Preface

Wicked problems are large and intractable issues – highly complex problems, often framed in political, social, economic and scientific dimensions that have multiple stakeholders who see the problem in different ways. Wicked problems require a high degree of process knowledge about creativity and collaboration in order to make even a dent in them. (Former Head of Civil Service Singapore, Peter Ho, 2008)

Rittel and Webber (1973) coined the term ‘wicked problem’ to refer to issues that are difficult to solve, not because the problem is inherently difficult, but because such problems do not offer themselves up to solutions. A wicked problem may be hard to define, and its causes may be complex and nebulous. Conventional solutions are unlikely to bring about a wicked problem’s resolution, and there are unlikely any definitive answers. Rittel and Webber (1973) described ten properties of wicked problems that make them distinct from ordinary problems:

1. We can define an ordinary problem, but a definitive formulation of a wicked problem will remain elusive. The formulation of a wicked problem is the problem!
2. We will know when a solution to an ordinary problem has been found; with wicked problems, we never really know when to stop searching for the solution.
3. With ordinary problems, we may objectively determine whether a solution was correct or incorrect; with wicked problems, it is a judgment call whether the solution was satisfactory or not.
4. We can tell if a solution has been effective in resolving an ordinary problem. On the other hand, solutions to wicked problems will generate consequences over an extended period of time, making it very difficult to measure the solution’s effectiveness.
5. With ordinary problems, we can apply solutions and learn by trial and error; with wicked problems, every trial must count because of the consequences that follow.
6. Ordinary problems come with a limited set of potential solutions, whereas wicked problems may not.
7. Every wicked problem is unique – we may learn to solve ordinary problems through experience over time, but with wicked problems, experience may not be as helpful.
8. A wicked problem is intertwined with other problems, whereas an ordinary problem may not.
9. There are many ways to explain wicked problems, and the choice adopted to explain the problem will determine the choice of solution in resolving it.
10. Solvers of wicked problems have to get it right, as they will be held responsible for the consequences of their actions, which have a large impact that are hard to justify.
Preface

Violent extremism is one such wicked problem.

It has persisted over time, and continues to evolve in its manifestation over time. This is made more daunting by the problematic nature of defining violent extremism and its closely-related phenomenon, especially terrorism\(^1\). There is no consensus in the literature regarding a universally accepted definition of violent extremism and terrorism in spite of decades of research. For the purposes of this book titled ‘Combating Violent Extremism and Radicalisation in the Digital Era’, a working definition of violent extremism would be “a willingness to use or support the use of violence to further particular beliefs, including those of a political, social or ideological nature. This may include acts of terrorism.” (Nasser-Eddine, Garnham, Agostino, & Caluya, 2011, p. 9). Online radicalisation can be defined as “the process by which an individual is introduced to an ideological message and belief system that encourages movement from mainstream beliefs toward extreme views, primarily through the use of online media such as Facebook, Twitter, and YouTube” (Community Oriented Policing Services, 2014, p. 1).

Having said that, ideologically motivated violence defies conventional categorisation and definition. It may be perpetrated by individuals or by groups; it may be motivated by various belief systems; it may be discriminate or indiscriminate. Violent ideologies attract a diverse audience – the religious, the thrill seekers, the humanitarians, the martyrs, the anti-establishment, the naïve. With the advent of the Internet and social media, this wicked problem is swaddled with an added layer of complexity.

In recent years, the violent extremism threat landscape has evolved rapidly. The threat of the past decade, Al-Qaeda, appears to have rescedind somewhat, although it has not been eradicated. In its place, various Salafi Jihadi groups, supposed affiliates of Al-Qaeda, have sprouted to continue applying the pressure of violent extremism. Exploits of the Boko Haram and Al-Shabab, for instance, continue to grab headlines and occupy news space. While most of the expression of violent extremist ideology has its epicentre in the Middle East region, the trend of lone wolf terror attacks in traditionally Western countries such as Australia, Canada, the United Kingdom, the United States and France, has also emerged. Such attacks, although limited in the scale of damage, are hard to detect and thwart, and bring the war on terror uncomfortably close to home. More importantly, these drive home the point how social media has expanded the reach of violent extremist ideology.

Alongside these developments is the emergence of the Islamic State in Iraq and Syria (ISIS), which signalled its arrival and determination with decisive military victories in Iraq and Syria. In fact, the expansion of ISIS influence into other countries in the Middle East and beyond suggests that it is still on an ascendant trajectory, and this is unlikely to abate any time soon. An incipient ISIS presence in the Southeast Asia region provides some proof of this growth.

ISIS is a particularly interesting case study because of its sophisticated use of social media to communicate its violent extremist ideologies. Using the Internet to its advantage, ISIS appears successful in putting forward an effective media campaign to raise its profile, attract and recruit fighters to its ranks, share practical information on performing jihad, and push out propaganda materials coupled with up-to-date videos, posts and images of its soldiers fighting at the warfront for a noble cause. In this digital era, ISIS appears highly successful in attracting foreign fighters to join them, and numerous violent extremist groups have affiliated themselves to it. A large part of ISIS success may be attributed to its online presence. While it may be argued that individual dispositions and vulnerabilities may cause one to decide to become a violent extremist, the ISIS example paints an equally compelling picture that online system factors may enlarge these vulnerabilities, increasing an individual’s susceptibility to persuasion by violent extremist ideologies. What, then, are the individual motivations and psychological attributes that increase one’s likelihood of becoming involved in violent extremism? How have online platforms
been exploited by violent extremists to their advantage? How do both these circles of influence interact, and how does the interplay between the person factor and the system factor result in involvement in violent extremism and online radicalisation?

Owing to the complexity of the wicked problem of violent extremism, a creative and collaborative effort is required to conceive answers. This means that problem solvers need to look further beyond traditional boundaries of thinking and work further beyond conventional partners to exact that dent in violent extremism. Knowledge drawn from diverse fields, such as psychology, sociology, economics, history, political science, technology, communications, statistics, and more, are vital and needed to contribute pieces to the puzzle of violent extremism. For an effective resolution of this wicked problem, interdisciplinary collaboration must take place.

This book was put together with the aim to help understand and address this wicked problem. There are three ways in which this book adds unique value.

1. We adopted a multidisciplinary approach, and asked experts and researchers in various fields to share their perspectives on the issue of violent extremism. Contributors to this book include psychologists, historians, experts in cyber systems, linguistics experts, and researchers in behavioural sciences. Each discipline provides a unique perspective of the wicked problem, and the confluence of perspectives through a multidisciplinary approach will give us greater confidence on the steps that need to be taken to resolve this problem.

2. With wicked problems, we only have one shot at them, because any actions we take to address them may result in further consequences. Bearing this in mind, we asked the contributors to this book to search wide and look deep into their respective fields to look for solutions. The end objective was to arrive at a collection of thoughts that is solution driven and deeply considered.

3. With ISIS theatre of operations taking a foothold in the Southeast Asia region, it is critical to revisit this wicked problem from an Asian perspective. Most of the literature on violent extremism has largely come from Western perspectives. To this end, this book aims to present some of the thinking from an Asian lens, in the hope that the concurrence of ideas, or a counterpoint as the case may be, may lend to more holistic points of view.

**ORGANISATION OF THE BOOK: SUMMARY OF CHAPTERS**

To facilitate your understanding of issues pertaining to countering violent extremism and radicalisation in the digital era, the chapters in this book have been organised broadly in the following themes, demarcated by sections. These sections are:

**Section 1:** Exploitation of the Internet by Violent Extremists (Chapters 1-5)  
**Section 2:** Understanding the ‘Person’ within Online Violent Extremism (Chapters 6-11)  
**Section 3:** Countering Violent Extremism and Radicalisation (Chapters 12-20)  
**Section 4:** Emerging Trends (Chapters 21-23)  
**Section 5:** Summary and Future Directions (Chapter 24)

Section 1 on the theme of ‘Exploitation of the Internet by violent extremists’ comprises a group of chapters that discuss the role of online platforms and how violent extremists can leverage – and in many
Preface

cases, have leveraged – on these online media for their needs and to propel their cause. Loo Seng Neo and his team in their chapter ‘Understanding the Psychology of Persuasive Violent Extremists Online Platforms’ highlight how violent extremist groups have not just exploited, but also created, online platforms that enhanced their recruitment campaigns across the world. The chapter examines the features of these platforms which enhance the appeal of violent extremist messages. Thomas Steinfatt and Dana Janbek focus on the history and use of propaganda in their chapter ‘Persuasion and Propaganda in War and Terrorism’, and discuss recent examples of how propaganda is used in online violent extremist mediums by terrorist groups such as Al-Qaeda and ISIS. Robyn Torok in her chapter ‘Social Media and the Use of Discursive Markers of Online Extremism and Recruitment’ examines the shift in recent years towards the use of social media to fuel violent extremism. The chapter discusses key discursive markers based on existing radicalisation models and how these markers are used to fuel violent extremism. Fajar Erieka, Idhamsyah Eka Putra, and Sarlito Sarwono in ‘ISIS Discourse in Radical Islamic Online News Media in Indonesia: Supporter or Opponent’ examine how discourses about ISIS based on two Islamic news websites are supported or rejected by radical Islamic groups. Finally, David Romyn and Mark Kebbell in their chapter ‘Using the Internet to Plan for Terrorist Attack’ discuss how terrorists can use the Internet as a source of information to plan for terrorist attacks, and how this information can be manipulated to reduce the likelihood or severity of a terrorist attack.

Countries and nations have treated and managed terrorism as a military issue, but it is a primarily human-cultural-psychosocial issue. Hence, there is a need to focus on the human actor. Section 2 is thus the theme of ‘Understanding the ‘person’ within Online Violent Extremism’, providing a person-specific focus on the issue of online violent extremism. This section contains chapters which examine the motivations and psychological attributes of the individual who may increase his/her likelihood of becoming involved in online violent extremism. Joyce Pang in her chapter ‘Understanding Personality and Person-specific Predictors of Cyber-based Insider Threat’ discusses the major challenges for understanding insider threat in the context of cyber security. It examines cyber-based insider threat from a personality and person-specific perspective that emphasises internal characteristics of the individual actor as explanations of actions and events. Omer Saifudeen in his chapter ‘Getting out of the Armchair - Potential Tipping Points for Online Radicalisation’ highlights another interesting angle affecting the human actor, that is, how the key to understanding tipping points in online violent extremism lies in understanding the cognitive, social and emotive barriers to violent extremist thinking and action. He discusses the need for research and experimentation on persuasional tactics for countering online extremism. Loo Seng Neo and colleagues in their chapter on ‘Why is ISIS so Psychologically Attractive?’ use a behavioural sciences perspective to explicate how individual motivational factors and organisational factors may contribute to the overall appeal of ISIS. Adding to this person-centric theme, Weiying Hu in her chapter on ‘Psychological Effects of the Threat of ISIS: A Preliminary Inquiry of Singapore Case Studies’ identifies five psychological drivers that have contributed to the radicalisation process of the cases of Singaporean individuals who had been attracted by ISIS radical online propaganda. Erin Saltman in her chapter ‘Western Female Migrants to ISIS: Propaganda, Radicalisation and Recruitment’ highlights how women continue to play strong roles in online and offline recruitment to violent extremist organisations. The chapter addresses questions of gender within current radicalisation trends through an analysis of online data that tracks Western females migrating to territories under the control of ISIS. Finally, Loo Seng Neo in his chapter on ‘An Internet-mediated Pathway for Online Radicalisation: RECRO’ introduces a framework to explain the interaction between cyber systems and person factors, and
highlight how this framework can be used to guide the identification of key behavioural markers for an individual’s involvement in online violent extremism.

In Section 3, the theme of ‘Countering Violent Extremism and Radicalisation’ comprises of chapters that bring us into the thick of key areas valuable for implementing measures to counter online violent extremism. Geoff Dean in his chapter on ‘Framing the Challenges of Online Violent Extremism: Policing-Public-Policies-Politics’ Framework’ uses a framework to expound real and relevant implications surrounding efforts to combat online violent extremism. Kumar Ramkrishna in his chapter on ‘Towards a Comprehensive Approach to Combating Violent Extremist Ideology in the Digital Space: The Counter-Ideological Response (CIR) Model’ introduces a model aimed to gradually diminish the appeal of violent extremist ideology. This model can potentially guide ideology-relevant policy interventions to impact the overall reach and appeal of the violent extremist narrative vis-a-vis any countervailing narrative put out against it. Damien Cheong in his chapter on ‘Countering Online Violent Extremism: State Action as Strategic Communication’ focuses on the utility of strategic communication strategies, particularly state action, in countering violent extremism both online and offline, while Jethro Tan and his team in their chapter ‘Building National Resilience in the Digital Era of Violent Extremism: Systems and People’ focus on building national resilience as a macro-level strategy for countering violent extremism. The latter chapter examines the ‘systems’ within a nation such as critical infrastructures and how they can be built ‘resilient-by-design’ to ensure continuity in times of crisis, and also explores ‘person’ factors of crisis communication, cohesion, and social capital, and discuss how instilling these factors can engender a cohesive society that can overcome the cracks in social order and harmony often caused by violent extremism. Jennifer Yang in her chapter on ‘Social Media Analytics for Intelligence and Countering Violent Extremism’ discusses collection methods and analytical tools for the study of social media data to facilitate intelligence-gathering and efforts to counter violent extremism. The coverage in this chapter includes social network analysis, sentiment analysis, multilingual analysis, geo-coding, automated entity extraction, semantic search and multimedia analysis.

There are also chapters in this section which introduce tools for assessing risk of online violent extremism and which discuss the challenges of making assessments in the online domain. Neil Shortland in his chapter on “On the Internet, nobody knows you’re a dog”– The Online Risk Assessment of Violent Extremists’ draws links on how psychology can contribute to conducting online risk assessment of violent extremism. Fredick Johansson and colleagues in their chapter on ‘Detecting Linguistic Markers of Violent Extremism in Online Environments’ discuss the use of linguistic markers in natural language processing as warning behaviours to detect online violent extremism. Elaine Pressman and Cristina Ivan in their chapter ‘Internet Use and Violent Extremism: A Cyber-VERA Risk Assessment Protocol’ introduce a new tool named CYBERA (adapted from the pre-existing tool VERA-2), which is designed to be a systematic, empirically-grounded, cyber-focused assessment guide to assess the risk of online violent extremism. CYBERA focuses on cyber-related behaviours and content to guide assessment of early signs of online violent extremism. Finally, Priscilla Shi in her chapter ‘A Supplementary Intervention to Deradicalisation: CBT-based Online Forum’ propounds the idea of online deradicalisation and delves into online therapeutic engagement and its potential applicability to deradicalisation.

Section 4 on the theme of ‘Emerging Trends’ comprises of chapters that highlight the potential threat posed by violent extremists as they adopt modus operandi commonly associated with cyber criminals. Leevia Dillon in her chapter on ‘Cyberterrorism: Using the Internet as a weapon of destruction’ focuses on cyberterrorism and draws on parallels from research on cyber threats and terrorism based on six themes (i.e., modus operandi, domain, targets, impact, antagonists and motivations) to formulate a cyberterror-
Preface

ism conceptual framework. The chapter provides a hypothetical four-step cyberterrorism attack sequence and suggestions for best practice. Penelope Wang in her chapter on ‘Death by Hacking: The Emerging Threat of Kinetic Cyber’ focuses on kinetic cyber threat and highlights various forms of kinetic cyber as well as the vulnerabilities that make devices and systems (e.g., personal medical devices, cars, critical infrastructures) susceptible. The chapter introduces motivations and characteristics of violent extremists who might engage in kinetic cyber attacks. Arun Vishwanath in his chapter on ‘Spear Phishing: The Tip of the Spear Used by Cyber Terrorists’ focuses on spear phishing, which is an email spoofing fraud attempt that seeks unauthorised access to confidential data, highlighting it as the vector used to gain access to a computer network in almost all forms of cyber attacks. The chapter, which emphasises the need for policy interventions, provides an overview of the different strategies being used to combat it and their relative effectiveness.

The final section, Section 5, brings the discourse on combating online violent extremism and radicalisation to a close by summarising the key learning lessons from the preceding chapters, as well as identifying future research directions. This concluding chapter on ‘What we know and what else we need to do to address the problem of violent extremism online’ by Majeed Khader, highlights potential future trends for online violent extremism and in tackling these trends, the need to understand the critical catalysts for change of which violent extremists can exploit. The chapter also discusses the need to evaluate counter violent extremism measures and identifies areas for future research.

In closing, we cite Brian Michael Jenkins, senior advisor to the president of the RAND Corporation, who wrote that:

[C]ounterterrorist efforts focus on only the operational portion of this cycle, the visible tip of the iceberg: from late in the recruitment process to death or capture. Insufficient attention is paid to defeating radicalisation, indoctrination, and recruitment at the front end or to developing a coherent strategy for dealing with detainees at the back end. We have concentrated on degrading the jihadists’ operational capabilities by eliminating jihadists, but not by impeding recruiting, inducing defections, or getting detainees to renounce jihad … this narrow vision is understandable. It reflects the traditional law enforcement approach in which the task of the police is to apprehend criminals and gather evidence for their prosecution. It comes from a narrow military approach in which the armed forces close with and kill or capture enemy soldiers and interrogate them for operational intelligence but do not consider prisoners a possible resource. (Jenkins, 2006, p. 124)

These comments greatly echo the sentiment of the editors of this book, who are psychologists and behavioural scientists by training. As co-labourers in this wicked problem of violent extremism, then, our counter-terrorism strategy must adjust to also address the sociological and psychological dynamics of violent extremism and radicalisation, and focus more at the front end.

Majeed Khader
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore

Loo Seng Neo
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore
Gabriel Ong  
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore  

Eunice Tan Mingyi  
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore  

Jeffery Chin  
Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore  

REFERENCES  


ENDNOTE  

1 According to Schmid (2011), the revised academic consensus definition of terrorism is: “Terrorism refers on the one hand to a doctrine about the presumed effectiveness of a special form or tactic of fear-generating, coercive political violence and, on the other hand, to a conspiratorial practice of calculated, demonstrative, direct violent action without legal or moral restraints, targeting mainly civilians and non-combatants, performed for its propagandistic and psychological effects on various audiences and conflict parties” (p. 86).