inquiry into the intelligence and security failings that allowed it to happen. The Israeli Government formed an inquiry committee, identifying several coordination faults between Israeli and German security forces. Following the review, then Prime Minister Golda Meir appointed a special adviser on counterterrorism (CT) to the Prime Minister. This chapter highlights the achievements and perspectives of various special advisers on the critical role of inter-office coordination in the Israeli Government to this day, as a way of providing insights on CT for other jurisdictions.

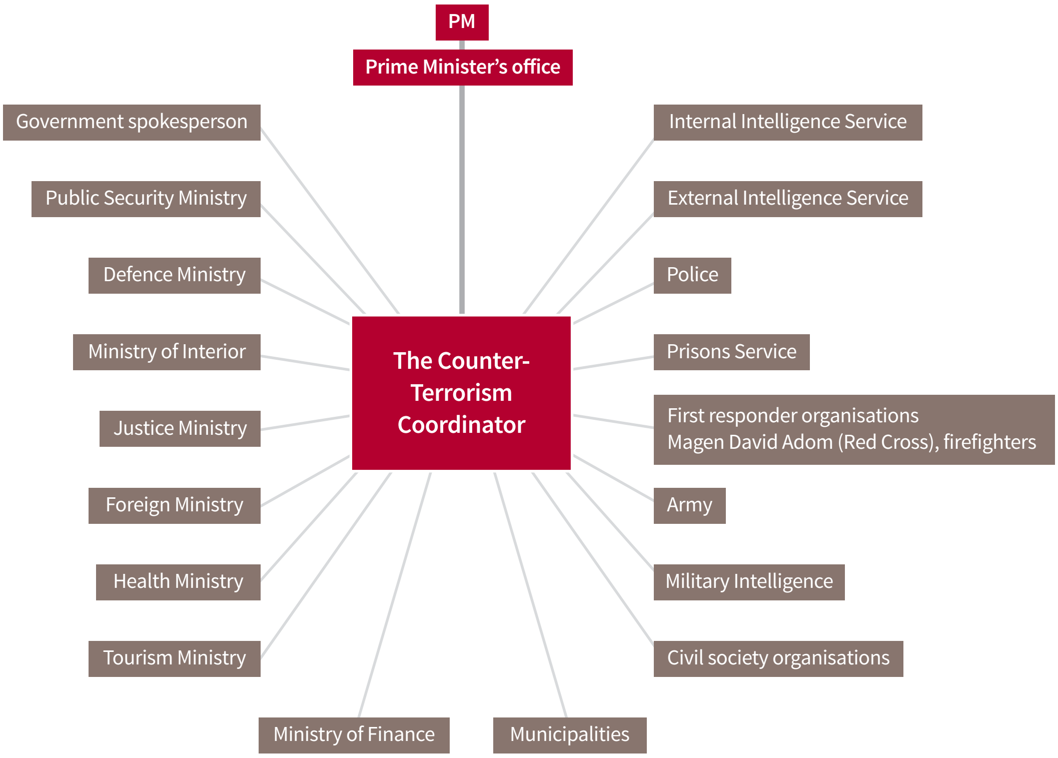
The first special adviser for CT appointed by Prime Minister Meir was the outgoing head of the Intelligence Corps, General Aaron Yariv. Yariv determined that the adviser's job was to advise, coordinate and supervise the build-up and execution of Israel's CT strategy as well as to coordinate the various agencies dealing with the subject matter, including the Israeli Defense Forces, the intelligence community and the Ministry for Foreign Affairs.[1]

The Munich attack brought to light the critical need for internal coordination and international cooperation among intelligence, security and enforcement agencies, government ministries, and many others who deal with CT. Professional reasons, such as the natural inclination of intelligence agencies to protect their sources and treat intelligence as a rare resource that needs to be highly protected and sparingly shared with others, coupled with personal considerations such as ego clashes and rivalries, are indeed the real enemy of an effective CT effort. Thwarting attacks, mitigating attacks' consequences and damages and strengthening the public's resilience all require close cooperation among multiple entities, including:

- intelligence agencies—in Israel, the Military Intelligence Corps, the Israel Security Agency (ISA) and Mossad
- government ministries, such as the ministries of Defense, Interior, Foreign Affairs, Finance, Public Security, Tourism, Education, Justice and so on
- security and law enforcement agencies and first responders (Police, Prisons Service)
- the media, including social media and internet companies
- other relevant elements, such as professional experts and scholars, community leaders, private-sector security and technology companies and non-profit organisations (Figure 9).

Only a consistent and well-coordinated effort among those groups and individuals can lead to an effective campaign against terrorism.

Figure 9: Domestic counterterrorism coordination in Israel


PM
Prime Minister's office
Government spokesperson
Public Security Ministry
Defence Ministry
Ministry of Interior
Justice Ministry
Foreign Ministry
Health Ministry
Tourism Ministry
Ministry of Finance
Municipalities
The Counter-Terrorism Coordinator
Internal Intelligence Service
External Intelligence Service
Police
Prisons Service
First responder organisations
Magen David Adom (Red Cross), firefighters
Army
Military Intelligence
Civil society organisations

Exactly for that reason, Prime Minister Meir decided to form the Counter-Terrorism Coordination Office after the Munich attack. Between 1972 and 1999, all prime ministers appointed advisers for CT. The appointees were usually senior veterans of one of the security apparatuses in Israel and had a close personal, confidant-type relationship with the Prime Minister. This informal personal relationship was of utmost importance in guaranteeing the success of the coordination of Israel's CT efforts. The fact that the adviser had an open door to the Prime Minister's chambers created attentiveness and reception within the various agencies, as they tried to avoid unnecessary conflicts between the adviser and their teams. Meir Dagan, who served as the adviser for CT for Prime Minister Benjamin Netanyahu (1996–1999), explained that the adviser draws their authority from their ability to bring disputes to the government's table for decision-making.[2] Prime Minister Netanyahu explained that, even though the adviser is merely a coordinating body devoid of any real authority, the adviser can 'establish order' by reporting to the Prime Minister.[3] The adviser has managed to resolve many interagency conflicts by reaching out to the Prime Minister for decisions.

Rafi Eitan, who served as the adviser for Prime Minister Menachem Begin between 1978 and 1981, said that attendees at the weekly coordination meeting presented all the intelligence warnings they had and deployed their forces according to their decisions. Eitan stressed that the weekly meeting focused on defensive aspects rather than offensive ones.[4] Yigal Pressler, who served as adviser to Prime Minister Itzhak Rabin between 1992 and 1996, clarified that the bulk of his job was to coordinate security within the state, including between the police, the Israel Defense Forces, civil guards and the population in general, in order to better defend against terror threats. He also stressed that he dealt with reviewing the security of Israeli installations overseas.[5] All the advisers emphasised that their job didn't include responsibilities for coordinating the various intelligence agencies, as they mostly focused on the security–defensive derivative emanating from the intelligence gathered. Meir Dagan added that he mostly dealt with strategic and CT policy issues that required coordination among the various government agencies, such as contending with the terrorist organisations' infrastructure—recruitment, incitement, finance and so on. Dagan said that, during his appointment, there was a critical need to coordinate legislation and enforcement activities among the police, ISA, various ministries and others. Dagan further stressed that the importance of the coordination stemmed from the fact that all those entities came from different branches of government (legislative, executive, judicial) and they all had to act in concert. However, due to the separation of authorities in a democratic regime none was willing to be instructed by the other, so the need for coordination became even more acute, although it was difficult to execute and synchronise.[6]

That said, not all leaders of Israel's various intelligence and security services favoured the adviser's activity. They saw the position as a gatekeeper between them and the Prime Minister regarding CT issues, which didn't sit well with them. Jacob Perry, who served as the head of the ISA, stressed that intelligence and operational entities in Israel cooperated well, so the adviser's position was redundant. His position was that the adviser didn't add anything to CT efforts and, at most, the position served as a landing spot for some of the graduates of Israel's defence apparatus.[7] Shlomo Gazit, the former head of the Intelligence Corps, thought the same.[8] Against that backdrop, Meir Dagan cautioned that the adviser mustn't think that they are senior to the ISA or Mossad. On the contrary, they should support those agencies' CT activity, connect it with other CT activities of other agencies, synchronise all efforts and guide a coordinated strategic policy.[9]

In 1996, following a wave of suicide attacks in Israel, the government formed the Counter Terrorism Bureau (CTB), with a special focus on the prevention of suicide attacks by Hamas and Palestinian Islamic Jihad.[10] At first, the bureau was separate from the CT adviser to the Prime Minister's office. After a few months, Dagan was appointed as both the head of the bureau and the adviser to the Prime Minister on CT. After Dagan was replaced, the position of adviser to the PM on CT was cancelled; however, the CT coordinator maintained his role as head of the bureau. The CTB was subsequently moved from the Prime Minister's office to the National Security Council in 2001. At that point, the weekly coordination meetings ceased.

The ministerial committee for national security issues determined that the National Security Council 'will operate as a designated permanent staff whose job is to create efficiency in the fight against terrorism, by forming recommendations, setting goals and initiating plans of action; maximising capabilities and resources; setting priorities and following up on execution of decisions'.[11] The head of the CTB was appointed by and reported to the Prime Minister. The bureau comprised representatives of the various government ministries and security and defence apparatuses, and all carried out their activities as per their prescribed authority and responsibilities, as the formation of the bureau replaced neither the above entities nor their authorities, division of roles or responsibilities.[12]

In 2001, the ministerial committee for national security issues moved the CTB under the auspices of the National Security Council,[13] and in 2005 it resolved that the bureau would serve as the staff of the Prime Minister as well as the government and its committees on CT issues.[14]

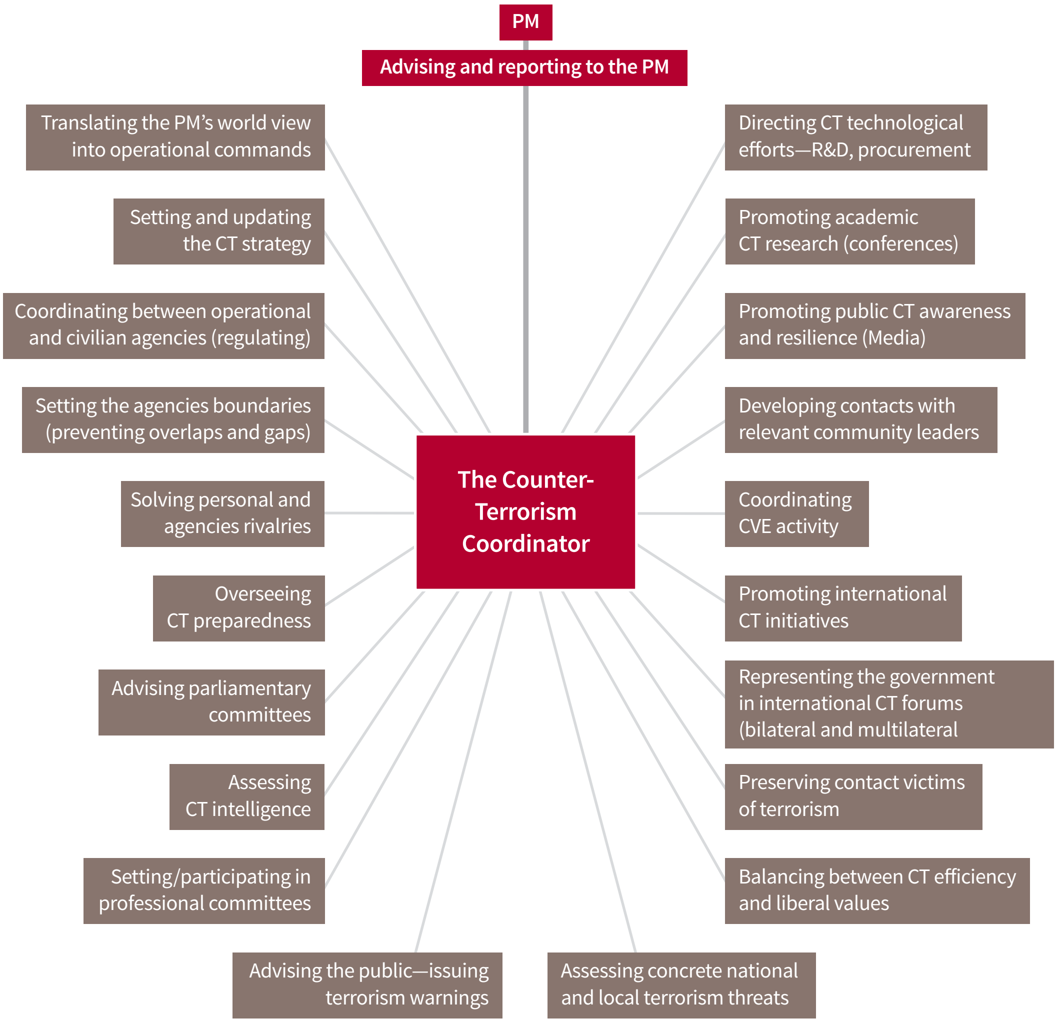
The responsibilities of and issues dealt with by the CTB over the years can be gleaned from the annual reviews published by the Office of the Prime Minister:

- *Policy and core issues:* The CTB formalised strategic principles for the Israeli policy on CT and contending with the Palestinian Authority on terrorism issues, as well as operational concepts to contend with core terrorism issues.
- *Routine security:* The CTB held weekly assessment meetings on terrorism threats and made recommendations on the response to those threats. The unique value of this assessment is that it reflected an integrated threat landscape and incorporated operational responses into that intelligence picture. Additionally, the CTB dealt, *ad hoc*, with unique threats that required an integrative interagency or public–private response.
- *Critical infrastructure security:* This issue was central to CTB activity. The bureau conducted preparatory work on the general principles and policy of infrastructure security and handled multiple security problems that arose over the years. Moreover, it took part in supervising the security regulations in Israel and abroad.
- *Position papers:* The bureau intensively issued position papers on the division of roles and responsibilities, reviewing and improving processes in CT and its derivatives.
- *International cooperation:* The CTB dealt with CT resource allocation and monetary supervision, enlisting the international system to fight terror infrastructure, developing CT dialogues with other countries, reducing potential terror threats by cooperating with other countries and fighting institutions that served as ‘fronts’ for terrorist organisations.
- *Legislative and regulatory:* The bureau acted to promote legislative and regulatory amendments (the Order for Prevention of Terrorism, the Money Laundering Law) to improve the ability to contend with terrorism in general and provide solutions for particular problems. The CTB also led Israel’s contribution to UN activity on international legislation to combat terrorism and terrorist organisations’ infrastructure and support mechanisms.
- *Special responsibilities:* The CTB recommended the transfer of security responsibility for the border crossings between Israel and the Palestinian Authority to the Israeli Airport Authority. Within this framework, the bureau allocated a significant portion of the special US aid to counter terrorism to acquire advanced inspection equipment (for goods and cargo) and the development of a biometric array. The CTB also formalised recommendations to contend with unconventional terrorism as well as cyber terrorism.[15]

In addition, the CTB dealt with aviation, marine and land security.[16] It was in charge of issuing travel warnings to Israeli tourists and businessmen overseas;[17] formalised the security principles for schools,[18] school trips[19] and the protection of critical infrastructure and national strategic installations[20] (including gas rigs[21] and sea ports[22]); examining ‘super terrorism’ threats,[23] setting the division of roles and responsibilities for the protection of public officials;[24] reviewing technologies to protect buses from explosives,[25] the security of the Israeli water supply network[26] and drone threats;[27] securing Israel’s biometric database;[28] and reviewing safety and security aspects of vehicles[29] and the receipt and review of passenger name record information on all flights in and out of Israel or passing through its airspace.[30]

At the end of 2017, the CTB was consolidated with the Internal Security and Home Front division in the National Security Staff (the new name of the National Security Council) and dubbed the Division for Counter Terrorism, Internal Security and Home Front, headed by Brigadier General (Res.) Yigal Slavik. The division’s mandate has been expanded and defined as the staff organ for the Prime Minister, the government and its committees on CT and home-front readiness in emergency situations. The division coordinates the activity of all entities dealing with those matters to continuously improve the national response to various terrorism threats and home-front readiness for emergencies. Its goals are to improve contending with terrorism threats in Israel or abroad, threats of war and emergency situations. The division coordinates and regulates interagency protection for public officials and delegations, marine and aviation security and the improvement of civilian security systems. It also coordinates and regulates terrorism prevention activities on Israel’s international borders (land, air, sea) and the internal border crossings on the ‘security fence’ and Gaza. It acts to promote national preparedness vis-a-vis super terrorism and unconventional terror attacks and dangerous materials. Finally, the division is responsible for promoting international cooperation in the fields of CT and home-front protection.[31]

Figure 10: The role of the Counter-Terrorism Coordinator


PM
Advising and reporting to the PM
The Counter-Terrorism Coordinator
Translating the PM's world view into operational commands
Setting and updating the CT strategy
Coordinating between operational and civilian agencies (regulating)
Setting the agencies boundaries (preventing overlaps and gaps)
Solving personal and agencies rivalries
Overseeing CT preparedness
Advising parliamentary committees
Assessing CT intelligence
Setting/participating in professional committees
Advising the public—issuing terrorism warnings
Assessing concrete national and local terrorism threats
Directing CT technological efforts—R&D, procurement
Promoting academic CT research (conferences)
Promoting public CT awareness and resilience (Media)
Developing contacts with relevant community leaders
Coordinating CVE activity
Promoting international CT initiatives
Representing the government in international CT forums (bilateral and multilateral
Preserving contact victims of terrorism
Balancing between CT efficiency and liberal values

Summary and conclusions

Judging from the Israeli experience in CT, one can determine that the formation of an entity coordinating the intelligence community, law enforcement agencies, government ministries and civilian entities is a required condition to ensure effective CT efforts of the combined state apparatus, prevent terrorism and maximise national capabilities and resources.

To win the trust and cooperation of the myriad agencies and entities, the CT coordinator has to be appointed by and report to the chief decision-maker in the state (in Israel, the Prime Minister) and have direct and constant access to that decision-maker. The role of the coordinator is varied and includes all of the activities outlined in Figure 10, and more.

The coordinator must remember that, even though they speak for the country's most senior leader—the Prime Minister—they are merely an adviser and coordinator and therefore forbidden from taking a role in decision-making as far as CT is concerned. In that sense, the coordinator is not part of the hierarchical chain of command of the country's intelligence and security apparatuses, even though under certain circumstances the coordinator may direct those agencies' activities vis-a-vis the ever-changing terrorism threat. The coordinator must avoid damaging the interactions between the Prime Minister and the heads of the intelligence and security agencies and must also bear in mind that they aren't responsible for gathering and analysing intelligence.

The role is critical in coordinating the diverse and important roles and responsibilities of myriad organisations focused on CT operations, policy and law. It's clearly a major challenge but a necessary one to ensure effective inter-office coordination in government.

Notes

1 Yariv Aharon, 'A strategy to counter Palestinian terrorism', in Merari Ariel (ed.), *On Terrorism and Combating Terrorism: Proceedings of an International Seminar*, Tel-Aviv, 1979, 1; *On terrorism and combating terrorism*, University Publications of America, USA, 1985, 6.

2 Interview with Meir Dagan, 4 December 1998.

3 Interview with Prime Minister Netanyahu, 20 December 1999.

4 Interview with Rafi Eitan, 31 October 1999.

5 Interview with Yigal Pressler, 31 October 1999.

6 Interview with Meir Dagan; B Ganor, *The counter-terrorism puzzle: a guide for decision makers*, Routledge, 2017, 61.

7 Interview with Meir Dagan; Ganor, *The counter-terrorism puzzle: a guide for decision makers*, 60.

8 Shlomo Gazit, 7 November, 1999.

9 Interview with Meir Dagan.

10 *Report on the Office of the Prime Minister*, State Comptroller's Office, 2016, online (in Hebrew).

11 *Israel's State Comptroller Annual Report No# 57B, Report on Israel's Security System,* 2006, online (in Hebrew).

12 *Israel's State Comptroller Annual Report No# 57B, Report on Israel's Security System,* 2006, online (in Hebrew).

13 *Israel's State Comptroller Report on the National Security Council,* September 2006, online (in Hebrew).

14 *Israel's State Comptroller Report on the National Security Council,* September 2006, online (in Hebrew).

15 Yoel Hasson (ed.), *Information on the Office of the Prime Minister's Activity in 2000*, October 2001 (Israel's State Comptroller's reports) (in Hebrew).

16 Public tender for the Prime Minister's Office, 1 March 2020, online (in Hebrew).

17 *Israel's State Comptroller Annual Report No# 54B, Report on Israel's Ministry of Foreign Affairs*, 2003, online (in Hebrew).

18 *Minutes no# 294 of the 13th Knesset Culture and Education Committee,* 1 August, 1995 online (in Hebrew).

19 *Minutes no# 86 of the 14th Knesset Culture and Education Committee,* 24 June, 1997 online (in Hebrew).

20 *Israel's State Comptroller Annual Report No# 54B, Report on Prevention of Events Involving Hazardous Materials,* 2003, online (in Hebrew).

21 Amir Oren, 'The Brussels and Istanbul attacks have proved: the lottery is unnecessary', *Haaretz*, 25 March 2016, online (in Hebrew).

22 'Law for Regulating Security in Public Bodies (Amendment no. 10), 5719–2019', *Open Knesset*, 4 June 2018, online (in Hebrew).

23 Threats that are the next level up compared to current terrorism patterns and have a direct bearing on national security; *Israel's State Comptroller Annual Report No# 57B, Report on Israel's Security System,* 2006, online (in Hebrew).

24 *Israel's State Comptroller Annual Report No# 53A, Report on Israel Security Agency's Security Division,* 2002, online (in Hebrew).

25 Amos Harel, 'The Counter-Terrorism Headquarters is planning protection for buses', *Haaretz*, 22 August 2011, online (in Hebrew).

26 *Government of Israel's Resolution no# 633 Re the Formation of a National Authority for Water Security,* 11 November, 2006, online (in Hebrew).

27 *Israel's State Comptroller Special Report on Israel's Preparedness to Fend Off UAV Threat,* 2017, online (in Hebrew).

28 Information on the trial period for the inclusion of biometric identifiers within identification documents and databases, pursuant to the *Inclusion of Biometric Identifiers Within Identification Documents and Databases – 2009*, published 4 March, 2017, online (in Hebrew).

29 *Government of Israel's Resolution no# 1925 Re GPM Gas Propelled Vehicles,* 6 June, 2002 (updated 29 December, 2019), online (in Hebrew).

30 *Government of Israel's Resolution no# 2258 Re Receipt of Personal Information from Airlines on Passengers Entering, Departing or Passing through Israel,* 30 November, 2014 (updated 18 September, 2017), online (in Hebrew).

31 Israel National Security Council (NSC), 'Lottery Division in TF and Home Front', NSC, no date, online (in Hebrew).

About the authors

LEANNE CLOSE

Leanne Close APM is the former head of the counterterrorism program at ASPI. She is a member of the Victorian Government External Advisory Panel on Countering Violent Extremism and the ACT Sentence Administration Board. Leanne currently works at the Business Council of Australia.

Before joining ASPI, Leanne was a Deputy Commissioner of the Australian Federal Police (AFP), with over 33 years policing and law enforcement experience. As Deputy Commissioner National Security, she was responsible for counterterrorism operations, the protection of VIPs and critical infrastructure, and aviation operations. Leanne was also the AFP representative at the Australia—New Zealand Counter-Terrorism Committee. From 2015 to 2019, she was the Co-Chair of the Asia/Pacific Group on Money Laundering and Counter-Terrorism Financing.

Her qualifications include a Master of Education Leadership from the University of Canberra and two Graduate Certificates in Professional Development Education (University of Canberra) and Applied Management (Australian Institute of Police Management).

THOMAS MORGAN

Thomas Morgan is a Senior Research Fellow at the Institute for Economics and Peace, where he's the chief researcher on the Global Terrorism Index and Global Peace Index. In 2013, he was a visiting researcher at the Oxford Poverty and Human Development Institute at the University of Oxford. He holds a Master of Economics degree from the University of Sydney.

OLIVIA ADAMS

Olivia Adams is a Research Fellow at the Institute for Economics and Peace. Before joining the institute, she worked as a research assistant at the Lowy Institute. She holds a Bachelor of International Relations from King's College London, where she focused on counterterrorism, gender and international security.

DR DAVID HAMMOND

Dr David Hammond is the Research Director at the Institute for Economics and Peace. Before being appointed Research Director, he worked at the institute as a Senior Research Fellow from 2012 to 2018. In 2016 and 2017, he was a visiting Research Fellow at King's College London. He holds a PhD in Operations Research from the University of Portsmouth.

DR JOHN BATTERSBY

Dr John Battersby is a Teaching Fellow at the Centre for Defence and Security Studies, Massey University, Wellington, lecturing in intelligence and counterterrorism. Graduating with a PhD in History in 1995, John was a research historian with the Crown Law Office, advising the Crown on the NZ Wars aspects of Treaty of Waitangi claims. In 2005, he joined the NZ Police and served in frontline roles before joining the School of Leadership, Management and Command at the Royal New Zealand Police College, Porirua. In 2016, John was a Research Fellow at the Centre for Strategic Studies, Victoria University, Wellington, where he commenced research into the impact of terrorism in New Zealand—an interest that has led to a number of publications since. John is also Managing Editor of the *National Security Journal* and a regular commentator on security issues in New Zealand.

CHRISTOPHER WINTER

Christopher Winter is a PhD candidate at Victoria University. His work explores the situational and emotional dimensions of lone-actor terrorist violence though a micro-sociological framework. He is also a member of the Applied Security Science Partnership at Victoria University. He holds a BA in Politics and a Master of Counter-Terrorism Studies from Monash University.

RAMÓN SPAAIJ

Ramón Spaaij is a sociologist based at Victoria University and the University of Amsterdam. He co-leads the Applied Security Science Partnership at Victoria University. His books include *The age of lone wolf terrorism* (Columbia University Press, 2017, with Mark S Hamm) and *Understanding lone wolf terrorism: global patterns, motivation, and prevention* (Springer, 2012).

JEREMY DOUGLAS

Jeremy Douglas is the Regional Representative of the United Nations Office on Drugs and Crime (UNODC) for Southeast Asia and the Pacific, overseeing and managing operations and strategy from Myanmar to the Pacific in the areas of the rule of law, non-traditional security threats, law enforcement, criminal justice and drug-related supply and health issues. He is also the UNODC liaison to China, Korea, Japan and Mongolia and to regional organisations, including ASEAN and the Pacific Islands Forum Secretariat. He has held this role since 2013. Jeremy is a graduate of the London School of Economics in the UK and Bishop's University in Canada.

NIKI ESSE DE LANG

Niki Esse de Lang has worked as Counter-Terrorism Advisor with the United Nations Office on Drugs and Crime (UNODC) for Southeast Asia and the Pacific since November 2017. Before joining UNODC, he completed over three years of service as Evidence Reviewer with the Special Tribunal for Lebanon, Office of the Prosecutor, in Leidschendam, The Netherlands. Previously, Niki also worked with two NGOs on the Thailand–Myanmar border on issues of internal armed conflict and human rights. He earned two Master of Laws degrees from the University of Amsterdam in the Netherlands and specialises in criminal law, international law and human rights law. During his studies, he interned with the Amsterdam Court of Appeals, Criminal Department, a human rights law firm and with the UN Office of the High Commissioner for Human Rights in Bangkok, Thailand. Niki has previously published on issues such as anti-terrorism blacklisting in the EU, national human rights commissions in Southeast Asia and the dire human rights situation of Muslim minorities in Myanmar.

LEVI J WEST

Levi J West is the Director of Terrorism Studies at the Australian Graduate School of Policing and Security at Charles Sturt University (Canberra). He has previously lectured to law enforcement, intelligence and military audiences both domestically and internationally, including at Oxford University, New York University, the Naval War College in the US, the Jakarta Centre for Law Enforcement Cooperation in Indonesia, the National Security College and the Centre for Arab and Islamic Studies at ANU, and at the Australian War College as well as delivering numerous bespoke presentations to various organisations within the national security apparatus.

Levi holds a Bachelor of Arts degree in Politics and International Studies from Southern Cross University; a Master of International Security Studies and a Master of Policing, Intelligence, and Counter Terrorism from Macquarie University; and a Graduate Certificate in National Security Policy from the ANU. He's currently a PhD scholar at Victoria University, Melbourne.

ELISE THOMAS

Elise Thomas is a former researcher with ASPI's International Cyber Policy Centre. She also works as a freelance journalist and an open-source intelligence analyst with the Institute for Strategic Dialogue. Her work covers a range of topics, including disinformation, influence operations, conspiracy theories and online extremism.

DR JOSHUA SINAI

Dr Joshua Sinai is Professor of Practice, Counterterrorism Studies, Capitol Technology University, in Laurel, Maryland. He also serves as Adjunct Faculty, Department of Criminal Justice, Southern New Hampshire University, in Manchester, New Hampshire, where he teaches a graduate-level distance learning course on global terrorism. He also serves as a consultant to TorchStone Global, a national security firm.

DR GORDON HOOK

Dr Gordon Hook is the Executive Secretary of the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force-style regional organisation, based in Sydney. The APG consists of 41 member countries in the Asia–Pacific region and 40 observer countries and organisations. Gordon has conducted 14 mutual evaluations of APG member countries since 2006. Mutual evaluations assess a member country's compliance with the Financial Action Task Force's global standards against money laundering and terrorist financing.

Gordon has degrees in philosophy and law, including a PhD in law from Victoria University of Wellington. He practised private and public law in Canada and in New Zealand prior to his current position and also served in the Royal Canadian Navy and the Royal New Zealand Navy as prosecuting counsel in numerous courts-martial in Canada, Germany and New Zealand.

Gordon is a barrister and solicitor of the Manitoba Queen's Bench (1984) and the High Court of New Zealand (1996).

SYLVIA LAKSMI

Sylvia Laksmi, an Indonesian national, is a renowned subject-matter expert in the field of anti-money-laundering and counter-terrorism-financing. Since 2007, she has worked as a senior financial intelligence analyst in the Indonesian Financial Intelligence Unit in the specialised area of financial crimes intelligence investigations.

Sylvia is currently a PhD candidate at the Australian National University, examining Indonesian counterterrorist financing policies and their impact on terrorist operations in Southeast Asia and the Asia–Pacific. Apart from her research work, she's also an established trainer who has provided training to government officers and private-sector specialists domestically as well as at the international level. In 2016, she was called upon to be a member of the National and Regional Anti-Money Laundering and Counter-Terrorist Financing Team to develop risk assessment projects and a training syllabus.

Her other notable posts include Teaching Fellow of Military and Defence Studies Program for the Australian War College at the Australian National University; Adjunct Lecturer at Charles Sturt University, Canberra; Research Fellow in International and Strategic Studies at the University of Malaya; Visiting Scholar at the International Centre for Political Violence and Terrorism, Singapore; and Senior Researcher at the Centre for Terrorism and Radicalism Studies, Indonesian Police Science College. In 2019, given her considerable depth and credibility, Sylvia was called upon to assist the Philippines Government in a project for Peace Youth Communities to generate counter-narratives against IS-inspired groups and the Communist Party.

She holds a Bachelor of Political Sciences, which included a thesis on the Abu Sayyaf Group, from University Padjadjaran (Indonesia), and an MSc focused on terrorist financing study from the University of Indonesia.

DR JOHN COYNE

Dr John Coyne is Head of Strategic Policing and Law Enforcement and Head of the North and Australia's Security at ASPI. He was the inaugural head of ASPI's Border Security Program and more recently established the North and Australia's Security Program.

John has worked in intelligence and national security for over 25 years. He's been an intelligence professional at tactical, operational and strategic levels across a range of military, regulatory, national security and law enforcement organisations.

Since commencing at ASPI, John has conducted field research on Mexican organised crime; biosecurity; regional coastguards; border security; people smuggling; illicit drugs; corruption and foreign bribery; regional intelligence sharing; and ASEAN economic integration. He has authored numerous research publications and provided expert commentary to media and news outlets.

DARIA IMPIOMBATA

Daria Impiombata is a researcher with ASPI's International Cyber Policy Centre. Her research interests include human rights, grassroots movements and activism in authoritarian regimes, Chinese public and foreign policy and the role of communications and new media in international politics. She also researches broader issues of national security, counterterrorism, organised crime and policing.

She has published reports and articles about censorship and surveillance on Chinese apps, as well as the EU's relations with China, among other things.

Daria has a Bachelor of Chinese Studies from Ca' Foscari University of Venice, Italy, a Master of International Relations and a Master of Journalism from Monash University. She has studied Mandarin at Tsinghua University in Beijing.

DR ALEXANDRA PHELAN

Dr Alexandra Phelan is Deputy Director of Gender, Peace and Security Centre (Monash GPS), and a Lecturer in Politics and International Relations at Monash University. In 2019, she completed her PhD, which examined why the Colombian Government alternated between counterinsurgency and negotiation with the Revolutionary Armed Forces of Colombia (FARC). Based on an extensive examination of negotiation documents and primary FARC material, field work and interviews with former and active FARC, ELN, M-19 and AUC members, she critically examined the role that insurgent legitimation activities had in influencing Colombian Government responses between 1982 and 2016. Before she was appointed as a Lecturer in Politics and International Relations, she was a postdoctoral fellow at Monash GPS. She was also a visiting scholar at Georgetown University's Center for Security Studies, Walsh School of Foreign Service (2019). Alexandra's research interests include insurgent governance and legitimation activities, insurgent women, political violence and organised crime, with a particular focus on Latin America. She edited the book *Terrorism, gender and women: toward an integrated research agenda* (Routledge, 2021). She currently serves on the editorial board for *Studies in Conflict and Terrorism*.

DR ANNE ALY MP

Dr Anne Aly MP has been the federal member for Cowan since 2016.

By her late twenties, Anne was a single mother of two young boys earning the minimum wage to put food on the table. She went on to study for her Masters and PhD and worked as a professor, academic and practitioner in counterterrorism and countering violent extremism. The founder of People against Violent Extremism, Anne was the only Australian representative to speak at President Obama's 2015 White House summit on countering violent extremism.

Inducted into the Western Australian Women's Hall of Fame in 2011, Anne was nominated for Australian of the Year in 2016 and received the prestigious Australian Security Medal.

PROFESSOR MICHELE GROSSMAN

Professor Michele Grossman is Research Chair in Diversity and Community Resilience at the Alfred Deakin Institute for Citizenship and Globalisation at Deakin University, where she also serves as Director of the Centre for Resilient and Inclusive Societies and Convenor of the AVERT Research Network for Australian terrorism studies. Her research and publications on preventing and countering violent extremism have had key national and international academic, policy and practice impacts. Michele is on the editorial board of *Terrorism and Political Violence* and on Hedayah's International Advisory Board, and is a Robert Schuman (Distinguished Scholar) Fellow at the European University Institute in Florence as part of a Horizon 2020 Research and Innovation project, among other appointments.

ASSOCIATE PROFESSOR DR NATALIE DAVIS

Associate Professor and Federal Agent Natalie Davis commenced her policing career with the Australian Federal Police in 1987. She has diverse experience in criminal investigations, including a two-and-a-half year attachment to the National Crime Authority and as the Principal Operational Psychologist. She has been an operational psychologist in the AFP for more than 20 years after receiving specialist training in the UK. She's currently the Principal Operational Psychologist, providing behavioural science advice to investigative teams and operations and oversight of operational psychology within the AFP.

COMMANDER SANDRA BOOTH

Sandra Booth began her policing career with the Australian Federal Police in 2000. She has diverse experience in criminal investigations and has worked in a broad range of operational areas, including ACT Policing, Specialist Response Group, People Smuggling, Organised Crime and Intelligence.

Promoted to the AFP Executive in January 2019, she had responsibility for the joint counterterrorism teams in Victoria, South Australia, Tasmania and Western Australia. In May 2020, Sandra assumed the role of Commander Counter Terrorism—Enduring Risk Investigations to manage AFP responsibilities in relation to the release of high-risk terrorist offenders and national risk analysis and disruption.

Her AFP experience includes two deployments to Solomon Islands, a short-term deployment to Timor-Leste and three years as the Senior Liaison Officer in Jakarta, where she worked closely with the Indonesian National Police on terrorism, narcotics, people smuggling and child protection operations.

Sandra has been conferred with a Masters in Leadership and Management from Charles Sturt University, is a graduate of the FBI National Academy, and has been awarded the Commissioner's Group Citation for Conspicuous Conduct, the Commissioner's Group Citation for Excellence in Overseas Service and the AFP Operations Medal for Operation Crowea, among others.

DEPUTY COMMISSIONER ROSS GUENTHER APM

Ross Guenther APM, Deputy Commissioner Victoria Police, joined Victoria Police in 1985. He's an accomplished police officer, and his professional experience encompasses the leadership and management of teams across investigative, general policing, specialist operations and business environments.

As a commissioned officer, Ross has managed and led successful change management programs at Victoria Police's Centre for Investigator Training, Airlie Leadership Development Centre, Security Services Division and more recently as a Divisional Manager within the Southern Metropolitan Region. In 2015, he was promoted to the rank of Assistant Commissioner and in 2016 became the inaugural head of Victoria Police Counter Terrorism Command.

In June 2016, Ross was honoured to receive the Australian Police Medal as part of the Queen's Birthday honours, the citation praising his 'strong and deep commitment to people and leadership development'. In 2017, he was elected to the Leadership in Counter Terrorism (LinCT) Alumni Association Executive and currently holds the role of President. In 2019, Ross joined the International Association of Chiefs of Police and was subsequently nominated as a member of its Committee on Terrorism.

Ross was appointed Deputy Commissioner, Public Safety and Security in July 2020 and has portfolio responsibility for Counter Terrorism Command, Crime Command and Transit & Public Safety Command. He holds a Masters degree in criminology along with professional qualifications in project, business, training and strategic management streams.

ASSOCIATE PROFESSOR DEBRA SMITH (PHD)

Associate Professor Debra Smith (PhD) is a Principal Research Fellow at Victoria University. Her research focuses on questions of violent political extremism, social conflict and social change. She has a particular interest in the role of emotion within violent extremism beliefs and action, in the role of social media in radicalisation to violence, and in translating research for applied practitioner outcomes. Debra co-leads the Applied Security Science Partnership, which brings together researchers and law enforcement practitioners to undertake collaborative applied research on violent extremism for translation into frontline practitioner tools. She recently co-edited the first book on Australia's contemporary far-right and is currently co-authoring *International terrorism and counter terrorism in the Australian context*. In 2020, Debra was awarded the Vice-Chancellor's Award for Excellence in Research (Individual).

PIA VAN DE ZANDT

Pia van de Zandt is the Director of the Office of Community Safety and Cohesion at the NSW Department of Communities and Justice.

The office works closely with NSW Police, Corrective Services, Youth Justice and a range of social policy agencies such as Multicultural NSW, Education and Health to advise on policy related to terrorism and violent extremism. The office leads strategy development and implementation on CVE, and designs and delivers programs to promote community safety, cohesion and inclusion.

AFTAB MALIK

Aftab Malik is the Research and Community Engagement Manager at the Office of Community Safety and Cohesion.

MADELEINE COOREY

Madeleine Coorey is a Senior Policy Officer at the Office of Community Safety and Cohesion.

ANGEL ADAMS

Angel Adams is a PhD candidate with a focus on online and offline extremism in Australia at Deakin University and an international security research analyst with a focus on political violence, radicalisation, online and offline extremism and P/CVE programs in the Asia–Pacific and the Americas. She recently graduated from Monash University with a Master's degree in international relations, focused on political violence and counterterrorism. Angel obtained an Advanced Certificate in Politics and International Studies at the University of Melbourne and a Bachelor of International Relations at the Instituto Universitário de Pesquisas do Rio de Janeiro.

PETA LOWE

Peta Lowe is a Principal Consultant with Phronesis Consulting and Training. She is the former Director, Countering Violent Extremism for Juvenile Justice in the NSW Department of Justice. Peta has over 15 years experience working with young people involved with the justice system and has worked with individuals, families and communities to address offending behaviours and criminogenic risks. Peta graduated from Newcastle University in 2005 with a Bachelor of Social Work (Honours Class I) from Charles Sturt University. In 2010 she was conferred with a Masters of Social Work (Advanced Practice / Couples and Family Therapy Specialisation) from Queensland University of Technology. In 2016, she completed a Graduate Certificate in Business (Public Sector Management) and most recently, in 2018, from Charles Sturt University, was conferred with a Masters in Terrorism and Security Studies (Postgraduate University Medal). Peta participates as an international expert with the International Institute for Justice and the Rule of Law in Malta, working on the institute's Juvenile Justice Initiative, and is a Specialist Consultant with the CVE Unit at the Commonwealth Secretariat. She has also provided assessments related to risk for terrorism offences before the Supreme Court in Victoria.

LYDIA KHALIL

Lydia Khalil is a Research Fellow at the Lowy Institute and the Alfred Deakin Institute at Deakin University and a member of the Centre for Resilient and Inclusive Societies.

She has a broad range of policy, academic and private-sector experience and has spent her career focusing on the intersection between governance and security—whether it be understanding the rationales behind terrorism and counterinsurgency, how to create governance systems that lead to functioning societies, effective policing strategies or the security and policy effects of new technology. Lydia's professional background in politics, international relations and security has focused on US national security policy, authoritarianism, Middle East politics and counterterrorism. She has held previous positions at the Council on Foreign Relations, the US Department of Defense, and the New York and Boston police departments. Lydia is a frequent media commentator and conference speaker and has published widely on her areas of expertise. She holds a BA in International Relations from Boston College and a Masters in International Security from Georgetown University.

PROFESSOR BOAZ GANOR

Professor Boaz Ganor is the Ronald S Lauder Chair for Counter-Terrorism and former dean of the Lauder School of Government and Diplomacy at the Interdisciplinary Center (IDC) Herzliya in Israel. He is the founder and executive director of the International Institute for Counter-Terrorism. In 2019–20, he was on sabbatical from IDC Herzliya and served as a visiting fellow at ASPI, as an adjunct professor at the Australian Graduate School of Policing and Security at Charles Sturt University and as the Aaron and Cecile Goldman Visiting Israeli Professor and Israel Institute Fellow at Georgetown University. In his previous sabbatical (2008–09), he served as a Distinguished Visiting Fellow at the Hoover Institution at Stanford University.

Boaz serves as the founding president of the International Academic Counter-Terrorism Community, which is an international association of academic institutions, experts and researchers in fields related to the study of terrorism and counterterrorism.

Boaz has served as a consultant to the Israeli Government on counterterrorism and was appointed as a member of the International Advisory Team of the Manhattan Institute to the New York Police Department.

He obtained his BA in Political Sciences from Hebrew University and his MA in Political Studies from Tel Aviv University (thesis: 'Terrorism and public opinion in Israel'). His PhD thesis for the Hebrew University was on Israel's counterterrorism strategy.

Acronyms and abbreviations

AFP	Australian Federal Police
AML/CTF	anti-money-laundering and counter-terrorism-financing
ASG	Abu Sayyaf Group
ATA 2020	Anti-Terrorism Act of 2020 (Philippines)
AUSTRAC	Australian Transaction Reports and Analysis Centre
BACRIM	criminal bands (*bandas criminales* (Colombia)
CASA	Committee for Counter-Terrorism Strategic Analysis (*Comitato di Analisi Strategica Antiterrorismo*) (Italy)
CTB	Counter Terrorism Bureau (Israel)
CTF	counterterrorism financing
CV	Red Command (*Comando Velmelho*) (Brazil)
CVE	countering violent extremism
DEM	disaster and emergency management
ELN	National Liberation Army (Colombia)
FARC	Revolutionary Armed Forces of Colombia (*Fuerzas Armadas Revolucionarias de Colombia*)
FATF	Financial Action Task Force on Money Laundering
FIU	financial intelligence unit
FTF	foreign terrorist fighter
FTF	foreign terrorist fighter
GDP	gross domestic product
GTD	Global Terrorism Database
GTI	Global Terrorism Index
GTI	Global Terrorism Index
HRTO	high-risk terrorism offender
IED	improvised explosive device
IEP	Institute for Economics & Peace
INTRAC	Indonesian Financial Transaction Reports and Analysis Center
IPAC	Institute for Policy Analysis and Conflict
IS	Islamic State
ISA	Israel Security Agency
ISIL	Islamic State of Iraq and the Levant

ISIS	Islamic State of Iraq and Syria
ISWAP	Islamic State West Africa Province
JAD	Jamaah Ansharut Daulah
JI	Jemaah Islamiyah
MENA	Middle East and North Africa
MIT	Mujahidin Indonesia Timur
NFR	new far right
NGO	non-government organisation
P/CVE	preventing and countering violent extremism
PCC	First Capital Command (Primeiro Comando da Capital) (Brazil)
POI	person of interest
ReCAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia
RUSI	Royal United Services Institute (UK)
START	Study of Terrorism and Responses to Terrorism
TSA	*Terrorism Suppression Act 2002* (New Zealand)
UN	United Nations