Detecting markers of radicalisation in social media posts : the role of person-centric and psychosocial risk factors, and protective factors

Neo, Loo Seng

2020

Neo, L. S. (2020). Detecting markers of radicalisation in social media posts : the role of person-centric and psychosocial risk factors, and protective factors. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/145173>

<https://doi.org/10.32657/10356/145173>

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

Downloaded on 26 Apr 2023 18:35:23 SGT

**NANYANG
TECHNOLOGICAL
UNIVERSITY**

SINGAPORE

**DETECTING MARKERS OF RADICALISATION IN SOCIAL MEDIA
POSTS: THE ROLE OF PERSON-CENTRIC AND PSYCHOSOCIAL
RISK FACTORS, AND PROTECTIVE FACTORS**

NEO LOO SENG

SCHOOL OF SOCIAL SCIENCES

2020

**DETECTING MARKERS OF RADICALISATION IN SOCIAL MEDIA
POSTS: THE ROLE OF PERSON-CENTRIC AND PSYCHOSOCIAL
RISK FACTORS, AND PROTECTIVE FACTORS**

NEO LOO SENG

SCHOOL OF SOCIAL SCIENCES

A thesis submitted to the Nanyang Technological University
in partial fulfilment of the requirements for the degree of
Doctor of Philosophy

2020

Statement of Originality

I certify that all work submitted for this thesis is my original work. I declare that no other person's work has been used without due acknowledgement. Except where it is clearly stated that I have used some of this material elsewhere, this work has not been presented by me for assessment in any other institution or University. I certify that the data collected for this project are authentic and the investigations were conducted in accordance with the ethics policies and integrity standards of Nanyang Technological University and that the research data are presented honestly and without prejudice.

11 July 2020

.....

Date

.....

Neo Loo Seng

Supervisor Declaration Statement

I have reviewed the content of this thesis and to the best of my knowledge, it does not contain plagiarised materials. The presentation style is also consistent with what is expected of the degree awarded. To the best of my knowledge, the research and writing are those of the candidate except as acknowledged in the Author Attribution Statement. I confirm that the investigations were conducted in accordance with the ethics policies and integrity standards of Nanyang Technological University and that the research data are presented honestly and without prejudice.

11 July 2020

.....

Date

.....

Assoc Prof Joyce S. Pang (Ring)

Authorship Attribution Statement

This thesis contains material from one paper published in the following peer-reviewed journal in which I am listed as an author.

Chapter 4 is published as Neo, L. S., Khader, M., & Pang, J. S. (2018).

Comparing ISIS foreign fighters versus sympathisers: Insights from their Twitter postings. *Home Team Journal*, 7, 87-106.

<https://www.mha.gov.sg/docs/default-source/publications/hta-journal-hr-issue-no-7.pdf>

The contributions of the co-authors are as follows:

- I wrote the drafts of the manuscript and performed all the data collection and data analysis.
- The manuscript was revised together with Dr Khader.
- Assoc Prof Pang edited the manuscript drafts, and provided guidance in the interpretation of the results.

11 July 2020

.....

.....

Date

Neo Loo Seng

Acknowledgements

This thesis has been an interesting journey of intellectual self-discovery. There are many people that I would like to acknowledge for their help and support as I embarked on this journey to complete my PhD.

First and foremost, I would like to take this opportunity to thank Associate Professor Joyce Pang for agreeing to be my supervisor and guiding me through the process of completing my PhD with her keen interest and invaluable critique of my research ideas and thesis writing. Next, I wish to express my sincere thanks for the guidance and support provided by my TAC members, Associate Professor Kumar Ramakrishna, and Adjunct Associate Professor Majeed Khader. Dr Majeed also happens to be someone whom I looked up to. Their expertise and valuable insights have an impeccable impact on my research direction. Special mention goes to Dr Shashi Jayakumar for sharing his database of Kurdish foreign fighters with me.

More importantly, I would like to thank each one of the participants and coders for my research studies. Thank you all for taking your time to participate in the research. I would also like to acknowledge the terrorism researchers whose work continued to inspire me to explore this field, as well as the valued relationships that I have developed with some of them over the years. Many of them are cited in the thesis.

Furthermore, I wish to convey my heartfelt appreciation to my friends (Jethro Tan, Leevia Dillon, Pamela Goh, Ken Chen, Jeffery Chin, Chan Chunmu, Dr Damien Cheong, Dr Omer Ali Saifudeen) and colleagues at HTBSC for their personal and professional support.

Lastly, this thesis is a tribute to my parents (Neo Chye Hock, Tan Siam Lang), sister (Neo Wenling), wife (Onpapha Detthammarong), and my three children (Neo Xi Zhen, Neo An Qi, and Neo An Ping). It would not have been written if were not for their love, understanding, and unwavering support.

Table of Contents

List of Tables	vii
List of Figures	ix
List of Appendices	x
Abstract	xi
CHAPTER ONE: INTRODUCTION AND OVERVIEW	1
1. Terrorism and the Internet	1
1.1 Autonomy to Create Radical Narratives	2
1.2 Form Online Communities of Like-minded Individuals	3
1.3 Threat of Radicalisation via the Internet	4
2. Foreign Fighters and the Internet	6
2.1 The Peculiar Case of the Islamic State in Iraq and Syria	8
3. Threat to Singapore	11
4. Aims of Research	12
4.1 Outline of Research	13
4.2 Significance of Research	18
4.3 Outline of Thesis	20
CHAPTER TWO: LITERATURE REVIEW	22
1. Deciphering Insights from Social Media Use	22
1.1 Markers of Radicalisation in Social Media Posts	24
1.2 Inherent Challenges in Identifying Markers of Radicalisation	26
2. Understanding Radicalisation Models	29
2.1 Pathway Models of Radicalisation	30
2.2 Pathway Models of Online Radicalisation	33
2.3 Operationalising Radicalisation Models	36
3. Extrapolating Insights from Theories of Online Radicalisation	38
3.1 Torok's Explanatory Model for Online Radicalisation	38
3.2 Shortland's Approach to Online Risk Assessment of Terrorists	39
3.3 Neo et al.'s Model for Assessing Risk of Radicalisation via the Internet	39
3.4 Bayerl et al.'s Radicalisation-factor Model	40
3.5 Summary	41
4. A Framework for Analysis: Person-centric, Psychosocial and Protective Dimensions	42

4.1 Person-centric Dimension	42
4.2 Psychosocial Dimension	45
4.3 Protective Dimension	48
5. Summary of Insights from Literature	50
CHAPTER THREE: IDENTIFICATION OF PERSON-CENTRIC AND PSYCHOSOCIAL RISK FACTORS, AND PROTECTIVE FACTORS	52
1. Modified Delphi Technique	54
1.1 Expert Panel Selection	55
1.2 Research Design	56
1.3 Three Rounds of Modified Delphi Technique	64
1.4 Results and Discussion	65
2. Literature Review to Supplement Modified Delphi's Findings	68
2.1 Relevant Areas of Research	70
3. Synthesising Person-centric and Psychosocial Risk Factors, and Protective Factors	72
3.1 Grouping the Modified Delphi's Factors into the Person-centric, Psychosocial, and Protective Dimensions	73
3.2 Person-centric Risk Factors	74
3.3 Psychosocial Risk Factors	79
3.4 Protective Factors	83
4. General Discussion	85
CHAPTER FOUR: COMPARING ISIS FOREIGN FIGHTERS VERSUS SYMPATHISERS: INSIGHTS FROM THEIR TWITTER POSTINGS	88
1. Which Terrorists' Supporters Goes on to Fight?	88
2. Method	91
2.1 Research Design	91
2.2 Sampling Procedure	93
2.3 Data Coding Procedure	95
3. Results	96
3.1 Factors Present in the Majority of the Foreign Fighter Subsample ...	98
3.2 Factors Present in the Majority of the Sympathiser Subsample	102
3.3 Comparing Foreign Fighters with Sympathisers	104

4. Discussion	107
CHAPTER FIVE: COMPARING ISIS FOREIGN FIGHTERS	
VERSUS SYMPATHISERS: INSIGHTS FROM THEIR SOCIAL	
MEDIA POSTS	112
1. Method	113
1.1 Inclusion Criteria for Sample	113
1.2 Identification of Sample	114
1.3 Data Coding	116
2. Results	118
2.1 Differences Between ISIS Foreign Fighters and Sympathisers	118
2.2 Predictor(s) for Becoming an ISIS Foreign Fighter	134
3. Discussion	137
3.1 Limitations	139
CHAPTER SIX: COMPARING ISIS FOREIGN FIGHTERS	
VERSUS KURDISH FOREIGN FIGHTERS: INSIGHTS FROM	
THEIR SOCIAL MEDIA POSTS	141
1. Background about Kurdish Foreign Fighters	141
1.1 Online Recruitment of Kurdish Foreign Fighters	142
1.2 Objectives of Study	143
2. Method	144
2.1 Identification of Kurdish Foreign Fighters	144
2.2 Consolidation of Sample Containing both ISIS and Kurdish Fighters	145
2.3 Data Coding	146
3. Results	147
3.1 Differences Between ISIS and Kurdish Foreign Fighters	147
3.2 Predictor(s) for Becoming an ISIS Foreign Fighter	160
4. Discussion	163
4.1 Limitations	165
CHAPTER SEVEN: UNDERSTANDING COMMUNITY'S	
PERCEPTIONS TOWARDS RADICALISATION VIA THE	
INTERNET AND TERRORISM	166
1. The Important Role of the Community in Countering	
Radicalisation	167

1.1 Objectives of Study	168
2. Method	169
2.1 Participants	169
2.2 Measures	170
2.3 Procedures	171
3. Results and Discussion	171
3.1 Group Differences Between NTU and MTurk Samples	171
3.2 Factor Analysis of the Ratings of the Indicators	174
3.3 Group Differences on General Awareness of Online Radicalisation and Terrorism	181
4. Conclusion	190
CHAPTER EIGHT: GENERAL DISCUSSION	193
1. The Detection of Online Radicalisation	200
2. Implications for Online Risk Assessment	204
2.1 Mapping of Indicators to Radicalisation Models	206
2.2 Automating the Screening Process	207
3. Broader Implications and Future Directions	208
3.1 Research Design for Terrorism Studies	209
3.2 Ethical Issues	211
3.3 Terrorists' Learning Capability	212
3.4 Generalising the Findings to Different Terrorists' Supporters	213
3.5 Inoculate the Community Against Online Radicalisation	214
4. Conclusion	215
References	218

List of Tables

Chapter 2

Table 1. Eight Warning Behaviours	25
Table 2. Behavioural Indicators of Stage Progression in Radicalisation Trajectories	33
Table 3. Mapping RECRO Pathway Framework to Younes Tsouli	36
Table 4. Pathway Models of Radicalisation	37
Table 5. Compilation of Research Themes	41

Chapter 3

Table 6. Terrorism Risk Assessment Tools included in the Modified Delphi Technique	59
Table 7. Consensus Rating for the Top 12 Factors	65
Table 8. Review of Three Academic Databases	68
Table 9. Dimensions and Factors for Detecting Radicalisation in Social Media Posts	74

Chapter 4

Table 10. Person-centric, Psychosocial, and Protective Dimensions and their Associated Factors and Indicators	92
Table 11. Presence of Factors for Foreign Fighters and Sympathisers	97
Table 12. T-test Results Comparing ISIS Foreign Fighters' and Sympathisers' Tweets	106

Chapter 5

Table 13. Information about the Social Media Accounts of 36 ISIS Supporters (2012 to 2015)	115
Table 14. Intra-class Correlation (ICC) Agreement Between the Three Coders	117
Table 15. Prevalence of Factors and Indicators Across ISIS Supporters	121
Table 16. Logistic Regression Model for Predicting Who Becomes a Foreign Fighter	135

Chapter 6

Table 17. Information about the Social Media Accounts of 40 Foreign Fighters (2012 to 2015)	145
--	-----

Table 18. Intra-class Correlation (ICC) Agreement Between the Three Coders	146
Table 19. Prevalence of Factors and Indicators Across ISIS Fighters and Kurdish Fighters	151
Table 20. Logistic Regression Model for Predicting Who Becomes an ISIS Foreign Fighter	162
Chapter 7	
Table 21. Differences Between NTU and MTurk Participants in their Ratings of the Indicators	173
Table 22. Factor Analysis of the Ratings of the 42 Indicators	176
Table 23. Questions Relating to Information Source	183
Table 24. Questions Relating to Countering Terrorism Measures	187
Table 25. Questions Relating to Radicalisation	190
Chapter 8	
Table 26. Summary of Studies Conducted	197
Table 27. Mapping the Factors to RECRO	207

List of Figures

Chapter 2

Figure 1. Involvement in Terrorism	30
Figure 2. Framework for Detecting Markers of Radicalisation in Social Media Posts	42

Chapter 3

Figure 3. The Research Process to Identify the Factors and their Associated Indicators	53
Figure 4. The 3-round Modified Delphi Technique	57
Figure 5. Sampling Procedure for Creating the Survey Items	58

Chapter 5

Figure 6. Median Severity Ratings Across Four Factors	126
Figure 7. Multidimensional Scaling Plot of ISIS Supporters	128
Figure 8. Multidimensional Scaling Plot of the 37 Indicators	130
Figure 9. Multidimensional Scaling Plot of ISIS Supporters and the 37 Indicators	131

Chapter 6

Figure 10. Median Severity Ratings Across Four Factors	155
Figure 11. Multidimensional Scaling Plot of Foreign Fighters	157
Figure 12. Multidimensional Scaling Plot of the 39 Indicators	158
Figure 13. Multidimensional Scaling Plot of Foreign Fighters and the 39 Indicators	160

Chapter 7

Figure 14. Source of Information on Terrorism	182
Figure 15. Definitional Elements of Terrorism	184
Figure 16. Channels to Report Suspicious Behaviours	186
Figure 17. Reasons for Not Reporting	188

Chapter 8

Figure 18. Assessment of Risk using the Indicators	203
--	-----

List of Appendices

Appendix A. Commonalities across the Six Terrorism Risk Assessment Tools	259
Appendix B. Survey Used for Modified Delphi Technique	270
Appendix C. Codebook for Identifying Factors and their Indicators	275
Appendix D. Survey on ‘understanding community’s perceptions towards radicalisation via the internet, and terrorism’	279
Appendix E. Mean and Standard Deviation for Ratings on the 42 Indicators	285

Abstract

The ubiquity of online radicalisation warrants the need for law enforcement to learn how to harness open-source intelligence to assess the threat posed and identify potential terrorists in advance. Although much is known about the online radicalisation process, there is a lack of risk assessment instruments developed specifically for online radicalisation, as well as little empirical research in this field. To address these research gaps, this thesis aims to articulate a set of person-centric and psychosocial risk factors and protective factors for identifying radicalisation in social media posts. Five studies were conducted. The first study (chapter 3) involved the use of a modified Delphi technique and literature review to derive a list of 12 factors and 42 indicators. The second study (chapter 4) served as a pilot to map the said factors and indicators to two groups of supporters of terrorists who have been influenced by radical online propaganda. These two groups comprise individuals who travelled to join the Islamic State in Iraq and Syria [ISIS] (i.e., foreign fighters), and individuals who did not travel to join ISIS (i.e., sympathisers). Next, the third study (chapter 5) built upon study 2 and incorporated changes to the research design (e.g., use of multidimensional scaling, logistic regression) to map the factors and indicators to a larger sample of ISIS foreign fighters and sympathisers. The fourth study (chapter 6) was designed to replicate the research methodology of study 3 using a different sample (i.e., Kurdish fighters) to compare against ISIS fighters. Finally, the fifth study (chapter 7) detailed a survey conducted with members of the community (NTU undergraduates and MTurk workers) on their perceptions towards the indicators and their general understanding of online radicalisation and terrorism. The

practical, methodological, and theoretical implications of this research as well as suggestions for future studies are discussed in chapter 8.

CHAPTER ONE: INTRODUCTION AND OVERVIEW

Contemporary society has witnessed how terrorists have exploited the internet and social media for their nefarious agendas. With the advancement of new information and communications technology, terrorists have effectively used the internet to create and disseminate propaganda materials to their supporters (Weimann, 2010). Specifically, the internet's open architecture expands the reach of terrorists to previously unreachable audiences and transforms the way they engage with one another and with their supporters. This is best exemplified by the rapid growth in online discourse, e-publications, and platforms—e.g., social media accounts, forums, websites—created by terrorists (Lemieux et al., 2014). As Holbrook and Horgan (2019) argue, this would increase the likelihood of individuals chancing upon radical materials fortuitously and developing interest in it.

From a law enforcement perspective, it is therefore not surprising that attention has focussed on how terrorists exploit the internet. This is not least because recruitment by terrorists is increasingly mediated through online social networks (Torok, 2013). In particular, concerns for authorities come in the form of an increased number of individuals who engaged in attacks after they were radicalised via the internet (Edwards & Gribbon, 2013; Yasin, 2017). As the threat shows no signs of abating, there is a need to better understand how terrorists have used the internet to radicalise and mobilise their supporters into action. One way of advancing such knowledge is by developing and examining some potential measures of online radicalisation that can assist law enforcement in their intervention efforts.

1. Terrorism and the Internet

The internet has redefined and blurred the geographical boundaries of terrorism. In the past, the influence of terrorist groups was restricted to traditional channels of communications, such as radio broadcasts, newspapers, and television. Terrorist groups thus faced recruiting limitations due to the limits of their physical social networks. With increased scrutiny and pressure from law enforcement, many terrorist groups were also denied a physical place to operate, recruit, and propagate their ideologies (Mukhtar, 2016).

The growth of the internet and social media platforms has allowed terrorists to thrive virtually without any of the same restrictions that they faced in the past. For example, Ramalingam (2012) observed that many far-right organisations in the United States are highly efficacious in utilising the internet to expand their operations beyond national borders, and avoid police investigations. Many observers have argued that the affordances offered by the internet have provided terrorists with the platform to reach a wider audience more quickly than traditional offline methods (Baumgarten, 2017; Dauber & Winkler, 2014). In short, it is easier for terrorists to disseminate their propaganda online and to convince individuals to join them.

1.1 Autonomy to Create Radical Narratives

The internet also grants terrorists the autonomy to better control the messages they convey to a mass audience, enabling them to paint a positive and powerful image about themselves while undercutting the legitimacy of their enemies. Kimmage and Rudolfo (2007) have observed:

Once an affiliated individual has received that footage [actual attack] and basic accompanying information, which can be transferred over the internet or by mobile phone, he has only to add the insurgent group's logo, a short title sequence, and perhaps a soundtrack with a motivational song. He then uploads the resulting video

product to a free upload-download site and posts an announcement to a forum. The video-editing software required to produce such a video is cheap and readily available. More importantly, the only material needed from Iraq is the actual footage of the attack. All of the additional elements required to create a video clip—insurgent group logo, songs, etc.—are readily available on the internet. (p. 35)

The relative ease of information production therefore endows terrorists with the means to communicate their ideas more effectively to their supporters.

Terrorist groups, such as ISIS, have also used the internet to propagate distressing images or videos of beheadings to create an environment of fear and panic amongst the masses. The repeated exposure to such videos, as Lim (2016) emphasised would intimidate and incite negative reactions amongst the public. In other examples, Rogan (2007) asserts that groups, such as Al-Qaeda, would reframe their narratives to illustrate the noble cause of defending Islam using violence. Such narratives may gain traction amongst certain segments of the population who were already angered by the suffering of Muslims in conflict zones (Hu, 2016). In comparison to the pre-internet era, the internet's interactivity and ease of creating user-oriented content help terrorists to disseminate their propaganda to their target audience and bring them together, across geographical boundaries, to form online communities.

1.2 Form Online Communities of Like-minded Individuals

The new communication means offered by the internet and various social media sites such as Facebook, YouTube, and Twitter have lent themselves to the purpose of forming online communities, where terrorists can recruit and connect with their supporters (Bowman-Grieve, 2013; Lara-Cabrera et al., 2017; Radlauer, 2007). As Conway (2012) puts it, the online community also makes it easier for individuals to reach out to terrorists and like-minded

others, as well as access propaganda materials. From a psychological perspective, the online congregation of like-minded people serves as an echo chamber, in which the sentiments and views of the members are shared, reinforced and polarised towards the extreme (Sunstein, 2002). As a result, the members may become more entrenched with the ideals propagated by the terrorists.

This can have several effects on the online community. Firstly, members may believe they belong to a larger global movement and start to identify with it (Caiani & Kröll, 2015). This perspective was also shared by Wimmer and Nastiti (2015) when they noted how terrorists' supporters would actively re-share the content put forth amongst themselves, in an attempt to gain recognition and acceptance. This may abet the supporters' radicalisation process. Secondly, it serves a practical purpose by allowing members to personalise their plight and circumstances within a larger movement to explain their current circumstances. Andre (2012) found that terrorists from southern Thailand would disseminate propaganda on YouTube that reposition their struggle against the Thai government within the ideology put forth by transnational groups such as Al-Qaeda. Lastly, these online communities also serve as virtual training camps for terrorists' supporters. For example, it allows members to share and gain access to technical information, such as how to conduct an attack or build an explosive (Barnes, 2012), as well as information about their targets (Gill & Corner, 2015). In some cases, these individuals may transit offline and perpetuate physical acts of violence against their targets.

1.3 Threat of Radicalisation via the Internet

The easy access to the terrorist online communities and radical propaganda, coupled with the increasing rates of internet usage worldwide gives rise to concerns about the internet in the radicalisation process (Jones et al., 2018; Neumann, 2012). In this thesis, radicalisation via the internet is defined as

the process by which an individual is introduced to an ideological message and belief system that encourages movement from mainstream beliefs towards extreme views, primarily through the use of online media, including social networks such as Facebook, Twitter, and YouTube. (Community Oriented Policing Services, 2014, p. 1)

Despite the recognition that the internet influences the radicalisation process, there is still a debate regarding the exact nature of the relationship between these two variables. On the one hand, some individuals have been radicalised solely by terrorist propaganda that they had consumed online, as exemplified by the case of Roshonara Choudry. Choudry was radicalised by the online lectures of Anwar al-Awlaki and had gone on to stab Stephen Timms—Member of U.K. Parliament—with a kitchen knife. However, such instances are considered by many to be an outlier within the terrorism literature (Pearson, 2015).

On the other hand, there are other individuals who are partially radicalised via the internet. Examples of such individuals are Nidal Hasan of the Fort Hood shooting, and the Tsarnaev brothers of the Boston Marathon attack. These individuals were affected by a mix of online and offline influence in their radicalisation pathways. They were not only shaped by the radical ideologies they had internalised from the internet but also influenced by the conversations they had with like-minded individuals (Bergin et al., 2009). In many cases, terrorists have utilised a gradual inoculation process to ‘groom’

potential members and get them more and more involved in their activities. Terrorists begin interacting with them on social media sites, before encouraging them to move to private encrypted online platforms or real world to continue the communication. Thus, the internet has levelled the playing field for terrorists to radicalise and recruit new supporters (Cohen et al., 2014; Nuraniyah, 2018; Vacca, 2019), giving rise to an unprecedented increase in cases of self-radicalised individuals and the attacks they perpetrated. It is noteworthy that most of these self-radicalised individuals are not full-fledged terrorists; they are best described as terrorists' supporters who have decided to conduct acts of violence after being radicalised by the terrorists' online rhetoric.

Regardless of how much attention is placed on the high-profile attacks and their perpetrators, we should not ignore the threat posed by the other non-violent supporters within the online communities (Hussain & Saltman, 2014; Mascini, 2006). Although they do not engage in acts of violence, the actions they take help terrorist groups to survive and stay relevant. Seib and Janbek (2011) assert that the real threat stems from the likes of young people who are avid followers of the radical online communities, where they engage in debates and discussions with one another. While they are generally consumers of terrorist rhetoric, some of them have also taken the step to produce radical content—i.e., they would repackage and re-disseminate the radical materials. In the process of doing so, they provide momentum for the movement. Brachman (2008), based on his analysis of the global jihadi movement, aptly termed these avid supporters as 'jihobbyists' who drive their radicalisation without any formal links to known terrorist groups.

2. Foreign Fighters and the Internet

This thesis argues that we can deepen our understanding of online radicalisation by studying foreign fighters. In recent times, news of foreign fighters gained media prominence as thousands of them left their home countries to join terrorist groups, such as ISIS and Al-Qaeda, in the Middle East. These groups have utilised various social media platforms to disseminate their propaganda, radicalise new supporters, and mobilise them to travel to Syria and Iraq as foreign fighters (Donnelly et al., 2017; el-Said & Barrett, 2017; Koch, 2019). This observation supports a point made by Ramakrishna (2013, p. 1): “to fully understand violent religious radicalisation, one must understand how a young person goes from being a ‘virtual’ to a ‘violent’ radical”. Hence, researchers interested in the phenomenon of online radicalisation should examine foreign fighters and how they are radicalised and subsequently mobilised via the internet.

Various academics (Cilluffo et al., 2010; Malet, 2013; Skidmore, 2014) have tried to define ‘foreign fighters’, and the most commonly accepted definition is the one proposed by Hegghammer (2013). He identified three criteria for someone to qualify as a foreign fighter: The person has to travel out of their home country and join a foreign conflict; they have to participate in military-related activities that target an enemy; the conflict is not located in any western countries. Neo et al. (2016) expanded Hegghammer’s definition to include foreign agents who are not from the West—as evinced by the influx of foreign fighters from other parts of the world. They define a foreign fighter as “an unpaid individual from outside the conflict zone who voluntarily joins and operates in a third-party conflict in which he/ she does not have a direct stake” (p. 151). This thesis adopted this definition of foreign fighters.

Efforts have been expanded to explain the influx of foreign fighters to Iraq and Syria, and how it has revolutionised the terrorism landscape. Some studies focus on how the internet facilitated the recruitment process of the fighters (Benmelech & Klor, 2018), whereas others examine the characteristics associated with them (van Ginkel & Entenmann, 2016). Some studies have highlighted the historical precedents of travelling abroad to take part in conflicts. For instance, at the beginning of 1979, thousands travelled to Afghanistan to defend Muslims against the Soviet occupation (Koch, 2019). Other conflicts where foreign fighters have played a significant role include Bosnia in 1992, Chechnya in 1994, Iraq in 2003, Syria in 2011 (Donnelly et al., 2017).

Some studies pointed out that the previous conflicts featuring foreign fighters were constrained by the lack of an effective communication medium, resulting in reduced media attention. As Donnelly et al. (2017, p. 2) opine, “media outreach began with Afghanistan in the 1980s with flyers and newsletters for propaganda purposes, while today’s international militants broadcast their battles using video cameras and curated social media strategies”. Not surprisingly, none of these conflicts had attracted as many foreign fighters as in the case of ISIS.

2.1 The Peculiar Case of the Islamic State in Iraq and Syria

Discussions of ISIS tend to be about the group’s ability to recruit foreign fighters using social media, prompting many to label the conflict as the most socially mediated one in history. While the recorded number of foreign fighters departing for Iraq and Syria varies, depending on the source, some estimates suggest that 41,490 fighters from 80 countries have joined the group,

of which 13 per cent were women (Cook & Vale, 2018). From the Southeast Asia region, the group has also managed to mobilise about 150-900 foreign fighters to travel and join them (Schulze & Liow, 2019).

While many factors could have contributed to ISIS' success in recruiting foreign fighters, such as the declaration of an Islamic Caliphate as its *raison d'être* (Simons, 2018), its ability to govern a state (Wood, 2015), and exert dominance over other terrorist groups (Ali, 2014), some scholars (e.g., Skinner, 2015; Stern & Berger, 2015) have suggested that the main factor is the ability of ISIS to use social media in a sophisticated manner. ISIS has placed a considerable emphasis on producing appealing messages that connect with its target audience and disseminate them via its online platforms. Online magazines, such as *Dabiq* and *Rumiyah*, were created to provide coverage of ISIS' military achievements, political news, and religious interpretations. In a *Dabiq* article titled "Hijrah from Hypocrisy to Sincerity", ISIS called on:

Every Muslim professional who delayed his jihad in the past under the pretence of studying Shariah, medicine, or engineering, etc., claiming he would contribute to Islam later with his expertise, should now make his number one priority to repent and answer the call to hijrah, especially after the establishment of the Khilafah. (Issue 3, p. 26)

Thus, such narratives have focused on the religious aspects of things and painted the caliphate that ISIS has established as the only place where Muslims should live (Ramakrishna, 2016). An eschatological narrative of a celestial battle between good and evil was also commonly featured. To attract the youths, narratives have been framed using imagery of battles and weapons to emphasise the adventure that they can experience if they were to join ISIS. Deliberate attempts were also made to humanise the ISIS foreign fighters by uploading pictures of them living their lives within the caliphate—e.g.,

enjoying food and playing with their pets; this served to depict the caliphate as a liveable place. ISIS has therefore created an effective recruitment campaign by tailoring its propaganda materials for different target groups. Bloom and Daymon (2018) further contend that such carefully crafted narratives may capture the imagination of vulnerable individuals worldwide, and in doing so, increase their motivation to join the group.

Even in the wake of military setbacks and territorial losses in Iraq and Syria, ISIS continues to be a security concern for two reasons. Firstly, some countries have seen foreign fighters returning home (Holmer & Shtuni, 2017; Speckhard et al., 2017). These returning fighters have received training in ISIS training camps and are hardened with war experience, both of which provided them with the skill set required to carry out an attack (Byman, 2017), as seen in incidents such as the 2015 Paris attacks and the 2016 Brussels bombings. These returnees may also act as purveyors of ISIS' ideology and terror tactics in the regions that they migrate to (Jerard, 2017), and galvanise the local radical entities into action.

Secondly, ISIS has demonstrated great proficiency in staying relevant by inciting digital natives in its online community to promulgate its ideology and conduct attacks in their home or host countries (Freeman et al., 2017). For example, in the 2017 attempted attack in New York by Bangladeshi immigrant Akayed Ullah, Ullah said that ISIS online propaganda inspired him to commit the attack ("New York Port Authority", 2017). Thus, this warrants the need for law enforcement to channel their attention towards ISIS supporters in their home country, whose radicalisation process is greatly facilitated by social media.

3. Threat to Singapore

Singapore is not immune to terrorism-related developments. As outlined in the Ministry of Home Affairs [MHA]’s 2019 Terrorism Threat Assessment Report, “the terrorism threat to Singapore remains high ... we continue to detect Singaporeans, and foreigners working in Singapore becoming radicalised by terrorist propaganda” (para. 1). While the figures in Singapore pale in comparison to the radicalisation trends in other parts of the world, they are not inconsequential, especially when an actual act of terrorism can disrupt the communal harmony of our multi-racial society.

In the context of terrorism recruitment in Singapore, there are some notable observations. Firstly, Singapore has witnessed an increased number of self-radicalised individuals detained under the country’s Internal Security Act (ISA). Eighteen were arrested between 2015 and 2017, as compared to 11 between 2007 and 2014 (Loh, 2017). In the past three years, more than eight self-radicalised Singaporeans were also detained under the ISA. This suggests a growing threat of online radicalisation, perhaps exacerbated by the spread and availability of online terrorist propaganda. Secondly, some Singaporeans have travelled to join ISIS after they were radicalised from their online exposure to the group’s ideology (ISD Research Command, 2018). Lastly, the threat of online radicalisation is not unique to jihadi terrorism. In 2016, MHA reported that one of the detained Singaporeans, Wang Yuandongyi, had intended to join a Kurdish militia group that is fighting against ISIS (Jayakumar, 2016).

No fixed profile could be distilled from these arrested individuals. Instead, research—conducted by the psychologists who have interviewed them—has identified several psychological attributes that have increased their

susceptibility to online terrorist propaganda, and contributed to their radicalisation process (Hu, 2016; Robert 2019). This calls for the need to focus our attention on factors that may lead an individual to resonate with radical rhetoric, as these insights might enhance law enforcement's capability to detect terrorists and their supporters in advance. Nonetheless, there is a paucity of risk assessment tools developed specifically for online radicalisation, which undermines our efforts to identify malicious perpetrator in advance and/or triangulate offline intelligence (Dillon et al., 2017; Jore & Njå, 2010). Hence, increasing our knowledge about the detection of online radicalisation should be a priority for law enforcement officials, policymakers, and academics.

4. Aims of Research

For all these reasons, the primary aim of the current research is to articulate a set of person-centric and psychosocial risk factors and protective factors and their indicators that has the potential to aid the detection of online radicalisation. It is hoped that the factors and indicators revealed in this research will offer a preliminary template to outline germane online behaviours and expressions that serve as markers of radicalisation in social media posts.

Another aim of the current research is to test whether the identified factors and indicators can distinguish between two groups of terrorists' supporters: Sympathisers (i.e., did not participate in overseas conflict) and foreign fighters (i.e., participate in overseas conflict). Against the backdrop of the abovementioned conflict in Iraq and Syria, the factors and indicators were mapped against social media posts belonging to ISIS foreign fighters, ISIS sympathisers, and Kurdish foreign fighters.

Finally, the research is concerned about the community's perceptions towards the said indicators. The aim is not so much on getting the community members to assess the effectiveness of the indicators, but more to appraise their layman understanding of online radicalisation terrorist indicators. This can help to gauge their level of knowledge and any misconceptions regarding the topic. In sum, this entire research aims to contribute to the literature on terrorism by identifying a set of factors and indicators that can abet law enforcement in their counter terrorism efforts.

4.1 Outline of Research

To address these research aims, five studies were conducted. The first study involved the creation of person-centric, psychosocial, and protective factors and their associated indicators. A concurrent approach of an expert knowledge acquisition process (i.e., modified Delphi technique) and literature review was utilised to identify the relevant factors and indicators; this approach was also utilised by Post et al. (2002) to develop a framework to measure the risk that a terrorist group would pose. For the modified Delphi technique, a panel of seven subject-matter experts in the field of terrorism was asked to evaluate a list of factors that were collated from six terrorism risk assessment tools: Extremist Risk Guidance 22+ [ERG 22+] (Lloyd & Dean, 2015), Identifying Vulnerable People [IVP] (Egan et al., 2016), Terrorist Radicalisation Assessment Protocol [TRAP-18] (Meloy et al., 2015), Multi-Level Guidelines [MLG] (Cook, 2014), Violent Extremist Risk Assessment-2 [VERA-2] protocol (Pressman & Flockton, 2012), and Cyber-VERA (Pressman & Ivan, 2016). The consensus within the panel of experts serves to identify which factors are of greatest relevance for detecting radicalisation via the

internet. As these assessment tools were created based on in-depth literature review and interviews with terrorist offenders, they provide an excellent start point to reanimate research on identifying factors to detect online radicalisation. However, most of these tools tend to neglect the role of the internet (Dillon et al., 2017). Hence, the approach of conducting a parallel literature review on online radicalisation in this study complements the findings from the expert panel to identify relevant factors and indicators. In doing so, 12 person-centric and psychosocial risk factors and protective factors, and their 42 observable indicators were derived.

Study 2 mapped the identified set of factors and indicators from study 1 to two groups of individuals who have been influenced by ISIS' propaganda materials: Individuals who have successfully mobilised and travelled to join ISIS (hereafter denoted as foreign fighters), and individuals who are committed online supporters of ISIS but did not travel to join ISIS (hereafter denoted as sympathisers). As a pilot study, the aim was to examine whether the factors and indicators can be used to distinguish a foreign fighter from a sympathiser using their social media postings. 622 tweets posted by three ISIS foreign fighters and three ISIS sympathisers from the United Kingdom were mapped against the factors and indicators. After doing so, one significant difference between the two groups was found: Foreign fighters tend to create more postings that exhibited their readiness to commit violence. However, due to the small sample size, the findings have to be interpreted with caution. Having said that, this study has achieved its aim as an empirical probe to compare foreign fighters and sympathisers using the factors and indicators, and areas for improvement for the subsequent studies have also been identified.

Study 3 addressed the limitations identified in study 2 by increasing the sample size of the ISIS foreign fighters and sympathisers, by adding new criteria for coding in order to quantify the ‘severity’ of the social media posts, and by adopting new statistical techniques for data analysis (i.e., Fisher’s exact test and multidimensional scaling [MDS]) to distinguish foreign fighters from sympathisers based on their social media posts, and to identify any relations among the indicators. In study 3, the intra-class correlation (ICC) was used to measure the interrater reliability, and logistic regression was used to identify the indicator(s) that predicts the likelihood of someone becoming a foreign fighter. A sample of social media posts from 17 foreign fighters and 19 sympathisers was gathered using purposive sampling, and a total of 22,457 posts was used for analysis. Mean interrater reliability ranged from good to excellent across all variables. The study found several significant differences between the two groups. Foreign fighters tend to show their support to ISIS by expressing their interest to perform acts of martyrdom and reaching out to like-minded individuals. In contrast, sympathisers tend to show their support by displaying insignia related to ISIS on their social media accounts. Furthermore, foreign fighters’ postings were significantly rated to be more severe as compared to postings by sympathisers. Insights from MDS found that foreign fighters would engage in online expressions that underline their frustration and perceived grievances. Sympathisers, in contrast, were more inclined to perform ‘outreach’ efforts (e.g., sharing web-links) for the online community. Finally, the indicator “attempts to reach out to terrorists” (OR1) was found by the logistic regression model to increase the likelihood of the post creator to travel to Syria by 9.2 times. While I recognise that these findings may not be generalisable to the

entire terrorist population, they may help to further our understanding of this under-researched population using primary data, and provide some degree of postdictive validity in detecting markers of radicalisation in social media posts.

The fourth study was designed to replicate the research methodology of study 3 but using a different sample. Thus, study 4 investigates the external generalisability of the markers of online radicalisation. This study compared the social media output of 17 ISIS foreign fighters (from study 3) with 23 Kurdish foreign fighters. A total of 23,958 social media posts was used for analysis, and the mean interrater reliability ranged from good to excellent across all variables. This group of Kurdish foreign fighters, much like those affiliated with ISIS, was influenced and mobilised by the radical online propaganda that is disseminated by Kurdish militia groups and travelled to the Middle East to fight against ISIS. Several significant differences between the two groups were found. ISIS fighters tend to show their support towards the group by highlighting grievances affecting Muslims, expressing a higher level of intolerance towards others, and reaching out to like-minded individuals. Kurdish fighters, on the other hand, tend to showcase their interest in weapons and combat. As compared to their Kurdish counterparts, ISIS fighters tend to create posts that were rated more severe under the factors of “perceived grievances” and “intolerance towards multi-religious, multi-racial living”. The results of the MDS revealed that ISIS fighters were frustrated by their perceived grievances, as compared to the Kurdish fighters who were observed to be more interested in weapons and combat. Finally, the logistic regression model revealed five indicators that would increase the likelihood of a post creator to be an ISIS foreign fighter: “express willingness to die for cause, and achieve

martyrdom” by 7.8 times; “express frustration with the injustice targeted at one’s own community, faith, or belief” by 4.1 times; “express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice” by 4.5 times; “incites friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief” by 5.4 times; and “attempts to reach out to terrorists” by 3.1 times. These results added another dimension for the postdictive validity of the indicators.

The final study measured the community’s perceptions towards the indicators in terms of their utility to detect radicalisation on social media posts, as well as the community’s general awareness about online radicalisation and terrorism. A 74-item survey comprising of three sections was administered to 160 psychology undergraduate students from Nanyang Technological University (NTU) and 160 Amazon Mechanical Turk (MTurk) workers. The three sections were: Demographics (5 items); opinions about the indicators for detecting online radicalisation (42 items); and general awareness about online radicalisation and terrorism (27 items). Based on the ratings of the 42 indicators, two factor analyses were separately conducted using oblique rotation to uncover a four-factor structure for the NTU sample, and a three-factor solution for the MTurk sample. A follow-up comparison was made against actual terrorists’ online behaviours from study 3 to gauge the participants’ knowledge level about markers of online radicalisation. The results suggested that participants from both samples have identified the relevant predictor (OR1: “attempts to reach out to terrorists”) as a key indicator of interest. The last section of the survey focused on identifying where participants obtained their information on terrorists, their views on what constitutes the definition of

terrorism, their views on the role of the internet in radicalisation pathways, their perceptions on counter terrorism strategies, and their opinions on how an individual can become radicalised. The findings revealed differences across the two samples, and that they have certain misconceptions about radicalisation (e.g., MTurk workers were likely to view terrorist as mentally ill, from low-income families, and are male). Insights derived from this study have enhanced our understanding of the perceptions that community members may have concerning online radicalisation and terrorism, and provided valuable feedback that law enforcement can use to develop counter terrorism strategies.

4.2 Significance of Research

Because of the growing amount of resources and scholarly attention devoted to counter the threat of online radicalisation, it is natural for us to conclude that there would be many validated metrics to ascertain an individual's risk for online radicalisation. However, this is not the case, and this thesis attempts to address this research gap.

Firstly, as previous research demonstrated (Horgan, 2005; McCauley & Moskalenko, 2011), there is no one single perspective that can best illuminate our ability to discriminate amongst the general populace and detect the terrorist threat. Much more research, as this thesis argued, that integrates extant theories and models of radicalisation with known risk and protective factors to develop a theoretical point of reference that can be used to guide risk assessment for online radicalisation, is needed. Hence, this research proposes a set of person-centric, psychosocial, and protective factors and their associated indicators that can serve as an investigative template for identifying markers of radicalisation in social media posts.

Secondly, given that certain indicators may have a higher likelihood of co-occurring together (see Clemmow et al., 2020), this thesis utilised MDS to visualise the potential relationships among the indicators. This is especially pertinent in deciphering potential behavioural typology of a foreign fighter or sympathiser. In other words, if, during the course of assessing the social media posts of an individual, an indicator of concern was flagged, then the investigator should also look out for indicators which are highly-related with the one that was flagged.

Thirdly, researchers tend to rely heavily on secondary sources to study terrorism and radicalisation (Schuurman, 2018). It would therefore be useful to capture primary sources of data that can inform the study of online radicalisation. As LaFree and Dugan (2009, p. 417) remarked, “because of the unique interest that terrorist groups have in media attention, open-source information may be uniquely useful in the study of terrorism”. In line with this, this thesis utilised open-source social media posts of terrorists’ supporters for analysis. This is important because these postings provided valuable insights into the creators’ beliefs and online behaviours.

Next, within the terrorism literature, few studies to date have provided direct quantitative comparisons across groups (Conway, 2017). Most studies tend to focus on one particular group (e.g., Badawy & Ferrara, 2018; Ghajar-Khosravi et al., 2016), and the derived conclusion, no matter how parsimonious, are not generalisable to other terrorist groups. Thus, this thesis comparatively examines three groups of terrorists’ supporters: ISIS foreign fighters, Kurdish foreign fighters, and ISIS sympathisers. Specifically, the non-violent ISIS sympathisers served as an ideal control group against the violent ISIS foreign

fighters. This allows us to identify the factors and indicators that tipped an individual to transit from the online to the offline realm and become a foreign fighter. To ensure that fair comparisons are made, this thesis only used the social media posts of foreign fighters before they made their travel, and compared them with the postings made by the sympathisers within the same time frame—2012 to 2015. To the best of my knowledge, this is one of the first few scientific investigations that adopt this approach to identify factors and indicators that are unique to the foreign fighters.

Lastly, insights about the community members' understanding of online radicalisation and terrorism can inform law enforcement on areas that they can improve their public awareness messaging, and contribute to the development of counter measures for detecting radicalisation in social media posts. In conclusion, it is hoped that the findings from this thesis can have practical value for law enforcement officers, policymakers, as well as represent a stepping stone for academics to enhance theory construction and identify future studies in the domain of online radicalisation.

4.3 Outline of Thesis

This thesis consists of eight chapters. Chapter 1 introduces the role of the internet in radicalisation and presents an overview of the entire research. Chapter 2 identifies the person-centric, psychosocial, and protective framework that can help us to develop markers of online radicalisation. Chapter 3 presents study 1, which outlines the development of the person-centric, psychosocial, and protective factors and their associated indicators. Chapter 4 describes the findings of study 2, which is a pilot attempt to map the factors and indicators to the social media posts belonging to a small sample of ISIS foreign fighters and

sympathisers. Chapter 5 presents study 3, which is an enhancement of study 2. It mapped the factors and indicators with the social media posts belonging to a larger sample of ISIS foreign fighters and sympathisers. Chapter 6 is an elaboration of study 4, which compares ISIS fighters with Kurdish fighters based on how their social media posts were mapped onto the factors and indicators. Chapter 7, which describes study 5, details the findings from the survey conducted with NTU undergraduates and MTurk workers on their perceptions towards the indicators as well as their general understanding of online radicalisation and terrorism. Chapter 8 discusses the practical, methodological, and theoretical implications of this research.

CHAPTER TWO: LITERATURE REVIEW

This chapter begins by reviewing the literature on deciphering personal insights of an individual from their social media usage, followed by the inherent challenges of doing so. Next, existing models of radicalisation are presented. The literature on the theories of online radicalisation is then presented. The next section articulates a conceptual framework for identifying the relevant factors and their associated indicators for detecting radicalisation in social media posts. The final section highlights the key learning points of this literature review.

1. Deciphering Insights from Social Media Use

Psychology is one of the fundamental perspectives, by which we can understand human behaviours and decipher innate dispositions to distinguish one person from the others (Carver & Scheier, 2014). In general, the study of psychology can provide hints about how a person would probably react in different contexts. Research in personality psychology, for instance, has found that personality is related to important life outcomes, such as the formation of social networks (Selfhout et al., 2010), preference over the mode of communication (Boyd et al., 2015), predicting motivation and goal-directed behaviour (McClelland, 1987), as well as how one relates to the world (Allport, 1961).

As people—including terrorists and their supporters—spend more time online, their digital footprint grows, revealing insights about their behaviours and worldviews based on what they share and how they express it. Many behavioural science studies have adopted personality and social psychology theories to understand an individual's characteristics—e.g., belief systems, values, motivations—based on the information collected from online sources

(Golbeck et al., 2011; Gosling et al., 2011). For example, Alam et al. (2013, p. 6) made a comparative analysis of Facebook users' status text with the Big Five personality traits, and found "a strong correlation between users' personality and the way they behave on online social network". Other studies have found similar results of personality traits correlating with online word usage (Kern et al., 2014), and choice of profile image (Whitty et al., 2018). Twitter-centric studies have also made similar observations. Twitter users' following, followers, and listed counts have been found to accurately predict the users' personality (Qiu et al., 2012; Quercia et al., 2011). Utilising machine learning technique, Li et al. (2014) were able to predict Weibo users' personality traits based on their online behaviours on the micro-blogging site. Such works establish that it is reasonable to assume that we can gain a better understanding of a terrorist by coding their online generated content and behaviour.

Moreover, Back et al. (2010) have argued that social media profiles generally convey accurate impressions of the personality of their owners. Using aggregated scores from personality reports (measuring the Big Five personality dimensions), insights from the profile owners' self-reports, as well as reports from four well-acquainted friends, the personality ratings of social media profiles of 236 participants were found to reflect ratings on standardised measures of personality. This, as the authors argued, is contrary to the common assumption that people tend to paint a more flattering impression of themselves on their social media accounts.

At the same time, it is not just personality traits that are revealed online. Studies have shown that personality significantly correlates with several real-world behaviours. For example, researchers were able to identify an

individual's preferences for musical genres (Nave et al., 2018) and predict the hiring decisions by employers (Newness et al., 2012) based on their social media posts. In fact, Kosinski et al. (2013, p. 5802) remarked that “digital records of behaviour, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including ... religious and political views”. Such research suggests that it is possible to derive person-centric insights about individuals, perhaps even those who express radical worldviews from their digital footprints.

However, while social media sites may allow us to identify an individual's attribute, it is not by any means completely accurate, nor does it contain the complete psychological picture of an individual. Pang (2016) argues for the need to also consider the context in which the person is exposed to—specific environment conditions can influence the actual manifestation of attitudes, values, and other personality traits. Previously, some studies have suggested that such person-centric particularities are influenced by the presence of others in the cybersphere. In their analysis of personal value and word use on Reddit, Chen et al. (2014) found that individuals with high self-transcendence have a higher likelihood of expressing themselves using group-oriented words such as ‘we’ in the discussion website, and expend more effort to understand other people's perspectives. More recently, Crosset et al. (2018) observed that the relatability of values and technicalities associated with far-right ideology would contribute to the spread of such ideas within the online communities. In other words, the propagation of far-right content is found to be dependent on the extent to which the targeted recipients can relate to it.

1.1 Markers of Radicalisation in Social Media Posts

As stated above, research has shown that it is possible to decipher an individual's motivations and worldviews from their online communications. Importantly, this suggests that online information can potentially be used by law enforcement to detect individuals who are being radicalised online (Droogan et al., 2018). In fact, there are instances where individuals have been arrested for their online activities. For example, M Arifil Azim Putra Norja'i was detained under ISA in 2015 for making plans to join ISIS, or conduct attacks in Singapore if he was unable to travel (Wong, 2015). After being radicalised by ISIS online propaganda in 2013, Arifil started to recruit members to join him in carrying out attacks in Singapore, and "fortunately, another person who knew Arifil noticed the changes in him, and had brought him to the attention of the authorities, who were then able to investigate the matter and take action" (para. 15). Another example would be that of Syaikhah Izzah Zahrah Al Ansari, who came to the attention of the local authorities after she was actively posting and sharing pro-ISIS materials online (Cheong, 2017).

Table 1
Eight Warning Behaviours

Warning behaviour	Description
Pathway	Indication of an individual researching, planning, and preparing for an attack.
Fixation	The individual becomes preoccupied with a person or cause. It may be due to the obsessive drive for violence to redress or remediate the injustice.
Identification	The individual starts to identify with military paraphernalia, assassin, etc.
Novel aggression	The individual commits an act of violence on an unrelated target.
Energy burst	The sudden increase in frequency/variety of behaviours concerning the target.
Leakage	The individual shares with a third party of their intention to conduct attacks. The individuals may also release statements online.
Last resort	An indication that the individual is becoming desperate and distress.
Directly communicated	The individual directly communicates their intention to attack the target.

Note. Adapted from "The role of warning behaviors in threat assessment: An exploration and suggested typology", J. R. Meloy, J. Hoffmann, A. Guldemann, & D. James, 2012, *Behavioral Sciences & the Law*, 30(3), pp. 265-266, (<https://doi.org/10.1002/bsl.999>). Copyright 2012 by Wiley.

Hence, observable remnants of digital communications are a possible source of warning behaviours for intelligence gathering and means to understand terrorists' clandestine networks. Meloy and O'Toole (2011, p. 514) define these warning behaviours as any behaviour that "precedes an act of targeted violence, is related to it, and may, in certain cases, predict it". There are eight types of warning behaviours that are indicative of targeted violence (see Table 1), of which Cohen et al. (2014) found that 'leakage', 'identification', and 'fixation' warning behaviours have the highest likelihood of being discovered in digital communication. The ability to uncover, collect and analyse these online warning behaviours would therefore help law enforcement to intervene and prevent malicious actors from conducting their attacks.

1.2 Inherent Challenges in Identifying Markers of Radicalisation

However, there is a myriad of challenges that we need to be cognizant of before undertaking research on the study of factors and indicators of online radicalisation. These challenges can be summarised into five main areas.

1.2.1 Terrorism and Radicalisation are Low Base-rate Events

One challenge would be that of base-rate. The relatively low occurrence of terrorist attacks and radicalised individuals makes it hard for any identified indicator to be empirically validated (Powis et al., 2019; Schouten, 2010). It is therefore difficult to demonstrate how valid an indicator is in predicting future cases of radicalisation, and consequentially, affects the generalisability of that indicator as well.

1.2.2 Quantity and Quality of Terrorist Online Content

Identifying terrorist-related content on the internet is a daunting endeavour because of the sheer quantity of unrelated content that needs to be sifted through in order to obtain good quality relevant content. Within the cyber realm, anonymity, and the decontextualization of discourse in computer-mediated communication may undermine the credibility of the collected content as it is hard to verify the information (Crosset et al., 2018). In addition, the recent takedown by social media companies has directly reduced the amount of terrorist content online. For example, Twitter announced in 2016 that it suspended at least 360,000 terrorist-related accounts (“Combating Violent Extremism”, 2016). Concomitantly with this development is the adoption of new technologies by terrorists—especially those of an encrypted and ‘closed-door’ nature—to continue disseminating propaganda materials and communicating with their supporters (Bloom & Daymon, 2018). Thus, these conditions may leave authorities and researchers with a lack of access to relevant open-source information.

1.2.3 Identifying Relevant Factors and Indicators

Another challenge concerns the wide spectrum of online behaviours that can be associated with the radicalisation process. Some behaviours, such as the online expression of intolerance towards a specific group, are more typical of the earlier stages of radicalisation (Neo, 2016). Such behaviours are less obvious, and may not be easily recognised. In contrast, the later stages of radicalisation may be associated with obvious warning signs such as the explicit online communication of one’s intention to commit acts of violence or declaration of one’s loyalty to a terrorist group (Meloy et al., 2015). These behaviours are ‘red flags’ to those who are looking out for indicators of online

radicalisation. It is important to note that not all indicators would carry the same weight for everyone, and they should not be treated as such (Horgan, 2019).

This makes the identification of radicalisation markers a complex problem for which no single indicator can suffice. In line with this reasoning, Goodwill and Meloy (2019, p. 523) suggest the need to “identify those risk factors that co-occur and distinguish those who commit a terrorist act from the many who may be radicalised to a particular cause, and even support or facilitate such a cause, but pose no risk of violence”. Furthermore, researchers have called for the need to consider both protective and risk factors in the identification of potential threats (de Ruiter & Nicholls, 2011; Gill, 2015b).

1.2.4 Lack of Control Group Comparison

The lack of studies with a control group in terrorism research makes it hard for readers to identify factors that can differentiate terrorists from non-terrorists. In a recent systematic review on factors associated with terrorism, Desmarais et al. (2017) found that only six studies had a control group to compare against their terrorist counterparts. More studies are gradually adopting control groups in their methodology, which would serve to increase our confidence in developing knowledge that will help to distinguish the terrorists who engage in violence from their non-violent counterparts.

1.2.5 Lack of Terrorist Profile

The last challenge would be the lack of terrorist profiles in terms of age, ethnicity, gender, or socioeconomic status. While profiles have been developed to help law enforcement agencies pinpoint a potential terrorist, it is unrealistic to imagine that radicalised individuals would have a certain appearance or physical profile that distinguishes them from the general population. Studies

have indicated that such profiles lack the benefit of scientific groundwork (Dernevik et al., 2009; Silke, 1998), and do not take into account the influence of risk factors such as ideology on an individual's radicalisation trajectory. Hence, it would be more beneficial instead to focus on the observable signs—in terms of behaviours and beliefs—that are associated with radicalisation (Borum, 2015a), as they can help us better understand the process by which an individual becomes radicalised, stay involved in terrorism, and ultimately leave it.

2. Understanding Radicalisation Models

While scholars have introduced many different models of radicalisation, one point of relative consensus is that there is no one fixed pathway to radicalisation (Borum, 2011b; Topal, 2019; Torok, 2016). The social and psychological factors that underpin the radicalisation process will vary from individual to individual, as they move from socially normative opinions and perspectives towards more extreme ones (Wilner & Duboulos, 2011). Furthermore, what might motivate someone to become involved with a terrorist group is going to be very different from the kinds of influences that motivate that same person to remain committed and engaged.

To illustrate how different variables may underpin one's involvement in terrorism, Taylor and Horgan (2006) created a conceptual framework with three broad domains—"personal factors", "setting events", and "social/ political/ organisational context" (see Figure 1). In particular, they suggest that the interaction of the variables can help explain why someone becomes involved in terrorism. Having said that, it is essential to note that not all radicalised individuals would go on to commit acts of terrorism (Schuurman & Eijkman,

2015). Most individuals who adhere to radical beliefs will not act on them.

Hence, from a law enforcement perspective, how does someone become radicalised? Is it due to a process of increasing commitment? Furthermore, can we account for those who will go on to perpetrate violence?

Figure 1
Involvement in Terrorism

Note. From “A conceptual framework for addressing psychological process in the development of the terrorist”, by M. Taylor and J. Horgan, 2006, *Terrorism and Political Violence*, 18(4), p. 591, (<https://doi.org/10.1080/09546550600897413>). Copyright 2006 by Taylor & Francis Group.

2.1 Pathway Models of Radicalisation

This section will review three major pathway models of radicalisation (for a detailed review, see Borum, 2011b) that can contribute insights to the abovementioned questions.

2.1.1 Moghaddam’s Staircase Model

Using a metaphor of a staircase, Moghaddam (2005) introduces six stages or floors to depict the psychological processes that an individual passes en route to terrorism. According to the staircase model, an individual is motivated to move from the ‘ground floor’ (“psychological interpretation of material conditions”) to the ‘first floor’ (“perceived options to fight unfair

treatment”) by feelings of perceived deprivation and grievances. If attempts to alleviate their circumstances fail, it leads to frustrations and creates the impetus for them to advance to the ‘second floor’ (“displacement of aggression”). At this floor, it is characterised by feelings of aggression targeted at the perceived enemy. The transition to the ‘third floor’ (“moral engagement”) starts when the individual begins to sympathise with terrorist groups and their radical ideology. After the individual is socialised into the terrorist group, they start to recognise the legitimacy of the group—‘fourth floor’ (“solidification of categorical thinking and the perceived legitimacy of the terrorist organisation”). Finally, they overcome any remaining barriers to action and engage in acts of terrorism—‘fifth floor’ (“terrorist act and sidestepping inhibitory mechanisms”).

The pool of radicalised individuals also become smaller as the staircase progresses. The hallmark of the model is its recognition of how psychological processes and increasing level of commitment at each level will determine if they could move onto the next level.

2.1.2 New York Police Department (NYPD)’s Four-stage Radicalisation Process

Based on an in-depth review of Al-Qaeda related cases coupled with insights gleaned from terrorism experts, Silber and Bhatt (2007) propose a four-stage radicalisation process. The “pre-radicalisation” stage details the individual’s life circumstances before they come into contact with jihadi-Salafi ideology. “Self-identification” stage is the point where the individual starts to explore jihadi-Salafi ideology and gradually begins to adopt it whilst gravitating away from their old identity. It also entails the presence of triggers that “shakes

one's certitude in previously held beliefs and opens an individual to be receptive to new worldviews" (p. 6). The third stage of "indoctrination" involves the intensification of their new worldview, leading them to embody a hardened ideological position. The individual also increases their commitment towards the in-group and starts to view militant jihad as a necessary cause to support. Finally, "jihadisation" is the stage where they make progressive plans for an attack after accepting that it is their duty to perform jihad. The hallmark of this model is the consistent four-stage radicalisation process that the authors found across their case studies.

2.1.3 Klausen et al.'s Behavioural Model of 'Homegrown' Radicalisation

Klausen et al. (2016) adapted the NYPD's radicalisation model and identified 24 observable indicators in relation to the following four stages: "pre-radicalisation" stage where the individual experiences a cognitive opening and searches for a new worldview; "detachment" stage where the individual starts to distance themselves from their old lives; "peer immersion" stage where they immerse themselves in the newfound ideology and increase their commitment to the in-group; and "steps to actions" stage where they attempt to conduct attacks or join an overseas terrorist group.

Table 2 illustrates the behavioural indicators. This model attempts to operationalise the radicalisation process by linking specific overt behaviours to each of the four stages. Klausen and colleagues argue that this approach allows users to better assess the radicalisation trajectory of terrorists as well as the time taken for them to become radicalised.

Table 2*Behavioural Indicators of Stage Progression in Radicalisation Trajectories*

Pre-radicalisation	Stage 1: Detachment	Stage 2: Peer-immersion and training	Stage 3: Planning and execution of violent Action
Description			
Searching behaviour indicative of cognitive opening.	Detachment from previous life.	Leaves home to become closer to a peer group of like-minded individuals.	Attempts or enacts violent action—or joins a terrorist group abroad or attempts to join a group.
This could include:			
Expressions of disillusionment with world affairs or with religious or political authorities.	Actively seeking get closer to new authority figures, or engaging in da'wah online or real-life.	Attempting to go abroad to join an organisation or a network to “live” as prescribed by the ideology.	Actively supporting another person carrying out violent action on behalf of the ideology.
Behaviour indicative of a personal crisis in response to personal events.	Picking fights with local mosque or teachers, colleagues, and family—or otherwise trying to convince others to change by starting a blog or a website.	Behaviour indicative of a desire to permanently join the militant community.	Issuing threats online or real-life, or in other ways supporting immediate violent action.
Seeking out information in venues outside the individuals' established social milieu, either online or real-life, from new authority figures.	Experiencing a revelation or making changes to lifestyle such as dropping out of school or work.	Seeking out ways to demonstrate commitment to the new ideological community and its mission.	Joining a foreign terrorist organisation or taking practical steps to carry out an attack.

Note. From “Toward a behavioral model of “homegrown” radicalization trajectories”, by J. Klausen, S. Campion, N. Needle, G. Nguyen, & R. Libretti, 2016, *Studies in Conflict & Terrorism*, 39(1), p. 72, (<https://doi.org/10.1080/1057610X.2015.1099995>). Copyright 2016 by Taylor & Francis Group.

2.2 Pathway Models of Online Radicalisation

Models focusing specifically on the factors and processes underpinning online radicalisation have received less research attention. As highlighted earlier, the growing literature has recognised the importance of the internet in facilitating the radicalisation process. It has made it easier for terrorists to interact with each other and with their supporters (Gill et al., 2017), disseminate their propaganda (Rieger et al., 2013), and capture the attention of their targeted audience (Neubronner, 2019). A recent systematic review also found a strong

association between exposure to radical online propaganda and the recipient's radical online and offline attitudes. Not surprisingly, there is a higher likelihood for active seekers of online propaganda to conduct physical acts of political violence (Hassan et al., 2018). Furthermore, Nuraniyah (2018) notes that online supporters of terrorist group have augmented or replaced the role of traditional recruiters by developing a close relationship with potential recruits on the internet—characterising a bottom-up, peer-to-peer form of recruitment. In other words, it is vital to understand how the person and their online environment interact and influence their radicalisation process.

2.2.1 Weimann and von Knop's Five-phase Process

A five-phase model was introduced by Weimann and von Knop (2008) to explain why terrorist online narratives may influence some individuals. If the narratives managed to address the individual's emotional needs, they would then progress in their radicalisation pathway. The five phases are: “searching phase” where the individual develops the motivation—driven by their emotional needs—to search for answers that can address their needs; “seduction phase” where they are exposed to propaganda materials disseminated online by terrorist groups; “captivation phase” where the individual finds and connects with like-minded others in the terrorist online community; “persuasion phase” where they actively participate in activities and conversations within the online community; and finally the “operation phase” where they start participating in the operational activities of the terrorist group. By highlighting the interactions between the individual and the online community, this model helps researchers to conceptualise and aggregate factors associated with online radicalisation.

2.2.2 Neo's RECRO Model of Internet-mediated Radicalisation

Building upon the framework by Weimann and von Knop (2008), the RECRO model was proposed by Neo (2016) to incorporate psychological processes into the online radicalisation pathway. The “reflection phase” details the period where the individual begins to ‘open-up’ and search for new beliefs as their extant worldviews are inept in explaining their current circumstances. The “exploration phase” involves the individual appraising the terrorist narratives that they found online, and making sense of them. The individual may start to interact with like-minded others and form a new identity around that of the terrorist online communities in the “connection phase”. This is the point where they become supporters of a terrorist group. Following which, in the “resolution phase”, they may encounter triggers (e.g., call-for-actions) that provide the impetus for the supporters to act on their radical beliefs. The individual becomes mentally prepared to contribute to the group’s cause either in the online or offline setting in the “operational phase”, and to start preparing for it. The crux of this model is that it places emphasis on identifying potential risk factors within each phase, making it relevant for conducting online risk assessment.

2.2.2.1. Case of Younes Tsouli. Younes Tsouli was the first in the United Kingdom to be prosecuted for inciting terrorism using the internet (Holden, 2007). Using the username of ‘irhabi007’, Tsouli published manuals on hacking and uploaded terrorist videos and propaganda, and became an administrator of a key online forum (Bowman-Grieve, 2015). Table 3 illustrates the radicalisation process of Tsouli using the RECRO model.

Table 3*Mapping RECRO Pathway Framework to Younes Tsouli*

Phase	Factors	Case of Younes Tsouli
Reflection	The triggers, needs, and vulnerabilities that an individual may have, which increase their receptiveness towards alternative belief systems.	<ul style="list-style-type: none"> • Strong sense of loneliness. He was an immigrant to the U.K. (Corera, 2008). • His need for affiliation may have propelled him to search for immediate religious companionship and guidance online.
Exploration	The period where the individual begins making sense of the online information put forth by terrorists.	<ul style="list-style-type: none"> • While surfing the internet, Tsouli viewed footage of innocent Iraqi civilians being killed in Fallujah, Iraq (Corera, 2008). These experiences presumably incited moral outrage within him. • He perceived that change is not possible in the existing society and began to accept that radical change using violence is necessary.
Connection	The influence of like-minded individuals in the terrorist online community.	<ul style="list-style-type: none"> • Using the alias 'irhabi007', Tsouli was an active participant on many online forums. • Tsouli successfully helped Al-Qaeda solve their problems to distribute videos with large file sizes (Corera, 2008). As a result, he became an active link (in-group) between the group and the wider online communities of Al-Qaeda supporters. • Tsouli started to attract the attention of the authorities after he hacked into the official website of the state of Arkansas and posted terrorist propaganda there (Corera, 2008).
Resolution	The period during which the individual gains the momentum to translate one's radical beliefs into action.	<ul style="list-style-type: none"> • Tsouli knew that the authorities were monitoring him, and he was proud that he had yet to be apprehended, even taunting those who were monitoring his activity. • He had grown "enamoured of his own reputation" and was motivated to maintain his status within the radical enclave (Corera, 2008).
Operational	The period during which the individual is ready to commit violence to further the group's cause both online and/or offline.	<ul style="list-style-type: none"> • Tsouli encouraged others to conduct attacks and guided them to bomb-making websites (Sageman, 2008). • At the time of his arrest, he was in the process of creating a website called 'YouBombIt' to encourage others to become suicide bombers (Corera, 2008).

2.3 Operationalising Radicalisation Models

The above review of radicalisation models, albeit not comprehensive, draws our attention to two observations. First, radicalisation is a process where the individual moves from a socially normative perspective towards more extreme ones, and in some cases, culminates in acts of terrorism. Thus, the

models allow us to track the progression (i.e., is the person becoming more radical over time) of a person-of-interest over time using the depicted stages as a guide.

Table 4
Pathway Models of Radicalisation

Author	Cyber focused	Stages or factors
Moghaddam (2005)	No	<ol style="list-style-type: none"> 1. Psychological interpretation of material conditions 2. Perceived options to fight unfair treatment 3. Displacement of aggression 4. Moral engagement 5. Solidification of categorical thinking and the perceived legitimacy of the terrorist organisation 6. The terrorist act and sidestepping inhibitory mechanisms
Silber and Bhatt (2007)	No	<ol style="list-style-type: none"> 1. Pre-radicalisation 2. Self-identification 3. Indoctrination 4. Jihadisation
Klausen et al. (2016)	No	<ol style="list-style-type: none"> 1. Pre-Radicalisation 2. Stage 1: Detachment 3. Stage 2: Peer-immersion and training 4. Stage 3: Planning and execution of violent action
Weimann and von Knop (2008)	Yes	<ol style="list-style-type: none"> 1. Searching phase 2. Seduction phase 3. Captivation phase 4. Persuasion phase 5. Operation phase
Neo (2016)	Yes	<ol style="list-style-type: none"> 1. Reflection: Triggers, needs, and vulnerabilities 2. Exploration: Making sense of new information 3. Connection: The influence of online community 4. Resolution: Re-triggering the need for action 5. Operational: Preparing and contributing to cause

Second, there is a myriad of pathways into radicalisation, which makes it hard to ascertain the ‘best’ model. Nevertheless, it seems apposite to utilise these models as a starting point to identify relevant risk factors and their associated indicators within each stage of the online radicalisation process. The focus is, therefore, on the extraction of online-centric factors and indicators that are suggestive of an individual’s progression in their radicalisation pathway. A growing number of studies (e.g., Dean, 2014; Innes et al., 2007; King & Taylor, 2011; Saifudeen, 2019; Tan, 2006) have utilised this approach to discern common factors, some of which were elaborated earlier (see Table 4 for a summary). Such insights are highly relevant for the objective of this thesis,

which is to derive a set of factors and indicators to detect radicalisation in social media posts. However, most of the models were developed using a small number of cases, and as Schmid (2013) argues, limit the utility and generalisability of the identified factors.

3. Extrapolating Insights from Theories of Online Radicalisation

Instead of attempting to develop pathway models, some researchers have proposed theories to explain the phenomenon of online radicalisation. The following are summaries of selected theories that can add to our knowledge about detecting online radicalisation.

3.1 Torok's Explanatory Model for Online Radicalisation

Torok (2013) attempted to develop an explanatory model of online radicalisation by consolidating common characteristics of what shapes the process. Drawing heavily on Foucault's approach on psychiatric power (see Foucault, 2008) and her own analysis of terrorists' social media accounts, Torok emphasises how exposure to terrorist online content would influence the power relationship between an individual and the terrorist group, which over time normalises radical thinking and behaviour. In particular, she highlights three assumptions: as an institution, online terrorist communities—i.e., platforms and content—serve to narrow the range of discourses experienced by the individual; individuals are repeatedly exposed to radical narratives that are lauded as the truth; and their radical worldviews are reinforced by the discussions that they have with like-minded others in the online communities. In other words, the whole network of discourses within the terrorist online community not only plays an essential role on the process of online

radicalisation, but it also highlights the potential utility that reactions to the online discourses could be used to inform one's risk for radicalisation.

3.2 Shortland's Approach to Online Risk Assessment of Terrorists

To overcome the research lacuna on online risk assessment of terrorists, Shortland (2016) recommends integrating lessons learnt from three research domains. The first domain that Shortland suggests delving into is that of models underlying terrorism risk assessment tools such as VERA-2 (see Pressman & Flockton, 2012). Previous research on risk assessment of terrorism has determined a spectrum of factors and indicators that can be used to assess the risk of an individual becoming radicalised online. The next recommended domain concerns the influence of radical online propaganda on the radicalisation process. The changes in the individual's belief and online behaviour—whilst they engage with terrorist narratives in online propaganda materials—provide an indirect measure of the risk that they would pose. Finally, the last domain on 'risk assessment online' purports the need to synthesise knowledge that researchers from other disciplines have amassed in their efforts to detect non-terrorism related online vices. For example, Shortland recommends looking at how contact and non-contact offenders of indecent images of children (IIOC) were identified and evaluated based on their online behaviours (see Seto et al., 2011). The key then is to extrapolate lessons from these domains to identify relevant factors and indicators and have them validated via empirical means.

3.3 Neo et al.'s Model for Assessing Risk of Radicalisation via the Internet

Neo et al. (2017) offer four considerations which not only enhance our understanding of the progress of online radicalisation but also guide the

identification of relevant factors and indicators. The first consideration of “individual” examines the motivations and belief systems that spur an individual to engage in behaviours related to online radicalisation (e.g., postings on perceived grievances). Motivations can come in many forms, and they provide important clues about an individual’s receptivity towards terrorist narratives. The second consideration of “online environment” delineates the informational, instrumental, and emotional support that the internet confers on the individual, whilst they interact with radical content and like-minded individuals online. The third consideration is the “interactions between individual and the online environment”. Factors within this consideration are constructed based on how individuals interact in the terrorist online communities. Finally, the last consideration of “protective element” examines the factors that reduce the likelihood of an individual progressing in their radicalisation pathway. The theoretical argument is that not all individuals become radicalised after being exposed to radical online propaganda.

3.4 Bayerl et al.’s Radicalisation-factor Model

In a similar model, Bayerl et al. (2020) highlight the problem of developing models of online radicalisation around a single domain and propose four key interlinked domains to constitute a holistic representation of online radicalisation. The first domain concerns the “individual”, where demographic (e.g., age) and person-centric factors (e.g., perceived grievances) would contribute to their vulnerability towards radicalisation, and shape the expression of their online behaviours (e.g., the online communities that they would join). Next, the “online environment” within which the terrorist groups operate plays a role in propagating and amplifying the reach of their radical narratives. The

third domain addresses the type of “radical ideology” that an individual may encounter. These ideologies can range from jihadi to right- or left-wing. Given that certain ideologies increase one’s propensities towards adopting certain types of *modus operandi*, targets, etc., this knowledge can be used to predict their radicalisation trajectory. The last domain on “technologies” relates to how terrorist groups have exploited technological affordances such as anonymity, ease of creating and propagating radical beliefs, the unprecedented access to new audiences, to recruit new members via the internet. In particular, the authors stress the importance of understanding the interactions between these four domains, and to identify relevant factors and indicators in each of them.

Table 5
Compilation of Research Themes

Theme	Torok (2013)	Shortland (2016)	Neo et al. (2017)	Bayerl et al. (2020)
Person-centric	Individual reaction to radical ideologies	Risk assessment online Terrorism risk assessment	Individual consideration	Individual domain
Psychosocial	Interactions within the terrorist online communities Influence of terrorist online communities	Terrorism online	Online environment consideration Interactions between individual and the online environment	Online environment domain Technologies domain Radical ideologies domain
Protective	—	Terrorism risk assessment	Protective element	—

3.5 Summary

Instead of fixating on the processes of online radicalisation, the reviewed theories offer a framework within which factors and indicators can be conceived. On their own, each model offers valuable insights to guide risk assessment of online radicalisation. However, taken together, certain overarching themes (see Table 5) emerge, indicating some form of consensus

within the literature. The three distinct yet interrelated themes (person-centric, psychosocial, protective) will be explained in more detail shortly.

4. A Framework for Analysis: Person-centric, Psychosocial and Protective Dimensions

On the basis of the common stages found amongst the models of radicalisation and insights gleaned from theories of online radicalisation, this section presents a theoretical framework (see Figure 2). This framework forms the basis for this thesis and the subsequent identification and validation of factors for detecting online radicalisation and their associated indicators. The factors under the ‘person-centric’ dimension capture the characteristics of the radicalising individual (e.g., motivations, values, attitudes, belief systems) as explanations for getting involved in terrorism. The ‘psychosocial’ dimension emphasises factors that encapsulate the online behaviours and changes in cognition due to the individual’s interactions within the terrorist online communities. Finally, the ‘protective’ dimension consists of factors that reduce one’s risk of becoming radicalised.

Figure 2

Framework for Detecting Markers of Radicalisation in Social Media Posts

4.1 Person-centric Dimension

There is ample evidence of the importance of individual-level risk factors. Certain internal characteristics (e.g., motivation, values, immediate

experiences, beliefs, abilities, emotional state) of the individual actor have been found to be associated with involvement in terrorism. These characteristics may shape an individual's level of susceptibility towards terrorist narratives (Borum, 2011a; Edwards & Gribbon, 2013).

For a start, studies that examine terrorists' motivations and worldviews are particularly relevant to the present endeavour. Through systematic reviews and interviews with captured terrorists, researchers have identified a wide range of motivations for supporting terrorist groups. Hu (2016) identified five underlying psychological motivations that Singaporean detainees espouse in their support for the ISIS cause. They are "justifying violence, romanticising the notion of a utopian state, desire to be a 'good' Muslim, escaping the 'unbearable present' world, and existential anxiety in relation to End Times prophecies" (p. 168). Similar motivations were also derived from research on Western ISIS foreign fighters (Callimachi, 2015), women who join ISIS (Gan et al., 2019), as well as terrorists in general (Borum, 2014).

Another often-cited motivation is that of perceived injustice. In some cases, the innate need to address the perceived injustice—due to a sense of deprivation that their in-group is being unfairly treated and discriminated against—may motivate individuals to look for avenues to alleviate the perceived imbalance in the situation (King & Taylor, 2011; McCauley & Moskaleiko, 2008; Moghaddam, 2005). Terrorist groups have been known to exploit such opportunities and create narratives that ride on the grievances caused by these injustices. Terrorist groups would also prescribe solutions that can mitigate these injustices. For instance, Jemmah Islamiyah recruits in Singapore were recruited partly due to their interest in the plight of Muslims

suffering in countries such as Palestine and Afghanistan (Tan, 2006). However, the intensity of one's reaction to the terrorist narratives is affected by how much the described injustice resonate with their life experiences and sense of self (Borum, 2014).

Other significant person-centric factors include moral disengagement (Bandura, 2004), and the need for closure (Kruglanski et al., 2006). Moral disengagement refers to the changes in one's moral principles on the use of violence as a result of them internalising the radical rhetoric. Recent empirical findings on moral disengagement reaffirm its role as an antecedent for sidestepping our internalised moral standards (Moore, 2015). For example, Brenton Tarrant, the perpetrator of the Christchurch shooting, attributed his act of mass-shooting as a mean to protect his in-group: "I am just a regular White man, from a regular family. Who decided to take a stand to ensure a future for my people" (Tarrant, 2019). On the other hand, the need for closure may increase the willingness of an individual to explore new worldviews given that their existing belief systems were unable to provide a satisfactory explanation of their current life predicaments. If the ideology purported by the terrorists can offer solutions to the issues faced, the individual may start to 'open-up' to these radical ideas and over time, change the way they behave and think (Venhaus, 2010).

In sum, there are many different individual-level factors that can predispose one to the orchestrations of terrorist actors, and are operationalised by the individual's motivation, capability, values, and worldview. These can manifest in the individual's online expressions and behaviours, which can be

deciphered by law enforcement to detect and assess the risk for online radicalisation.

4.2 Psychosocial Dimension

The internet creates an environment in which terrorists can interact and engage with their supporters. In this sense, the factors that impinge on these social interactions play an essential role in the detection of online radicalisation.

Three psychosocial themes that can abet the development of relevant factors and indicators for online radicalisation have been identified. Firstly, as highlighted earlier, the internet makes it easier for an individual to gain access to radical propaganda and link up with a terrorist group. This aids in cultivating partisanships and providing the necessary sounding boards for potential recruits to connect their budding intentions to an ideological cause or a plan of action (Böckler et al., 2015). Such social online communications can be explicit (e.g., become a formalised member of a Facebook group) or implicit (e.g., likes, comments, and sharing of information) in nature (Bartlett & Miller, 2013). Such observations are also made by van Buuren (2012) who noted that lone-wolf actors would perceive themselves to be part of a larger global entity that is connected by a shared common identity, such as ideology. For example, right-wing lone-wolf perpetrators are known to encourage each other to conduct attacks, and are inspired by each successful right-wing attack (e.g., the 2019 Christchurch shooting, the 2019 El Paso shooting) as well as the online manifestos that were disseminated by the perpetrators (Neo, 2020). Within this context, Hussain and Saltman (2014) point out that the newly formed relationships in these online communities often compensate for the individual's

deficient offline social networks. Potential psychosocial factors can, therefore, focus on deciphering the interactions between such individuals.

Secondly, the terrorist online communities act as echo chambers to reinforce the radical narratives as well as to acclimatise their members to new social norms, identity, and behaviours expected of terrorist groups' supporters (Caiani & Kröll, 2015). In the process of interacting with like-minded others, the individual may start to adopt a polarised worldview in favour of the terrorist groups, and re-position their actions and thoughts around the newly internalised worldview. As part of their influence strategy, terrorist groups have also propagated a large number of their narratives online. Through sheer quantity, these narratives can easily dominate the individual's informational sphere, giving the false impression of being the 'majority' narrative and appearing to have 'social proof' (Pamment et al., 2018). By exploiting such cognitive biases, terrorist groups can nudge the individual to believe or behave in certain ways, underlining why online echo chambers are particularly integral for online radicalisation. For example, el-Said and Barrett (2017) found that the ISIS online network has a strong influence on the radicalisation trajectory of its foreign fighters:

The would-be FTFs [foreign fighters] appeared to turn to the internet to confirm and strengthen ideas, perceptions and narratives [information about the conflict in Syria] that they had already developed or were beginning to develop. The internet then played a key role in reinforcing a decision that had in part been taken already. This seemed particularly true when the process was also associated with friendship or network ties. (p. 39)

Hence, potential psychosocial factors can focus on digital footprints that reflect the individual's increasing commitment (e.g., attempts to proselytise to others, praising terrorist groups) to the terrorist online communities.

Lastly, emblematic of the 'us-versus-them' mentality, research has shown how the propagation of radical narratives can create an environment conducive for discrimination and intergroup hostility (Reicher et al., 2008). This involves defining an in-group and categorising others that do not share the same membership as the out-group. Members of the in-group tend to be portrayed with good qualities such as honourable and virtuous. In contrast, the out-group is often depicted as being problematic by virtue of their inherent characteristics (e.g., aggressive, deviousness), and that their existence would threaten the survival of the in-group (Levine et al., 2005; Soral et al., 2018). This has several implications. For example, Swann et al. (2010) noticed that people have a higher likelihood of protecting the integrity of the in-group if they espoused a high level of identification with the group. The terrorist online communities would also engage in what Noor et al. (2012) called 'competitive victimhood' where the terrorists portray themselves as the real victims, thereby creating a legitimate justification for retaliating against the out-group. Furthermore, this inevitably fuels a process of 'othering' where individuals perceive the need to eliminate the out-group in order to restore balance and justice to their lives (Loadenthal, 2019). This kind of labelling, as Berger (2018) argues, is typically needed before an individual can move from a stage of radical beliefs to a stage of radical actions, including violence. Given that research, such as Matsumoto et al. (2015), has found a relationship between words that evoke anger, contempt, and disgust (commonly found in radical

narratives), and intergroup hostility and political violence, progress can be made by developing factors that capture these negative emotions expressed by individuals in their online postings. In sum, the relevant psychosocial factors and indicators can be operationalised by features that characterise group interactions, group identity, and group communication.

4.3 Protective Dimension

The detection of radicalisation in social media posts should not focus specifically on identifying risk factors of concern, but also to detail the protective factors (de Ruiter & Nicholls, 2011; Lloyd, 2019). The evidence base underpinning our understanding of protective factors has grown over the last decade as researchers started to delve into the areas of deradicalisation and disengagement (Hettiarachchi, 2018; Horgan et al., 2017). Cragin (2014), for example, notes that not everyone becomes a terrorist despite being exposed to the same enabling environments. This finding is also relevant to the online sphere (Archetti, 2015). Research has suggested that only a small percentage of those drawn towards terrorist ideology, would end up committing physical acts of terrorism (Aly et al., 2014; Leuprecht et al., 2010). It could, therefore, be argued that there are protective factors that buffer against the risk of someone becoming radicalised online.

Some terrorism risk assessment tools have included protective factors as part of their assessment framework. For example, VERA-2 (Pressman & Flockton, 2012) contains six protective factors and they are: “re-interpretation of ideology less rigid, absolute”; “rejection of violence to obtain goals”; “change of vision of enemy”; “involvement with non-violent, de-radicalisation, offence-related programs”; “community support for non-violence”; and “family

support for non-violence”. These factors are associated with the changes in the individual’s mindset as well as external social support by their loved ones and/or the community.

In the context of online radicalisation, these protective factors could similarly be focused on the individual’s characteristics and/or the online environment. For the former, these can be observed through the individual’s online postings that challenge the terrorist group’s ideology or its use of violence. Kruglanski et al. (2018) explain that terrorist who becomes disillusioned with the group’s strategy or indiscriminate use of violence would often leave the group. There is also growing evidence that terrorists may leave the group because of their changing life priorities (Bjørge, 2009), and them developing an appreciation for diversity (Barrelle, 2015).

For the latter, protective factors can refer to online expressions of concerns about sanctions from social media companies, as well as the fear of being tracked and incarcerated the authorities (Lucas & Aly, 2015; Menn & Volz, 2016). These technological barriers may force individuals to disengage from the terrorist online communities. Furthermore, individuals may complain about the lack of opportunities, specifically in terms of connecting with the ‘right’ entities within the online terrorist communities. For example, de Bie et al. (2015) observe:

Regardless of social media’s potential, the search for social facilitators is not always successful. Some subjects have the ambition to travel to Syria, but do not know whom to consult specifically. They therefore make a public appeal to brokers in conflict areas by posting a call for help on social media and even by approaching them directly by e-mail. (p. 14)

In other words, the absence of a motivating factor (e.g., the ability to connect with like-minded individuals) can in itself be a source of protection. In sum, the presence of protective factors may reduce an individual's motivation or capacity to offend, thereby influencing the outcome of the online radicalisation process.

5. Summary of Insights from Literature

This literature review has found that online radicalisation is the product of many factors, namely the individual and their personal attributes (e.g., motivations, values, belief systems), and the internet as the platform that facilitates and supports the interactions between the individual and the terrorist online communities. This literature review has identified the following key insights:

- a) Psychological and communication literature has provided supportive findings that can be extrapolated to identify individual who may be radicalised based on their open-source digital footprints.
- b) Research suggests that three types of warning signs, namely, “leakage”, “identification”, and “fixation” warning behaviours have the highest likelihood of being discovered in digital communication.
- c) In order to enhance our capability to detect potential cases of online radicalisation, there is a need to address five challenges: radicalisation is a low base-rate event; ensure the quantity and quality of terrorist online content; need to identify relevant factors and indicators; identify the right control group; and do not fixate on identifying a terrorist profile.

- d) Online radicalisation is a process where the individual moves from socially normative perspectives towards more extreme ones, and in some cases, culminates as acts of terrorism.
- e) The stages of the radicalisation models serve as a useful starting point for identifying relevant risk factors because they allow us to track the progression of an individual (i.e., is the person becoming more radical over time) and for determining what online behaviours and expressions to expect.
- f) Online radicalisation theories point to the presence of overlapping research domains that can be used to guide the risk assessment of online radicalisation.

On the basis of the recurring stages found amongst the reviewed models of radicalisation, coupled with insights from theories of online radicalisation, a theoretical framework was proposed. It consists of three distinct yet interrelated dimensions: person-centric dimension, psychosocial dimension, and protective dimension. The ‘person-centric’ dimension capture the characteristics of the radicalising individual (e.g., motivations, values, attitudes, belief systems) as explanations for them to become involved in terrorism. The ‘psychosocial’ dimension encapsulates the online behaviours and changes in cognition due to the individual’s interactions within the terrorist online communities. The ‘protective’ dimension consists of factors that reduce one’s risk of becoming radicalised online. This framework will form the basis for the rest of the thesis and be used to inform the selection of relevant factor and indicators.

CHAPTER THREE: IDENTIFICATION OF PERSON-CENTRIC AND PSYCHOSOCIAL RISK FACTORS, AND PROTECTIVE FACTORS¹

The internet has become one of the most important arenas for terrorists to spread their messages and to radicalise recruits. The growth in numbers of self-radicalised individuals—facilitated by the internet—and the rising urgency to detect and takedown radical content on social media make the identification of factors and indicators to detect online radicalisation a timely pursuit.

Despite the growing demand, there is a paucity of research on risk assessment instruments that are designed specifically for detecting online radicalisation (Khader, 2016). To further confound issues, the low base-rate of online radicalisation coupled with the vast range of potential cyber-related behaviours and expressions associated with online radicalisation, make research on the topic extremely daunting.

Existing terrorism risk assessment tools could provide insights on the difficult task of ascertaining the relevant factors and indicators for an instrument to detect online radicalisation. In recent times, many terrorism risk assessment tools have been created, of which Lloyd (2019) reviewed six commonly used tools: Extremism Risk Guide (ERG 22+), Islamic Radicalisation (IR-46), Identifying Vulnerable People (IVP), Multi-Level Guidelines (MLG), Terrorist Radicalisation Assessment Protocol (TRAP-18), and Violent Extremism Risk Assessment-2 (VERA-2). Given that the factors within these tools were developed based on the creators' empirical research and interviews with terrorist offenders, they have some form of validity, thereby

¹ An earlier version of this chapter was presented at the 'Global Asia in Interdisciplinary Perspectives: Sustainability, Security, and Governance Conference' at Nanyang Technological University, Singapore, November 17, 2018.

making them an ideal starting point to identify factors and indicators for online radicalisation. The alternative would be to conduct an in-depth literature review (see Tranfield et al., 2003) to appraise various studies on risk factors for online radicalisation.

Figure 3

The Research Process to Identify the Factors and their Associated Indicators

To address the research gap, a modified Delphi technique (with seven Singapore subject-matter experts [SMEs] in the field of terrorism) combined with a literature review on risk factors for online radicalisation was used to construct a list of person-centric and psychosocial risk factors, and protective factors and their associated indicators. A similar approach was also used by Post et al. (2002) in their attempt to measure the risk that a terrorist group would pose. Figure 3 outlines the research process for this chapter.

In terms of factor and indicator development, Schuurman and Eijkman (2015) suggest that it is useful to tap on and incorporate the knowledge and experience of terrorism practitioners. Hence, the SMEs' opinions on the relevance of the factors from extant terrorism risk assessment tools for identifying factors for online radicalisation was sought. In my view, the existing

tools provide relevant data points for this study—i.e., to develop a cyber-focused risk assessment—as they were created based on in-depth literature review and the creators’ professional experience. Additionally, the parallel literature review of the relevant research publications served to complement the results from the expert panel by contextualising the identified factors to extant research, and in the process, identify meaningful factors and indicators of interest.

1. Modified Delphi Technique

In the 1950s, Olaf Helmer and Norman Dalkey developed the Delphi technique at the RAND Corporation. This is a type of research methodology used to gather knowledge from SMEs on a specific topic of interest (Dalkey & Helmer, 1963; Linstone & Turoff, 2002). It is an iterative process designed to collect—usually via surveys that are interspersed with feedback—and achieve a convergence of opinions from SMEs. The process stops when consensus is achieved, suggesting that the SMEs had agreed upon a collective solution to the research question. This methodology is beneficial for research areas where there is a paucity of information about a problem or phenomenon (Thangaratinam & Redman, 2005). For example, this research method has been deployed to establish the criteria for inappropriate prescriptions for elderly patients (Rognstad et al., 2009), select healthcare quality indicators (Boulkedid et al., 2011), determine research priorities for orthopaedic oncology (Schneider et al., 2016), identify future trends and projections (Tapio et al., 2011), formulate guidelines and standards in educational settings (Green, 2014), and develop a framework to analyse the risk a terrorist group would pose (Post et al., 2002).

While similar research methodologies such as Q-sort (see Stephenson, 1953) have been utilised in terrorism research (e.g., Koçak, 2012; Sezgin, 2007), the Delphi technique was chosen for two reasons. Firstly, I wanted to ride on the expertise of the SMEs to create a point of comparison for identifying relevant factors. Secondly, terrorism researchers such as Post et al. (2002) have already successfully utilised the Delphi technique to identify indicators, providing precedence for the use of this method in answering similar questions.

Utilising a three-round modified Delphi technique, seven local terrorism SMEs were asked to evaluate factors—obtained from six terrorism risk assessment tools—that are relevant and important to the endeavour of identifying radicalisation in social media posts. In the conventional Delphi technique, an open-ended questionnaire would be used to elicit responses from the experts on what they perceived to be factors important to the topic of interest. However, in this case, it was decided that the SMEs would instead provide their opinions on factors obtained from terrorism risk assessment tools. This flexibility to adapt the Delphi technique to the specific requirements of the study is one of the main advantages that has prompted many researchers to utilise it (Hirschhorn, 2019).

1.1 Expert Panel Selection

There are no standardised criteria in terms of the size for the expert panel. Studies involving the Delphi technique have utilised panel size that ranged from four experts (Gustafson et al., 1973) to 171 experts (Roberson et al., 2005). Adler and Ziglio (1996) highlight four considerations to guide the selection of an appropriate panel size: the participant is an SME in the subject

of investigation; they are willing to participate in the study; they have the bandwidth to complete the study; and they can communicate effectively.

In the present case, a panel of seven local SMEs was convened, and they fulfilled the above-mentioned considerations. The panellists were either practitioners or academics within Singapore, working in their own capacity on the topic of online radicalisation. Three panellists held doctorates of philosophy degrees, three held master degrees, and one of them was a candidate in a doctoral program. Four of them were employed in a think tank specialising in national security (they are actively involved in identifying and monitoring terrorist activities on the internet), and the rest worked for the government in the areas of terrorism and resilience. Two panellists had three years of experience in their current position, two had more than five years, and the remaining three panellists had more than ten years of experience. All of them had actively published on the topic in the form of peer-reviewed journals and book chapters, and presented their findings at many international conferences. These SMEs were invited via email to participate in the research. They participated voluntarily and were not representing their institutions or government agencies.

1.2 Research Design

An overview of the research design is presented in Figure 4. It involved three rounds of data collection with a panel of seven SMEs. The panel members were blinded to each other's identity and were systematically queried and re-queried about their responses via email.

Figure 4
The 3-round Modified Delphi Technique

Note. Seven SMEs in the field of terrorism were systemically asked to evaluate factors that are relevant and important to the endeavour of detecting radicalisation in social media posts.

1.2.1 Creation of Survey Items

Based on my search of the terrorism literature in 2017, a total of eight terrorism risk assessment tools were identified. After an initial screening of the tools, six of them were selected based on three criteria. Firstly, the tool must be developed to provide an assessment of an individual's level of radicalisation or involvement in terrorism. Secondly, the tool must contain factors and indicators that guide users to determine the risk level. Finally, the tool must have been developed recently—after 2010—and published in peer-reviewed literature.

Two tools (Risk Assessment for Violent Extremists [RAVE; Dean, 2014]; Islamic Radicalisation [IR-46; see Lloyd, 2019]) were not included as there was a lack of relevant information about their usage and effectiveness at the time of analysis (see Figure 5). The remaining six tools are ERG 22+ (used in England and Wales), IVP (used in the United Kingdom, Canada, and the United States), TRAP-18 (used in Canada, the United States, and Europe), MLG (used in North America and Europe), VERA-2 (used in Europe, North America, Australia, and

Southeast Asia), and Cyber-VERA. Table 6 details the factors found in the six terrorism risk assessment tools.

Figure 5
Sampling Procedure for Creating the Survey Items

To construct the items for the modified Delphi technique, all the factors from the six terrorism risk assessment tools were collated. This resulted in an initial list of 132 factors. Similarly defined factors from different tools were grouped together—refer to Appendix A for the detailed breakdown. For example, “personal grievance and moral outrage” from TRAP-18, “perceived grievance” from MLG, and “victim of injustice and grievances” were grouped under the heading “need to redress injustice and express grievance”. Another example would be that of the combined heading of “family or friends support terrorist offending”. This was made up of “negative peer influences” from IVP, “network (family, friends) involved in violent action” from VERA-2, and “family or friends support extremist offending” from ERG 22+. After this step, a final survey—see Appendix B—containing a list of 67 factors was compiled.

Table 6*Terrorism Risk Assessment Tools included in the Modified Delphi Technique*

Tool	Authors	Description	Domains	Items
Extremism Risk Guidelines (ERG 22+)	Lloyd and Dean (2015)	It is a risk assessment tool developed by the National Offender Management Service in the United Kingdom. Practitioners, in England and Wales, use it to identify the pathway and motivations of those convicted of engaging in terrorist activities, in order to better inform interventions for disengagement and desistance.	Engagement	<ol style="list-style-type: none"> 1. Need to redress justice and express grievances 2. Need to defend against threat 3. Need for identity, meaning, belonging 4. Need for status 5. Need for excitement, comradeship or adventure 6. Need for dominance 7. Susceptibility to indoctrination 8. Political/Moral motivation 9. Opportunistic involvement 10. Family or friends support extremist offending 11. Transitional periods 12. Group influence and control 13. Mental health
			Intent	<ol style="list-style-type: none"> 1. Over-identification with a group or cause 2. Us and Them thinking 3. Dehumanisation of the enemy 4. Attitudes that justify offending 5. Harmful means to an end 6. Harmful end objectives
			Capability	<ol style="list-style-type: none"> 1. Individual knowledge, skills and competencies 2. Access to networks, funding and equipment 3. Criminal history
				+ Any other factor
Terrorist Radicalisation Assessment Protocol (TRAP-18)	Meloy et al. (2015)	The creators combined the typology of eight warning behaviours with ten distal characteristics to develop the TRAP-18. This threat assessment tool has also incorporated insights from empirical studies and the authors' case experience of dealing with lone-wolf terrorists. This tool is used in Canada, the United States, and Europe.	Warning behaviours	<ol style="list-style-type: none"> 1. Pathway warning behaviour 2. Fixation 3. Identification 4. Novel aggression 5. Energy burst 6. Leakage 7. Last resort 8. Directly communicated threat
			Distal characteristics	<ol style="list-style-type: none"> 1. Personal grievance & moral outrage 2. Framed by an ideology 3. Failure to affiliate with an extremist group

Table 6 (continued)

Tool	Authors	Description	Domains	Items
(TRAP-18)			Distal characteristics	4. Dependence on the virtual community 5. Thwarting of occupational goals 6. Changes in thinking & emotion 7. Failure of sexual-intimate pair bonding 8. Mental disorder 9. Creativity & innovation 10. Criminal violence by history
Violent Extremism Risk Assessment 2 (VERA-2)	Pressman and Flockton (2012)	It is designed as a risk assessment tool for the correctional settings. It seeks to evaluate individuals convicted of terrorism-related offences, and assess their risk of re-offending and determine the nature of interventions required in custody. This tool is used in Europe, North America, Australia, and Southeast Asia.	Beliefs and Attitudes	1. Commitment to ideology justifying violence 2. Victims of injustice and grievances 3. De-humanisation/ demonisation of identified targets of injustice 4. Rejection of democratic society and values 5. Feelings of hate, frustration, persecution, alienation 6. Hostility to national collective identity 7. Lack of empathy, understanding outside own group
			Context and Intent	1. Seeker, consumer, developer of violent extremist materials 2. Identification of target (person, place, group) in response to perceived injustice 3. Personal contact with violent extremists 4. Anger and expressed intent to act violently 5. Expressed desire to die for cause or martyrdom 6. Expressed intent to plan, prepare violent action 7. Susceptible to influence, authority, indoctrination
			History and Capability	1. Early exposure to pro-violence militant ideology 2. Network (family, friends) involved in violent action 3. Prior criminal history of violence 4. Tactical, paramilitary, explosives training 5. Extremist ideological training 6. Access to funds, resources, organisational skills
			Commitment and Motivation	1. Glorification of violent action 2. Driven by criminal opportunism 3. Commitment to group, group ideology 4. Driven by moral imperative, moral superiority 5. Driven by excitement, adventure
			Protective	1. Re-interpretation of ideology less rigid, absolute 2. Rejection of violence to obtain goals 3. Change of vision of enemy

Table 6 (continued)

Tool	Authors	Description	Domains	Items
(VERA-2)			Protective	4. Involvement with non-violent, de-radicalisation, offence-related programs 5. Community support for non-violence 6. Family support for non-violence
Identifying Vulnerable People (IVP)	Egan et al. (2016)	The IVP is used to identify serious violence in persons convicted or killed in the process of committing a terrorist offence using open-source intelligence. This tool is used in the United Kingdom, the United States, and Canada.	—	1. Cultural and religious isolation 2. Isolation from family 3. Risk taking behaviour 4. Sudden change in religious practice 5. Violent rhetoric 6. Negative peer influences 7. Isolated from peer group 8. Hate rhetoric 9. Political activism 10. Basic paramilitary training 11. Travel/ residence abroad 12. Death rhetoric 13. Extremist group membership 14. Contact with known recruiters and extremists 15. Advanced paramilitary training 16. Overseas combat
Multi-Level Guidelines (MLG)	Cook (2014)	The MLG is a risk assessment tool designed for the assessment and management of group-based violence. This tool is used in North America and Europe.	Individual	1. Violent behaviour 2. Escalation in violent behaviour 3. Nonviolent criminal behaviour 4. Problems resulting from victimisation 5. Mental health problems 6. Lack of pro-social integration
			Individual-group	1. Group-based identity 2. Violent role or status in group 3. Commitment to group 4. Negative attitudes toward out-group
			Group	1. Group violence 2. Escalation of group violence 3. Violent group norms 4. Group cohesion 5. Strong violent leadership 6. Isolative group

Table 6 (continued)

Tool	Authors	Description	Domains	Items
(MLG)			Group-societal	<div>1. Intergroup threat</div> <div>2. Perceived injustice</div> <div>3. Extreme social status of the group</div> <div>4. Social instability</div>
Cyber-VERA	Pressman and Ivan (2016)	The VERA-2 protocol can be augmented with the cyber-focused risk indicator protocol referred to as Cyber-VERA. The combined use of the two tools provides a robust and cyber-focused risk assessment intended to provide early warning indicators of terrorist action and assist law enforcement analysts in their national security investigations.	Imagery	<div>1. Uses graphic representations, symbols/logos of terrorist groups, steganography</div> <div>2. Organises site/ page, rubrics to glorify violence, promote aggression, rigid worldview</div> <div>3. Uses musical background to incite hatred, recruitment to violent action</div> <div>4. Frequently changes profile and cover photos—inconsistent identity</div>
			Semantic content	<div>1. Personal, terrorist narrative to promote extremist views, aggression, grievances</div> <div>2. Uses multiple/ alternative narratives related to identity</div> <div>3. Uses idealised content about own community, vilifies others, dehumanisation</div> <div>4. Uses language to display extremist views, allegiance to terrorist group, narrative</div>
			Beliefs, attitudes, intention	<div>1. Commitment to ideology justifying violence</div> <div>2. Perceived victim of injustice, grievances for collective group or individual</div> <div>3. Rejection of democratic society and values</div> <div>4. Adherence to conspiracy theories about the affiliated ethnic/ religious group</div> <div>5. Moral emotions: hate, anger, frustration, persecution, and/or alienation</div> <div>6. Identity conflict, rejection of national collective identity</div> <div>7. Lack of understanding, tolerance outside own group</div> <div>8. Expresses intention to act violently, incites violence</div> <div>9. Expresses willingness to die for cause, achieve martyrdom</div> <div>10. Evidence planning, preparing for violent action</div>
			Virtual social network context	<div>1. Is affiliated with an online group/ social media promoting terrorist violence</div> <div>2. Repetitively accesses posts blogs, extremist forums, terrorist information, know-how</div> <div>3. Establishes friendship bonds, networks other violent extremists online</div> <div>4. Susceptible to influence, authority, indoctrination</div>
			Individual online activity related to capacity	<div>1. Has paramilitary, explosives training or information on explosives-bomb making</div> <div>2. Uses multiple e-mail addresses, names to obscure identity</div>
			Leadership, organisational skills	<div>1. Subject has large following, network, significant role as leader online</div>

Note. These tools are all structured professional judgment (SPJ) instruments.

From “The development of structured guidelines for assessing risk in extremist offenders”, by M. Lloyd, & C. Dean, 2015, *Journal of Threat Assessment and Management*, 2(1), pp. 40-52, (<https://doi.org/10.1037/tam0000035>). Copyright 2015 by American Psychological Association; “Investigating the individual terrorist in Europe”, by J. R. Meloy, K. Roshdi, J. Glaz-Ocik, & J. Hoffmann, 2015, *Journal of Threat Assessment and Management*, 2(3-4), pp. 140-152, (<https://doi.org/10.1037/tam0000036>). Copyright 2015 by American Psychological Association; “Calibrating risk for violent political extremists: The VERA-2 Structural Assessment”, by D. E. Pressman, & J. S. Flockton, 2012, *The British Journal of Forensic Practise*, 14(4), pp. 237-251, (<https://doi.org/10.1108/14636641211283057>). Copyright 2012 by Emerald Publishing; “Can you identify violent extremists using a screening checklist and open-source intelligence alone?”, by V. Egan, J. Cole, B. Cole, L. Alison, E. Alison, S. Waring, & S. Elntib, 2016, *Journal of Threat Assessment and Management*, 3(1), pp. 21-36, (<http://dx.doi.org/10.1037/tam0000058>). Copyright 2016 by American Psychological Association; “Risk assessment and management of group-based violence”, by A. N. Cook, 2014, Doctoral dissertation. Copyright 2014 by Simon Fraser University; “Internet use and violent extremism: A cyber-VERA risk assessment protocol”, by D. E. Pressman, & C. Ivan, 2016, In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era*, pp. 391-409. Copyright 2016 by IGI Global.

1.3 Three Rounds of Modified Delphi Technique

In round 1², each panel member was tasked to evaluate and rate the factors for its relevance in detecting radicalisation in social media posts, using a 7-point Likert scale that ranged from “strongly disagree” (1) to “strongly agree” (7). The panel members were instructed to submit any additional factors that were deemed to be relevant to the research. At the end of round 1, no new items were proposed by the panellists.

In round 2, the measures of central tendency (means, median, mode) and standard deviation were calculated for each factor. This allowed the panellists to gauge where their ratings stand in comparison to the rest of the panel (Hasson et al., 2000). They were instructed to re-evaluate and revise their ratings of the factors (on the same 7-point Likert scale) based on their previous ratings and the mean ratings across the panel from round 1. This provided panel members the chance to reassess their initial ratings about the factors. In the event that they were satisfied with their own ratings, they could choose not to revise them.

In round 3, the panel members were asked to re-evaluate and revise their earlier ratings—based on the newly consolidated ratings of the means, median, mode, and standard deviation from the previous round. Similar to round 2, the panel members had the choice to maintain their previous ratings if they were satisfied with them. At the end of round 3, the criteria to determine whether a factor is useful for detecting online radicalisation is based on the mean ratings across the panel. A high mean rating would indicate that consensus for that

² This study has been approved by the NTU’s Institutional Review Board (IRB), and the data was collected between September and December 2017. The IRB reference number is IRB-2017-08-023.

factor has been achieved and that the factor has been agreed upon by the panel to be essential. For this study, the threshold for inclusion of a factor was set at 85 per cent (see Ulschak, 1983)—i.e., the mean rating across panellists had to be six and above on the 7-point Likert scale.

1.4 Results and Discussion

After the first round of survey data collection with the expert panel, 10 out of 67 factors were identified to be essential—see Table 7. Consensus was not reached for the remaining 57 factors. On the 7-point Likert scale, 28 factors had a mean rating of between 70 to 85 per cent, whereas 29 factors had a mean rating of less than 70 per cent.

Table 7

Consensus Rating for the Top 12 Factors

Factors	Consensus (%)		
	Round 1	Round 2	Round 3
Dehumanisation of the enemy	95.9	97.9 (+)	97.9 (-)
Need to redress injustice and express grievance	93.8	95.9 (+)	95.9 (-)
Us and Them thinking	95.9	95.9 (-)	95.9 (-)
Pathway warning signs	91.8	92.8 (+)	92.8 (-)
Attitudes that justify offending	91.8	91.8 (-)	91.8 (-)
Need to defend against threat	89.7	91.8 (+)	91.8 (-)
Political/moral motivation	85.7	91.8 (+)	91.8 (-)
Need for identity and meaning	85.7	89.7 (+)	89.7 (-)
Group influence and control	87.7	87.7 (-)	87.7 (-)
Transitional periods	85.7	87.7 (+)	87.7 (-)
Establishes friendship bonds, networks other terrorists online	83.6*	87.7 (+)	87.7 (-)
Family or friends support terrorist offending	81.6*	87.7 (+)	87.7 (-)

Note. This list contains factors that achieved the criteria of 85 per cent consensus in round 3.

*Factors that did not fulfil the criteria in round 1.

After the second round, some panel members changed their ratings. As a result, in addition to the ten identified factors from the previous round, two more factors were selected. They were “establishes friendship bonds, networks other terrorists online” and “family or friends support terrorist offending”. This increase in consensus amongst the panellists could be attributed to the tapping of shared knowledge amongst members of the expert panel to identify factors of relevance (Franklin & Hart, 2007). Consensus was not reached for the

remaining 55 factors: Twenty-seven factors had a mean rating of between 70 to 85 per cent, and 28 factors had a mean rating of less than 70 per cent.

After the third and final round, this systematic expert knowledge acquisition exercise achieved a consensus where 12 out of 67 factors were identified to be relevant for detecting radicalisation in social media posts. The stability of the panel members' ratings across the successive rounds of data collection suggests the convergence (i.e., theoretical saturation) of opinions based on their expert knowledge (Scheibe et al., 1975).

The exercise and resulting findings highlight a couple of interesting observations. Firstly, the consensus obtained from the SMEs adds value to the endeavour of identifying factors from extant terrorism risk assessment tools. Other terrorism researchers could consider adopting the Delphi technique as it helps to overcome the lack of primary data by utilising the shared knowledge of the SMEs. Having said that, the quality of the findings is dependent on the depth of expertise of the invited SMEs. Secondly, the top five factors that were labelled as essential were: “dehumanisation of the enemy” (97.9%), “need to redress injustice and express grievance” (95.9%), “us and them thinking” (95.9%), “pathway warning signs” (92.8%), and “attitudes that justify offending” (91.8%). These are risk factors that previous studies on terrorism and radicalisation have found evidence for (e.g., Borum, 2011a; Horgan, 2005; Kruglanski et al., 2006; Moghaddam, 2005; Ramakrishna, 2009; Sageman, 2004). It suggests that the expert panel found these factors to be equally important in detecting radicalisation in the online sphere. Lastly, with reference to the lowest rated factors, most of them were protective factors. The bottom five factors were: “failure of sexually intimate pair bonding and the

sexualisation of violence” (46.9%), “greater creativity and innovation” (48.9%), “involvement with non-violent, de-radicalisation, offence-related programs” (53.0%), “rejection of violence to obtain goals” (57.1%), and “community support for non-violence” (57.1%). This is not surprising as researchers and practitioners tend to ignore the identification of protective factors and focus more on the risk factors (Gill, 2015b). Thus, this is of concern as protective factors have been identified to be a potentially key aspect of risk assessment (Sarma, 2017).

There are two limitations that need to be discussed. The main limitation involves the use of the modified Delphi technique. The revisions in the ratings made by the panel members could be affected by groupthink where panellists conform to the views held by the majority. However, this limitation does not have a significant effect on the study as there was anonymity and no face-to-face interaction between the panel members during the data collection phase. Furthermore, they were given the autonomy to revise their ratings—only if they felt it was needed—and were under no particular time pressure to complete their ratings. Thus, the likelihood of having a groupthink response biases is reduced.

Another limitation pertains to the fact that the results were based on the opinions derived from seven local SMEs. Therefore, the results should not be taken to be reflective of experts in other parts of the world, nor to be generalisable to the wider context for terrorism on a global scale. Given that the consolidated factors were derived from terrorism risk assessment tools that tend to neglect the role of the internet (Dillon et al., 2017), it is crucial to proceed with caution in interpreting the findings. In other words, the 12 identified

factors should be understood as the beginning of a process to develop the actual factors and indicators of interest. In the literature on the Delphi technique, it is not uncommon for researchers to conduct further studies to enhance and verify their findings. For example, attempts have been made to compare findings with a different sample (Keil et al., 2002), validate results using a field study (Nambisan et al., 1999), triangulate findings with a parallel electronic survey (Yousuf, 2007), and generalise results using interviews (Duncan, 1995). The next step in this study involves supplementing the expert consensus with a parallel literature review on online radicalisation to triangulate and address any research gaps (e.g., address the lack of protective factors).

2. Literature Review to Supplement Modified Delphi's Findings

There are not many empirically driven or systematic review type of studies on the topic of online radicalisation (Hassan et al., 2018; Shortland, 2016). Nevertheless, this chapter attempts to identify literature that focuses on factors associated with online radicalisation, as well as any observable online behaviours and expressions that may be of relevance to detect radicalisation in social media posts. To capture all the relevant literature, a three-prong approach was adopted.

Table 8
Review of Three Academic Databases

Keywords	Academic database		
	ScienceDirect	PsycINFO	SAGE
(Internet OR Online) AND Terrorism	5046	70	6010
(Internet OR Online) AND Radicalisation	131	3	830
(Internet OR Online) AND Radicalisation AND (Risk Assessment OR Risk Factor)	59	3	436

Note. The values represent the number of papers that were identified using the keywords.

Firstly, to identify the relevant literature, keywords derived from the research questions in chapter 1 were used to search three major databases (PsycINFO, SAGE, ScienceDirect) in December 2018. The keywords were

‘internet’, ‘radicalisation’, and ‘risk assessment’. Variations for the keywords were also used: ‘online’ for ‘internet’, ‘risk factor’ for ‘risk assessment’. The search period was set to be from 2010 to 2018. This led to a total of 1,462 papers (see Table 8), which were then appraised to determine their relevance. Identical papers were removed to reduce repetition. Eventually, the full text of 48 papers were reviewed in detail. Of interest, across the three databases, there is a smaller amount of literature concerning online radicalisation ($n = 964$) as compared to online terrorism ($n = 11,126$). This reaffirms what researchers (e.g., Hassan et al., 2018) have argued as a lack of research on online radicalisation, and more importantly, reflects a potential lack of theoretical clarity or academic interest on the topic of online radicalisation—as compared to the topic of online terrorism.

Secondly, to complement the review of academic databases, hand searching of relevant literature was also conducted (see Vassar et al., 2016). White papers, as well as working papers from government agencies and think tanks, were collated. Reference lists of useful peer-reviewed articles were used to search for additional articles. Specialised terrorism journals such as “Perspectives on Terrorism”, “Behavioral Sciences of Terrorism and Political Aggression”, “Journal of Terrorism Research”, “Journal for Deradicalization”, “Terrorism and Political Violence”, and “Studies in Conflict & Terrorism” were also examined for relevant articles.

Finally, my professional experience (13 years) in conducting online radicalisation research as a research analyst in a government agency was used to assist in the identification of relevant literature as well as establish the criticality of any identified factors and indicators. The insights derived from my

personal discussions with SMEs from various parts of the world were also factored into the analysis.

2.1 Relevant Areas of Research

The list below documents the research areas that were deemed relevant from the literature review:

- a) Pathways of online radicalisation (e.g., Archetti, 2015; Koehler, 2014; Neo, 2016; Saifudeen, 2014; 2016; Torok, 2013; Weimann & von Knop, 2008), extant radicalisation models (e.g., Moghaddam, 2005; Silber & Bhatt, 2007), as well as literature on how individuals join criminal gangs and cult groups (e.g., Hutchinson & O'malley, 2007; Weisburd et al., 2020). These areas of research provide insights about the individual's susceptibility to radical influence as well as how they build online relationships with like-minded others.
- b) Motivations of individuals whose radicalisation process is mediated by the internet (e.g., Dean, 2014; Gan et al., 2019; Geeraerts, 2012; Kruglanski et al., 2018; Neo et al., 2016; Roberts, 2019; Saltman, 2016). These scholarly works contribute insights about the motivations, such as perceived grievances, pursuit for significance, need for excitement, need for belonging, that motivate self-radicalised individuals.
- c) Persuasive features of radical online discourse and discussions (e.g., Andre, 2012; Bhui & Ibrahim, 2013; Cohen & Kaati, 2018; Dauber & Winkler, 2014; Erikha et al., 2016; Macnair & Frank, 2017; Mahood & Rane, 2017; Torok, 2016). Insights gleaned from these studies enhance

our knowledge about how the radical narratives propagated by terrorists may appeal to certain individuals.

- d) Exploitation of the internet by terrorists (e.g., Conway, 2017; Droogan et al., 2018; Hussain & Saltman, 2014; Seib & Janbek, 2010; Mair, 2016; Meleagrou-Hitchens & Kaderbhai, 2017; Romyn & Kebbell, 2016; Speckhard & Ellenberg, 2020; Weimann, 2004; 2010; Yasin, 2017; Zelin, 2013). These studies provide valuable insights about how terrorists have exploited the features of the internet to acquire information, communicate with one another, disseminate propaganda, radicalise new supporters, etc.
- e) Individual's reactions to terrorist online content (e.g., Baines et al., 2010; Conway & McInerney, 2008; Costello et al., 2018; Hassan et al., 2018; Lee & Leets, 2002; Pauwels & Schils, 2016; Rieger et al., 2013; Vergani & Bliuc, 2018). These studies attempt to find the link between the exposure to terrorist online content and the resultant effect it can have on an individual's attitude and behaviour.
- f) Case study analysis of individuals who were radicalised via the internet (e.g., Böckler et al., 2015; Halverson & Way, 2012; Pearson, 2016; Pressman & Ivan, 2016; von Behr et al., 2013). These studies provide an in-depth investigation of the factors that influence an individual's radicalisation pathway.
- g) Case study analysis of how ISIS exploited the internet (e.g., Berger & Morgan, 2015; Bodine-Baron et al., 2016; Callimachi, 2015; Carter et al., 2014; Dillon et al., 2019; Freeman et al., 2017; Pearson, 2018; Prucha, 2016; Vidino & Hughes, 2015; Winter, 2015).

- h) Case study analysis of how right-wing groups exploited the internet (e.g., Bowman-Grieve, 2009; Caiani & Kröll, 2015; Crosset et al., 2018; Koch, 2019; Tuck et al., 2016).
- i) The social interactions in the terrorist online communities (e.g., Bowman-Grieve, 2013; Brachman & Levine, 2011; Ducol, 2012; Hegghammer, 2014; Klausen, 2015; Klausen et al., 2012; Mans & Tuitel, 2016; O'Hara & Stevens, 2015; Radlauer, 2007; Weimann, 2012; Wojcieszak, 2010). Research from these studies shed light on how the online communities influence the individual's radicalisation process, as well as how the members interact and influence each other.
- j) Factors that hinder online radicalisation (e.g., Bergin et al., 2009; Lucas & Aly, 2015; Neumann, 2012; Ramakrishna, 2016; Shi, 2016). These studies elucidate the personal and/or situational factors that may hinder an individual's radicalisation trajectory.
- k) Detecting and assessing the risk of online radicalisation (e.g., Agarwal & Sureka, 2015; Bayerl et al., 2020; Johansson et al., 2016; Neo, 2020; Pressman & Ivan, 2016; Rowe & Saif, 2016; Scanlon & Gerber, 2014). These studies have adopted various techniques to measure the risk of online radicalisation.

3. Synthesising Person-centric and Psychosocial Risk Factors, and Protective Factors

This section will illustrate how the derived knowledge from the literature review was analysed in conjunction with the modified Delphi's findings to identify the final list of factors and their associated indicators.

3.1 Grouping the Modified Delphi's Factors into the Person-centric, Psychosocial, and Protective Dimensions

The framework of person-centric, psychosocial, and protective dimensions—proposed in chapter 2—was used as an anchor to conceptually categorise the 12 factors that were found after the modified Delphi process. The person-centric dimension recognises factors that capture the characteristics of the radicalising individual. In this sense, seven modified Delphi's factors fulfilled this criterion: “need to redress injustice and express grievance”, “pathway warning signs”, “need for identity and meaning”, “political/ moral motivation”, “transitional periods”, “need to defend against threat”, and “attitudes that justify offending”. In terms of the psychosocial dimension, the factors within it would account for the online behaviours and changes in cognition due to the individual's interactions with the terrorist online communities. With this in view, five modified Delphi's factors were identified as psychosocial risk factors: “dehumanisation of the enemy”, “us-and-them thinking”, “family or friends support terrorist offending”, “establishes friendship bonds, networks other terrorists online”, and “group influence and control”. With regards to the protective dimension, it encapsulates factors that reduce one's risk of becoming radicalised. However, given that no protective factors were rated as essential by the expert panel, I sought to derive relevant protective factors based on (i) the absence of the above-mentioned risk factors—such an approach to identify protective influence has been adopted in risk assessment tools such as ERG 22+ (see Lloyd & Dean, 2015); and (ii) the framework on protective factors proposed by Neo et al. (2017).

Table 9*Dimensions and Factors for Detecting Radicalisation in Social Media Posts*

Dimension	Factor
Person-centric (features of the radicalising individual)	<ol style="list-style-type: none"> 1. Perceived grievances 2. Knowledge and skill to commit terrorist offences 3. Redemption and the pursuit for significance 4. Personal uncertainty 5. Readiness to use violence
Psychosocial (interactions with the online communities)	<ol style="list-style-type: none"> 1. Intolerance towards multi-religious, multi-racial living 2. Commitment to terrorist groups 3. Online relationship building with like-minded individuals 4. Involvement in the terrorist online community 5. Negative social support
Protective (features that reduce the risk for radicalisation)	<ol style="list-style-type: none"> 1. Individual-centric protective elements 2. Online environment-centric protective elements

Note. These factors are identified based on online expressions and/or online behaviours.

The 12 factors derived from the modified Delphi technique were then analysed in parallel with the literature review. To better reflect the nature of online radicalisation, the factors were renamed into meaningful labels that take into account the insights gathered from both the findings of the literature review as well as the modified Delphi technique. These 12 renamed factors (see Table 9) were further substantiated with 42 indicators in order to provide a clearer definition of the types of online behaviours and linguistic expressions to look out for.

3.2 Person-centric Risk Factors

There are five person-centric risk factors and their 20 associated indicators.

3.2.1 Perceived Grievances

Originally termed as “need to redress injustice and express grievance”, this factor was renamed as “perceived grievance” to better reflect the personal expression of anger and grievance. The core element of this factor is the linguistic expression made by the individual about the injustice they felt. It can range from strong contemptuous feelings of anger arising from certain acts of

deprivation or discrimination to the revelation that their faith is being targeted unfairly. Research has found that such perceptions can be a powerful tool to motivate and propel people into action (Dean, 2014; Hu, 2016). In fact, terrorists and their supporters have been known to publicise their perceived grievances via social media (Carter et al., 2014; Pearson, 2018), whilst at the same time, highlight their frustration and hatred (Erikha et al., 2016; Torok, 2016).

The associated indicators of “perceived grievance” (PG) are:

- PG1: Publicise the injustices targeted at one’s own community, faith, or belief
- PG2: Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice
- PG3: Express frustration with the injustice targeted at one’s own community, faith, or belief
- PG4: Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice
- PG5: Openly challenge certain group(s) of concern about the injustice

3.2.2 Knowledge and Skill to Commit Terrorist Offences

Originally termed as “pathway warning signs”, this factor was renamed as “knowledge and skill to commit terrorist offences” to better reflect the interest espoused by the individual to learn skills and knowledge that would help them support or commit terrorist offences. As terrorist groups have disseminated online manuals containing operational information on how to make explosives or carry out an attack (Lemieux et al., 2014; Romyn & Kebbell, 2016), this has inadvertently increased the likelihood of supporters re-

propagating such information amongst themselves. In some cases, they may utilise the information to conduct attacks (Institute for Policy Analysis of Conflict [IPAC], 2019). Furthermore, terrorists' supporters have been known to carry pictures of weapons and/or themselves in combat actions as their profile pictures (Cohen & Kaati, 2018). However, it is vital to consider these images in relation to the individual's other online behaviours because the use of such imagery could be considered metaphorical.

The associated indicators of “knowledge and skill to commit terrorist offences” (K) are:

- K1: Demonstrate an interest in learning combat skills
- K2: Showcase interest in the use of weapons and explosives
- K3: Have information on explosives-bomb making

3.2.3 Redemption and the Pursuit for Significance

Originally termed as “political/moral motivation” and “need for identity and meaning”, these two factors were combined and renamed as “redemption and the pursuit for significance” to better reflect the individual's lack of identity and/or meaning in their lives, and their strong desire to bring about changes. Based on empirical findings, feelings of insignificance have been known to drive some individuals to embrace terrorism as a means to find purpose in their lives (Kruglanski, 2014; Kruglanski et al., 2018). Often these feelings can be exacerbated by the contempt they had of their prior practices (e.g., immoral lifestyles) as well as those of the governing bodies (e.g., not taking action to alleviate suffering). For example, many Kurdish foreign fighters are motivated to participate in the fight against ISIS because the conflict provided them with an avenue to do something meaningful for others (Tuck et al., 2016). Similarly,

Dillon et al. (2019) found the pursuit for significance as one of the major themes amongst the social media posts of those who travelled to join ISIS as foreign fighters.

The associated indicators of “redemption and the pursuit for significance” (S) are:

- S1: Desire to partake in humanitarian activities in countries associated with terrorism opportunities
- S2: Desire to repent by migrating to countries associated with terrorism opportunities
- S3: Express feelings of contempt for own prior practices
- S4: Intention to search for opportunity to do something meaningful

3.2.4 Personal Uncertainty

Originally termed as “transitional periods”, this factor was renamed to “personal uncertainty” to better capture the disorientating self-views and worldviews of the individual. The core element of this factor is the linguistic expression made by the individual in relation to drastic changes (e.g., loss of status, failure in studies) in their lives, which may increase their receptivity towards new ideology. Doosje et al. (2013) found that personal uncertainty—amongst a sample of Dutch Muslim youth—is one of the three risk factors for individuals to adopt a radical belief system. Other studies have found further empirical evidence for this factor. Meloy and Gill (2016), for example, noticed that this factor appeared in more than half of the sample of lone-actor terrorists investigated by them.

The associated indicator of “personal uncertainty” (P) is:

- P1: Desire to explore different ideologies and beliefs—inconsistent identity

3.2.5 Readiness to Use Violence

Originally termed as “need to defend against threat” and “attitudes that justify offending”, these two factors were combined and renamed as “readiness to use violence” to better reflect the self-driven need to redress or remediate the grievances. This is different from the first factor of “perceived grievance” as it concerns the fixation on those responsible—for the grievances—as a threat, and the need to ameliorate the situation. The core element of this factor is the linguistic expression made by the individual in relation to their expressed willingness to use violence. They may start to express the belief that extreme measures, such as the use of violence, are necessary to defend fellow in-group members. The trouble lies in the extent to which the individual imagined themselves as a pseudo-warrior fighting on behalf of a terrorist group or a beleaguered community. This is best exemplified by the example highlighted by Hu (2016), where the detainees perceived ISIS as the good guys who were forced to use violence to protect Muslims against the Western forces. McCauley and Moskalenko (2011) reason that the communication of such sentiments represents a crucial progression from the expression of intention without action to the potential action stage.

The associated indicators of “readiness to use violence” (R) are:

- R1: Voice strong support for the use of violence towards a certain group(s) of concern as a viable solution
- R2: Incite friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief

- R3: Express willingness to die for cause, and achieve martyrdom
- R4: Demonstrate a preoccupation with an individual from group(s) of concern as a potential target
- R5: Display themselves as a protector/hero of their fellow believers of the same faith, religion or belief
- R6: Perceive an urgency to act and that non-violent alternative are ineffective solutions
- R7: Indicate their intention to travel and participate in overseas conflict

3.3 Psychosocial Risk Factors

There are five psychosocial risk factors and their 16 associated indicators.

3.3.1 Commitment to Terrorist Groups

Originally termed as “us and them thinking”, this factor was renamed to “commitment to terrorist groups” to better reflect the in-group favouritism by the individual. Emblematic of the us-versus-them perspective, research has shown how the propagation of radical narratives has created an environment where members of the in-group are presented as being honourable and virtuous (Borum, 2011a; Reicher et al., 2008). The core element of this factor is the linguistic expression made by the individual in relation to their overt identification with particular terrorist personalities and/or groups. The individual moves from ‘thinking about the group’ to actually ‘identifying with it’, and displays an unhealthy obsession with radical materials. They may overtly praise and quote famous terrorists such as Anwar Al-Awlaki (Lucas & Aly, 2015), swear allegiance to terrorist groups (Hussain & Saltman, 2014), and express support for them (Carter et al., 2014).

The associated indicators of “commitment to terrorist groups” (C) are:

- C1: Quotations from/ associations with personalities known for their radical views
- C2: Identify with symbols of known terrorist groups on their online profile
- C3: Display their public allegiance to terrorist groups
- C4: Praise and defend terrorist groups

3.3.2 Intolerance Towards Multi-religious, Multi-racial Living

Originally termed as “dehumanisation of the enemy”, this factor was renamed to “intolerance towards multi-religious, multi-racial living” to better reflect the overarching sense of exclusivism espoused by the individual against the out-group. The core element of this factor is the linguistic expression made by the individual in relation to how the terrorist narratives have shaped their ‘exclusive’ views. These narratives tend to depict the members of the out-group as a threat by virtue of their inherent aggressive and devious characteristics, and their role in threatening the in-group’s way of life or survival (Baumgarten, 2017). This may lead adherents of such ideology to believe that they are the ‘privileged’ few who are fighting for the religion and/or community. These individuals may also express difficulties living in a secular society that does not share their worldviews (Milla & Umam, 2019), and display a lack of empathy towards people of other faiths; mostly due to the perceived negative influence that people of other faiths may have. This heightened sense of exclusivity may exacerbate the level of disdain that individuals have towards the out-groups, sometimes to the extent of dehumanising them (Tolis, 2019).

The associated indicators of “intolerance towards multi-religious, multi-racial living” (I) are:

- I1: Force friends, colleagues or family to distance themselves from certain group(s) or community
- I2: Dehumanise group(s) of concern who hold different viewpoints/beliefs system
- I3: Dissatisfaction with local cultures, practices, values, and governance
- I4: Anti-integration messaging—exclusivity of one’s own community, faith, or belief

3.3.3 Online Relationship Building with Like-minded Individuals

Originally termed as “establishes friendship bonds, networks other terrorists online”, this factor was renamed to “online relationship building with like-minded individuals” to better emphasise that the targeted audience is not just the terrorists, but also other like-minded online supporters. The core element of this factor is the linguistic expression made by the individual in their attempts to link up with key contacts within the terrorist online communities. Many studies have found a link between access to online networks and radical behaviours. For example, 14 per cent of the 223 convicted terrorists examined by Gill et al. (2017), went on to conduct attacks after receiving online invitations to join terrorist groups. For ISIS foreign fighters, one of the key determinants underlying their recruitment process is their ability to establish connections with those who have already joined the group (Holman, 2016; Reynolds & Hafez, 2019; Speckhard & Ellenberg, 2020). These relationships allowed the individual to gain useful information as well as moral support on how to make the trip to Syria or Iraq.

The associated indicators of “online relationship building with like-minded individuals” (OR) are:

- OR1: Attempt to reach out to terrorist
- OR2: Develop and disseminates terrorist content
- OR3: Attempt to set up physical meeting with terrorists

3.3.4 Involvement in the Terrorist Online Community

Originally termed as “group influence and control”, this factor was renamed to “involvement in the terrorist online community” to better reflect the effects of group membership on the type and level of individual engagement. The greater their exposure to the radical online communities, the higher the likelihood of individuals assimilating and eventually propagating the radical beliefs. The core element of this factor is the individual’s active participation in the online networks. Studies have underlined the importance of such social interactions on the radicalisation process. For example, Hassan et al. (2018) observed that engagement in acts of political violence is correlated with an active engagement of radical online content. Similarly, based on 236 in-depth interviews with ISIS foreign fighters, 49 per cent reported possessing and watching radical content as an entry point for becoming involved with ISIS ideology (Speckhard & Ellenberg, 2020). For many of the White supremacist actors examined by Kruglanski et al. (2017), they reported listening to White power music as an initial step for them to embrace White supremacist ideology.

The associated indicators of “involvement in the terrorist online community” (OC) are:

- OC1: Possess terrorist documents, music, videos, etc. on computer or mobile devices

- OC2: Host web-links to other online platforms that contain terrorist context
- OC3: Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism
- OC4: A sudden increase in the user's activity

3.3.5 Negative Social Support

Originally termed as “family or friends support terrorist offending”, this factor was renamed to “negative social support” to better emphasise the social support provided by family and close friends. The core element of this factor is the acknowledgement by the individual for the support that they received for getting involved in the terrorist online communities. The literature has highlighted the role of close social support as a key facilitator towards involvement in terrorism. For example, family influence is one of the six individual-level mechanisms underlying political radicalisation (McCauley & Moskaleiko, 2011). Similarly, Osman (2010)’s analysis of Jemaah Islamiyah indicates that family bonds and relationships exert the strongest influence on an individual’s radicalisation trajectory.

The associated indicator of “negative social support” (N) is:

- N1: Presence of supportive family members and friends that encourage involvement in the terrorist online communities and/or terrorist offending

3.4 Protective Factors

As there were no protective factors rated as essential by the expert panel, I decided to use the framework proposed by Neo et al. (2017) to guide the identification of protective factors. This framework acknowledges the need

to identify protective factors at the individual-level and online environment-level. Two protective factors and their six associated indicators were found.

3.4.1 Individual-centric Protective Elements

The core element of this factor is the linguistic expression made by the individual that reflects their negative perceptions towards the terrorist narratives. These perceptions can be observed in the individual's online postings when they challenge the terrorist group's ideology or its use of violence. Kruglanski et al. (2018) explain that terrorists who become disillusioned with the group's strategy or indiscriminate use of violence would often leave the group. There is also evidence that terrorists may leave the group because of their changing life priorities (Bjørge, 2009), and then developing an appreciation for diversity (Barrelle, 2015). Furthermore, Pressman (2009) highlights the essential role that family and close friends, plays in discouraging terrorist offending. Hence, if an individual expresses such thoughts, it can be an indication of them moving away from online radicalisation.

The associated indicators of "individual-centric protective elements" (IP) are:

- IP1: Presence of supportive family members and friends that discourage terrorist offending
- IP2: Demonstrate willingness to engage in discussions of ideology and the use of violence
- IP3: Disillusioned with using violence to solve problems
- IP4: Demonstrate an appreciation for diversity

3.4.2 Online Environment-centric Protective Elements

The core element of this factor is the linguistic expression made by the individual in relation to online barriers that hinder their radicalisation process. It could be due to the fear of being monitored by law enforcement agencies, as well as concerns about having their accounts taken down by the social media companies (Menn & Volz, 2016). In addition, it could be about their inability to connect with the ‘right’ entities within the terrorist online communities (de Bie et al., 2015). As Cole et al. (2010) suggest, individuals may not get an opportunity to engage in terrorism if they are unable to contact the terrorist recruiters.

The associated indicators of “online environment-centric protective elements” (OP) are:

- OP1: Inability to obtain access to the terrorist online community
- OP2: Recognise and fear the detection by law enforcement and social media companies

4. General Discussion

Historically, the role that law enforcement played in countering terrorism has always been reactive rather than preventive (Borum et al., 1999). This approach becomes unviable in the current security climate in which terrorists effectively exploit the internet to recruit and to radicalise new supporters. More emphasis is warranted on deciphering how an individual’s digital footprints can be utilised to identify potential indications of radicalisation from their social media, and in the process of doing so, enhance online risk assessment of terrorism.

A combination of the modified Delphi technique with an in-depth literature review was employed in this study. On its own, these two different

methodologies would not have led to the current finalised list of factors and indicators. A mere focus on the modified Delphi technique would have yielded a consensus amongst the panel experts about the relevance of the factors (obtained from extant terrorism risk assessment tools) in detecting online radicalisation. However, it would overlook the part of how the factors could be operationalised for the online context. While the SMEs were extremely knowledgeable about this area of research, they inadvertently omitted some factors, such as the protective factors. This oversight is reflective of a common bias on risk (as opposed to protective) factors (Gill, 2015b).

In contrast, the sole use of the literature review would be limited by the lack of empirical evidence and my subjective interpretation of the review. Hence, the literature review was corroborated by experts' opinions obtained from the modified Delphi technique. Indeed, it was only after the combined analysis of both the modified Delphi findings and the literature review that the list of factors and their indicators was constructed.

To that end, this study was successful in identifying 12 factors and their associated 42 indicators. From a risk assessment perspective, these factors and indicators cohere as an investigative template to detect radicalisation in social media posts. More importantly, this study shows what could be done to harness cyber behaviours and content to identify online radicalisation and provide the foundation on which further research can build on. Having said that, it is important not to view the factors and indicators in isolation or use them as standalone measures. The factors and indicators serve to provide a psychological perspective to inform the online risk assessment process and support other existing intelligence and operational interventions.

Given that there is currently insufficient evidence to suggest a direct link between the identified factors and indicators and an individual's online radicalisation process, efforts that utilise empirical data to test these factors and indicators are therefore required—this will be addressed in the next chapter.

CHAPTER FOUR: COMPARING ISIS FOREIGN FIGHTERS VERSUS SYMPATHISERS: INSIGHTS FROM THEIR TWITTER POSTINGS³

This study attempts to map a set of person-centric and psychosocial risk factors, and protective factors to the social media posts of two groups of individuals who were influenced by propaganda materials about or from the Islamic State in Iraq and Syria (ISIS). This study aims to see if—and how—the social media posts of the individual actor could be used to distinguish foreign fighters (i.e., individuals who travelled to join ISIS) from sympathisers (i.e., individuals who did not travel to join ISIS). Six hundred and twenty-two tweets posted by a sample of three foreign fighters and three sympathisers were mapped against 12 factors (from chapter 3). The mean interrater reliability, measured using Cohen’s kappa, was .81 and ranged from good to excellent across all variables (McHugh, 2012). One significant difference (factor: “readiness to use violence”) was found between the two groups, and the finding indicates a new direction for further research, with the goal of providing empirical support for the online risk assessments of terrorists.

1. Which Terrorists’ Supporters Goes on to Fight?

In recent years, the notion of online radicalisation has gained traction. Terrorists of all stripes have extensively used the internet to propagate their message and gain new followers and sympathisers (Conway, 2007; Egan et al., 2016; Gill, 2015a; Weimann, 2004). The unfolding of the 2013 attack on the Westgate Mall in Nairobi, Kenya was live-tweeted by Al-Shabaab through its Twitter account to inform followers of the developments as well as to draw

³ A version of this chapter was published as Neo, L. S., Khader, M., & Pang, J. S. (2018). Comparing ISIS foreign fighters versus sympathisers: Insights from their Twitter postings. *Home Team Journal*, 7, 87-106. <https://www.mha.gov.sg/docs/default-source/publications/hta-journal-hr-issue-no-7.pdf>

attention to the group's cause (Mair, 2017). The internet has also afforded greater opportunities for terrorists to radicalise and mobilise others into action (Gill et al., 2017). In fact, there is an increase in the number of individuals who have been radicalised via the internet. Consistent with the ideas and ideologies they consumed on the internet, some of these individuals then transited offline to carry out real-world violence against targets (Edwards & Gribbon, 2013; Neumann, 2012). This, therefore, warrants special emphasis to understand terrorists and their supporters' online behaviours.

The recent rise of ISIS has revolutionised the way terrorists use the internet and in particular social media platforms. As Klausen (2015, p. 4) argues, "social media has changed the dynamic fundamentally. It has eliminated the terrorists' dependency on mainstream media, reversing the relationship by making mainstream media dependent on the jihadist-run social media". Through the use of its social media platforms, ISIS has inspired an unprecedented surge of individuals to leave their homeland and travel to the Middle East in order to join the group (Dawson et al., 2016; Mans & Tuitel, 2016). Credible estimates now suggest that more than 30,000 fighters have travelled to Syria since 2012, originating from more than 90 different countries (The Soufan Group, 2015).

However, it is essential to note that in this online milieu where terrorists operate, while there are many members of the online terrorist community, very few become terrorists or law-breakers in the real world. The 'loudest' online members—those engaged in the most vigorous and aggressive forms of speech—may not be the ones most likely to engage in violence, while the most

passive members are not automatically the most peaceful. It is not possible, in other words, to draw a straight line between online ‘noise’ and offline action.

In the context of ISIS, while its foreign fighters have become a dominant security concern, there is a need to be cognizant of the phenomenon of ‘stay home supporters’ (i.e., sympathisers) who are not mobilised despite being part of the same online terrorist community from which the foreign fighters were recruited (Vidino & Hughes, 2015). There is, therefore, a need to examine how researchers and analysts can harness such online information to better assess the threat posed by those who espouse terrorism.

Insights from communication literature suggest that personal attributes can be gleaned from studying the social media footprint of targeted individuals. For example, Alam et al. (2013, p. 6) argue that “there is a strong correlation between users’ personality and the way they behave on online social network”. Furthermore, social media profiles have been found to be reflective of the users’ actual personality, contrary to the assumption that people tend to present only highly favourable or desirable news or information about themselves online (Back et al., 2010).

Hence, it is possible to derive insights about an individual’s personality based on their social media activity. Patterns of their worldviews, preferences, and expressions can be ‘read’ and interpreted to identify their personality traits. However, it is not just personality traits that reveal themselves online. A study by Kosinski et al. (2013) has shown that social media analysis can also offer a window into a broad range of characteristics, including propensity for recreational drug use, status of parents’ marriage, preference for certain sports and teams, and, of course, political and religious views. The latter is particularly

important in the context of understanding online support for terrorism. As Pressman and Ivan (2016, p. 404) suggest, “data on the views, beliefs, attitudes, grievances, intentions and ideology of identifiable individuals can be captured from the internet”. The authors further argue that social media platforms provide important opportunities for law enforcement and intelligence agencies to gain knowledge of terrorists.

Thus, this study aims to ascertain if there are any person-centric and psychosocial risk factors, and protective factors that distinguish sympathisers from those planning to break the law or engage in real-world violence (i.e., foreign fighters). To answer this question, relevant factors based on a literature review that outline patterns of terrorists’ online activities were mapped against ISIS foreign fighters and ISIS sympathisers.

2. Method

2.1 Research Design

Given that these foreign fighters and sympathisers have published remarkable amounts of highly personal and detailed information on their social media accounts, this allows us the opportunity to download their social media postings for comparison. For the purpose of this study, the social media output (i.e., tweets from Twitter) of the foreign fighters and sympathisers were mapped to the factors as highlighted in Table 10. These factors were derived from a combined analysis of a literature review on online radicalisation and a modified Delphi Technique based on six terrorism risk assessment tools such as ERG 22+, IVP, TRAP-18, MLG, VERA-2, and Cyber-VERA—see chapter 3.

Table 10

Person-centric, Psychosocial, and Protective Dimensions and their Associated Factors and Indicators

Dimension	Factor		Indicator
Person-centric	Perceived grievances (PG)	PG1	Publicise the injustices targeted at one's own community, faith, or belief
		PG2	Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice
		PG3	Express frustration with the injustice targeted at one's own community, faith, or belief
		PG4	Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice
		PG5	Openly challenge certain group(s) of concern about the injustice
	Knowledge and skill to commit terrorist offences (K)	K1	Demonstrate an interest in learning combat skills
		K2	Showcase interest in the use of weapons and explosives
	Redemption and the pursuit for significance (S)	K3	Have information on explosives-bomb making
		S1	Desire to partake in humanitarian activities in countries associated with terrorism opportunities
		S2	Desire to repent by migrating to countries associated with terrorism opportunities
		S3	Express feelings of contempt for own prior practices
	Personal uncertainty (P) Readiness to use violence (R)	S4	Intention to search for opportunity to do something meaningful
		P1	Desire to explore different ideologies and beliefs—inconsistent identity
		R1	Voice strong support for the use of violence towards a certain group(s) of concern as a viable solution
		R2	Incite friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief
		R3	Express willingness to die for cause, and achieve martyrdom
		R4	Demonstrate a preoccupation with an individual from group(s) of concern as a potential target
		R5	Display themselves as a protector/hero of their fellow believers of the same faith, religion or belief
		R6	Perceive an urgency to act and that non-violent alternative are ineffective solutions
		R7	Indicate their intention to travel and participate in overseas conflict
	Commitment to terrorist groups (C)	C1	Quotations from/ associations with personalities known for their radical views
		C2	Identify with symbols of known terrorist groups on one's online profile
		C3	Display their public allegiance to terrorist groups
		C4	Praise and defend terrorist groups
Psycho-social	Intolerance towards multi-religious, multi-racial living (I)	I1	Force friends, colleagues or family to distance themselves from certain group(s) or community
		I2	Dehumanise group(s) of concern who hold different viewpoints/ beliefs system

Table 10 (continued)

Dimension	Factor		Indicator
Psycho-social	Intolerance towards multi-religious, multi-racial living (I)	I2	Dehumanise group(s) of concern who hold different viewpoints/ beliefs system
		I3	Dissatisfaction with local cultures, practices, values, and governance
		I4	Anti-integration messaging—exclusivity of one's own community, faith, or belief
	Online relationship building with like-minded individuals (OR)	OR1	Attempt to reach out to terrorists
		OR2	Develop and disseminates terrorist content
		OR3	Attempt to set up physical meeting with terrorists
	Involvement in the terrorist online community (OC)	OC1	Possess terrorist documents, music, videos etc. on computer or mobile devices
		OC2	Host web-links to other online platforms that contain terrorist context
		OC3	Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism
		OC4	A sudden increase in the user's activity
	Negative social support (N)	N1	Presence of supportive family members and friends that encourage involvement in the terrorist online communities and/or terrorist offending
Protective	Individual-centric protective elements (IP)	IP1	Presence of supportive family members and friends that discourage terrorist offending
		IP2	Demonstrate willingness to engage in discussions of ideology and the use of violence
		IP3	Disillusioned with using violence to solve problems
		IP4	Demonstrate an appreciation for diversity
	Online environment-centric protective elements (OP)	OP1	Inability to obtain access to the terrorist online community
		OP2	Recognise and fear the detection by law enforcement and social media companies

2.2 Sampling Procedure

As this study aims to identify the factors that may distinguish individuals who have moved beyond the role of a sympathiser to that of a foreign fighter, the Twitter accounts of ISIS fighters (supporters of ISIS who have travelled to Syria and engaged in real-world violence) and ISIS sympathisers (supporters of ISIS who neither travelled to Syria nor engaged in real-world violence) were selected for comparison.

2.2.1 Criteria for Sample

The decision to include the Twitter accounts of potential foreign fighters and sympathisers in the current study was based on the following criteria:

- The account must be affiliated with ISIS, based on the content and context of the media postings sent from these accounts;
- The identified accounts belong to individuals and are not accounts belonging to a group or a communal account run by several users;
- The accounts were active during the period of 2013 to 2015⁴—this period was the time where most of the ISIS foreign fighters made the travel to Syria and Iraq to join ISIS; and
- The selected Twitter accounts originated from the United Kingdom.

In order to ensure that the account was authentic and belonged to a foreign fighter, there was a need to look for evidence such as pictures of them in combat, reference to/from other foreign fighters, description of battles, description of migration, descriptions of life in Syria and Iraq which tally with other accounts of life there. In contrast, sympathisers were identified based on the evidence of support for ISIS in their media postings, such as viewing ISIS' activities in a sympathetic light and being able to express a high level of knowledge about ISIS' history and developments.

2.2.2 Identification of Sample

My own Twitter accounts were used to identify potential foreign fighters and sympathisers from the United Kingdom. Many of the leads came from news stories, blogs, reports released by law enforcement agencies, academic literature on ISIS, think tanks, discussions with academics and practitioners, and recommendation algorithms by Twitter.

⁴ Some individuals may have more than two years' worth of Twitter activity preserved, whilst others have only a few months. In addition, many of the time periods for different ISIS supporters do not always overlap.

In total, three foreign fighters and three sympathisers from the United Kingdom were identified for this exploratory study. Even though there are only three subjects per group, the richness of the qualitative data allowed me to make comparisons between the two groups. These are also individuals whose case information was available in the public domain via Twitter. The sample of foreign fighters was picked because of the availability of rich online histories before their departure to join ISIS. The sample of sympathisers was obtained by identifying individuals with rich online histories and had not made the trip to travel to Syria to fight for ISIS.

To ensure that a standardised comparison of content between the two groups could be performed, two additional guidelines were implemented. Firstly, I chose Twitter accounts of foreign fighters and sympathisers that approximated 100 tweets each—the selected accounts tweeted in the range of 70 to 130 tweets (plus or minus 30 tweets from the average 100 tweets). For the fighters, tweets were taken from the time they set up the accounts until they made the travel. For the sympathisers, these were tweets taken from the time they set up the accounts until the accounts became inactive. Thus, this ensured that a similar number of tweets from each group was available for analysis. Secondly, the geographical location of both groups was kept constant as they were all residing in the United Kingdom when the tweets were created.

2.3 Data Coding Procedure

2.3.1 Data Coding

A codebook—see Appendix C—was developed based on the above-mentioned 12 factors and 42 indicators to guide and inform the coders about what to look out for. The coders were research analysts who had at least one

year of research experience on the topic of online radicalisation and terrorism. The coders were instructed to look at the overall context of the tweet (e.g., matching pictures with accompanying text and emoticons) to best decipher the attitudes, feelings, and opinions of the user.

For example, if a tweet quoted this verse of the Quran – ‘And I did not create the jinn and mankind except to worship me’ (51:56) – it would not be coded as a marker of terrorist belief. However, if the same verse appeared in a tweet alongside a picture of a fighter or suicide bomber, it could legitimately be taken as inferring jihad as a religious obligation.

All coding for the indicators was binary (present or absent), with a notation if there was insufficient information. Coders also recorded the number of instances an indicator was mentioned. This is particularly important because it allowed me to obtain an objective estimate of the prevalence of the 42 indicators in the sample’s social media output.

2.3.2 Interrater Reliability

Two independent coders were asked to code the Twitter accounts of the three foreign fighters and three sympathisers using the codebook after receiving instructions and practice in using it. Coders were blind to the status of the account holders (i.e., fighters or sympathisers). To measure the agreement between the two coders, Cohen’s kappa—which is a more robust measure than simple per cent agreement calculation—was computed (Landis & Koch, 1977). All kappa values ranged from good to excellent (.78 to .86; McHugh, 2012), and all were significant at $p < .001$; the mean kappa was .81. In other words, the coders exhibited a high level of agreement in terms of their coding.

3. Results

To examine the relationship between the factors and the social media posts of the foreign fighters and sympathisers, the presence or absence of each factor and its associated indicators was used for analysis. Table 11 lists each factor and its associated indicators and how they were coded.

Table 11
Presence of Factors for Foreign Fighters and Sympathisers

Factor	Indicator	% Present in overall sample	% Present in Fighters	% Present in Sympathisers
Perceived grievances (PG)	PG1	100 (6)	100 (3)*	100 (3)*
	PG2	83 (5)	66 (2)*	100 (3)*
	PG3	66 (4)	33 (1)	100 (3)*
	PG4	100 (6)	100 (3)*	100 (3)*
	PG5	66 (4)	66 (2)*	66 (2)*
Knowledge and skill to commit terrorist offences (K)	K1	16 (1)	33 (1)	66 (2)*
	K2	50 (3)	33 (1)	33 (1)
	K3	0 (0)	100 (3)*	100 (3)*
Redemption and the pursuit for significance (S)	S1	0 (0)	100 (3)*	100 (3)*
	S2	33 (2)	0 (0)	33 (1)
	S3	16 (1)	100 (3)*	0 (0)
	S4	33 (2)	0 (0)	0 (0)
Personal uncertainty (P)	P1	0 (0)	0 (0)	0 (0)
Readiness to use violence (R)	R1	66 (4)	66 (2)*	0 (0)
	R2	66 (4)	33 (1)	0 (0)
	R3	50 (3)	66 (2)*	0 (0)
	R4	16 (1)	0 (0)	0 (0)
	R5	33 (2)	100 (3)*	33 (1)
	R6	16 (1)	100 (3)*	33 (1)
	R7	16 (1)	100 (3)*	0 (0)
Commitment to terrorist groups (C)	C1	83 (5)	33 (1)	0 (0)
	C2	50 (3)	66 (2)*	0 (0)
	C3	33 (2)	0 (0)	33 (1)
	C4	83 (5)	0 (0)	33 (1)
Intolerance towards multi-religious, multi-racial living (I)	I1	50 (3)	66 (2)*	100 (3)*
	I2	33 (2)	33 (1)	66 (2)*
	I3	100 (6)	66 (2)*	0 (0)
	I4	100 (6)	66 (2)*	100 (3)*
Online relationship building with like-minded individuals (OR)	OR1	66 (4)	100 (3)*	33 (1)
	OR2	0 (0)	0 (0)	0 (0)
	OR3	16 (1)	33 (1)	0 (0)
Involvement in the terrorist online community (OC)	OC1	33 (2)	0 (0)	66 (2)*
	OC2	33 (2)	33 (1)	33 (1)
	OC3	66 (4)	100 (3)*	33 (1)
	OC4	0 (0)	0 (0)	0 (0)
Negative social support (N)	N1	0 (0)	0 (0)	0 (0)
Individual-centric protective elements (IP)	IP1	0 (0)	0 (0)	0 (0)
	IP2	33 (2)	0 (0)	66 (2)
	IP3	0 (0)	0 (0)	0 (0)
	IP4	16 (1)	0 (0)	33 (1)
Online environment-centric protective elements (OP)	OP1	0 (0)	0 (0)	0 (0)
	OP2	0 (0)	0 (0)	0 (0)

Note. *These indicators appeared in more than 50 per cent (i.e., at least 2 out of 3 individuals) of the two subsamples.

3.1 Factors Present in the Majority of the Foreign Fighter Subsample

Eighteen indicators appeared in more than 50 per cent of the tweets of the foreign fighter subsample. These 18 indicators were from the following eight factors: perceived grievances (PG); intolerance towards multi-religious, multi-racial living (I); knowledge and skill to commit terrorist offences (K); redemption and the pursuit for significance (S); readiness to use violence (R); commitment to terrorist groups (C); online relationship building with like-minded individuals (OR); and involvement in the terrorist online community (OC).

3.1.1 Perceived Grievances

For this factor, four out of five indicators appeared in more than 50 per cent of this subsample: PG1—100 per cent; PG2—66 per cent; PG4—100 per cent; PG5—66 per cent. For example, the foreign fighters would:

- Publicise the injustices targeted at one's community, faith, or belief (PG1): "Wallahi, very sad seeing women cry after the explosion. Children were injured, Allahul must'aan".
- Demonstrate a strong preoccupation with groups that they deemed to be responsible for the injustice faced by Muslim (PG2): "Abu_ilyaas91 akhi I can't give his info out as we know these kufaars would add 638 lies".
- Exhibit a strong sense of hatred towards the groups responsible for the injustice (PG4): "@ Panty_Python @ProxetSC2 @AbuAbdullah_RT Yep we cut heads, it's been 90 years we got bullied now its time to turn the table".

- Openly challenge those viewed as responsible for the injustice (PG5):

“Do these kufars think by killing Abu Bakr Al Baghdadi, they would stop Jihad?”.

3.1.2 Knowledge and Skill to Commit Terrorist offences

For this factor, one out of three indicators appeared in more than 50 per cent of this subsample: K2—100 per cent. For example, the foreign fighters would:

- Showcase interest in the use of weapons and explosives (K2): “Picture of Ali Kalantar firing a weapon; Post: {And fight them until there’s no fitnah and (until) the religion, all of it, is for Allah...} 8:39”.

3.1.3 Redemption and the Pursuit for Significance

For this factor, two out of four indicators appeared in more than 50 per cent of this subsample: S2—66 per cent; S4—66 per cent. For example, the foreign fighters would:

- Exhibit the desire to repent by migrating to countries associated with terrorism opportunities (S2): “2 married brothers went off for dogma. One of them didnt even tell his wife back home (not in sham). Wow these brothers know priorities!!”.
- Showcase intention to search for opportunity to do something meaningful (S4): “If anyone wants to support a good cause... kik me and we can deal with it inshallah”.

3.1.4 Readiness to Use Violence

For this factor, four out of seven indicators appeared in more than 50 per cent of this subsample: R1—100 per cent; R2—100 per cent; R3—100 per cent; R5—66 per cent. For example, the foreign fighters would:

- Voice strong support for the use of violence as a viable solution (R1):
“Executed many prisoners yesterday, sold their deen for \$70 which they didn’t even get. #IS #Khilafa”.
- Incite friends, colleagues or family to join the terrorist cause (R2): “Did Allah not provide for your family whilst you were in the womb? You do not control rizq, Allah does so come here .. Allah wont let u down”.
- Express willingness to die for cause, and achieve martyrdom (R3): “40 brothers from my old khatiba gave bay’ah to death, cut their own exit route, entered enemy ranks of 3000. Victory soon. #Iraq #IS”.
- Display themselves as a protector of their fellow Muslim brother (R5):
“Look how a few men that submit to their Lord and seek to meet Him are humiliating the armies of the world. #IS”.

3.1.5 Commitment to Terrorist Groups

For this factor, three out of four indicators appeared in more than 50 per cent of this subsample: C1—66 per cent; C3—66 per cent; C4—66 per cent.

For example, the foreign fighters would:

- Display associations with personalities known for their radical views (C1): “ahmadmusajibril I love you for the sake of Allah. You know how to remove doubt may Allah reward you”.
- Display their public allegiance to terrorist groups (C3): “We are no longer The Islamic state of Iraq and sham. We are only the ‘ISLAMIC STATE’. It’s official khilafa is restored!”.
- Praise and defend terrorist groups (C4): “Theres no brotherhood like tht in Jihad. Make dua 4 the ikhwa here, wallahi thy look afta u. May Allah unite us in Jannah”.

3.1.6 Intolerance Towards Multi-religious, Multi-racial Living

For this factor, two out of four indicators appeared in more than 50 per cent of this subsample: I3—100 per cent; I4—100 per cent. For example, the foreign fighters would:

- Be dissatisfied with local cultures, practices, values, and governance (I3): “Picture of a family begging in the street; Post: This is the situation of the ummah, while the mujahideens bring honour to Islam our Muslim people abandon them”.
- Espouse anti-integration messaging—exclusivity of one’s community, faith, or belief (I4): “I found a bible in my workplace 😊 by some next man who probs tryna give some shirky dawah.. Shall I burn it? He might of left it here tho?”.

3.1.7 Online Relationship Building with Like-minded Individuals

For this factor, one out of three indicators appeared in more than 50 per cent of this subsample: OR1—100 per cent. For example, the foreign fighters would:

- Attempt to reach out to terrorists (OR1): “@IbnShaheed wallah I wanted to tell u guys but had to keep it low. U gt my kik, if I hav net there...”.

3.1.8 Involvement in the Terrorist Online Community

For this factor, one out of four indicators appeared in more than 50 per cent of this subsample: OC3—100 per cent. For example, the fighters would:

- Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism (OC3): “RT @truthsMaster: #BREAKING US AIR FORCE JETS BOMBED HOUSES OF CIVILIANS IN DOMIEZ,

SINJAR INSTEAD OF ISLAMIC STATE ARTILLERY
POSITIONS!”.

3.2 Factors Present in the Majority of the Sympathiser Subsample

Fourteen indicators from five of the factors appeared in more than 50 per cent of the tweets of the sympathiser subsample: perceived grievances (PG); intolerance towards multi-religious, multi-racial living (I); commitment to terrorist groups (C); involvement in the terrorist online community (OC); and individual-centric protective elements (IP).

3.2.1 Perceived Grievances

For this factor, all the five indicators appeared in more than 50 per cent of this subsample: PG1—100 per cent; PG2—100 per cent; PG3—100 per cent; PG4—100 per cent; PG5—66 per cent. For example, the sympathisers would:

- Publicise the injustices targeted at one’s community, faith, or belief (PG1): “Shia militants burning #Adhamiyah a Sunni neighborhood in #Baghdad.. #Iraq #ISIS [http://t.co/ HibKd7wJXq](http://t.co/HibKd7wJXq)”.
- Demonstrate a strong preoccupation with groups that they deemed to be responsible for the injustice faced by Muslim (PG2): “What treaty?? Didn’t America invade our lands rape our women torture us and kill our children, what treaty are u talking about”.
- Express frustration with the injustice targeted at the Muslim community (PG3): “Your duty is to convey the message. Not to become a welcome mat for the kuffar in hopes that they become Muslim. It wont work”.
- Exhibit a strong sense of hatred towards the groups deemed responsible for the injustice (PG4): “When they take over Turkey and have a strong

airforce, then CAR we are coming for you. Burma, we are coming for you”.

- Openly challenge those viewed as responsible for the injustice (PG5):
“Why dont the kuffar just let us leave?! You dont want us there, yet you dont want us to leave either! Hypocrites!”.

3.2.2 Commitment to Terrorist Groups

For this factor, three out of four indicators appeared in more than 50 per cent of this subsample: C1—100 per cent; C2—66 per cent; C4—100 per cent.

For example, the sympathisers would:

- Display associations with personalities known for their radical views
(C1): “WARNING! Voting Will Negate Your Tawheed By Sheikh Omar Bakri Muhammad (may Allah release him)”.
- Identify with symbols of known terrorist groups on one’s online profile
(C2): “Please dua to #FreeSheikhOmarBakri as he is due in court tomorrow for trial”.
- Praise and defend terrorist groups (C4): “I feel honored by The Islamic State. The kuffar fear me when they see me in their streets”.

3.2.3 Intolerance Towards Multi-religious, Multi-racial Living

For this factor, three out of four indicators appeared in more than 50 per cent of this subsample: I1—66 per cent; I3—100 per cent; I4—100 per cent.

For example, the sympathisers would:

- Force friends, colleagues or family to distance themselves from the West (I1): “Do not support the trinity of evil (Israel, America, Peshmerga) you will end up in a blazing fire”.

- Be dissatisfied with local cultures, practices, values, and governance (I3): “Rafidhi Iraqi utes are so wasted, all they do smoke is Shisha and talk about girls, They swarm my area like mad”.
- Espouse anti-integration messaging—exclusivity of one’s community, faith, or belief (I4): “IS destroyed Palmrya’s prison because it was a symbol of oppression and humiliation to Muslims, We are not kuffar to make a memorial of it”.

3.2.4 Involvement in the Terrorist Online Community

For this factor, one out of four indicators appeared in more than 50 per cent of this subsample: OC1—66 per cent. For example, the sympathisers would:

- Possess terrorist documents, music, videos etc. on computer or mobile devices (OC1): “18+ this is an Iraqi army video showing the absolute babarity and depravity of #Obama allies Shia militia/Iraqi army”.

3.2.5 Individual-centric Protective Elements

For this factor, one out of four indicators appeared in more than 50 per cent of this subsample: IP2—66 per cent. For example, the sympathisers would:

- Demonstrate a willingness to engage in discussions of ideology and the use of violence (IP2): “One shouldnt go to extreme in takfir, but also the other side of the spectrum cant be forgotten, to go to extremes in NOT making takfir”.

3.3 Comparing Foreign Fighters with Sympathisers

After understanding how the factors and their associated indicators are mapped to the fighter and sympathiser samples, I examined the commonalities and differences between these two groups.

3.3.1 What are the Commonalities between Foreign Fighters and Sympathisers?

Several common factors were identified. As seen in Table 11, there are three factors of interest: perceived grievances (PG), intolerance towards multi-religious, multi-racial living (I), commitment to terrorist groups (C), and involvement in the terrorist online community (OC).

This is in line with research that highlights perceived grievance as a form of motivation that influences terrorists' radicalisation process (Borum, 2011a), the lack of understanding and tolerance exhibited by terrorists outside of their group (Hussain & Saltman, 2014), the process through which terrorists may re-negotiate their identities within the terrorist movement and become more supportive towards the movement (Bowman-Grieve, 2009), and the role of the online terrorist community (Neumann, 2012).

Thus, this observation suggests that ISIS supporters (foreign fighter or sympathiser) would create tweets that display: notions that highlight injustices perpetrated against their community, faith, or belief; signs of intolerance towards others, especially those who do not belong to their in-group; overt support for ISIS and its campaign to set up an Islamic State; and links or other accounts that propagate terrorist ideologies, news or in-group favouritism.

Furthermore, some factors were completely absent from both the foreign fighter and sympathiser groups. These factors were: Personal uncertainty (P); negative social support (N); and online environment-centric protective elements (OP). The absence of these factors could be attributed to the difficulties involved in deciphering and identifying them, or that these factors are not relevant in the online detection of ISIS fighters and sympathisers.

3.3.2 What are the Differences between Foreign Fighters and Sympathisers?

There are several factors that have the potential to distinguish foreign fighters from sympathisers. As highlighted in Table 11, this is based on the observed differences in the way the factors and their associated indicators were mapped between the two groups. The five factors were: the knowledge and skill to commit terrorist offences (K), redemption and the pursuit for significance (S), readiness to use violence (R), online relationship building with like-minded individuals (OR), and individual-centric protective elements (IP).

I further examined the frequency of tweets at which each indicator was being mapped; the total number of tweets that was coded under each factor for both groups was calculated—see Table 12.

Table 12
T-test Results Comparing ISIS Foreign Fighters' and Sympathisers' Tweets

Factor	Foreign fighter		Sympathiser		t-test
	<i>n</i>	<i>M (SD)</i>	<i>n</i>	<i>M (SD)</i>	
Perceived grievances (PG)	21	7.0 (6.2)	59	19.6 (8.5)	2.07, <i>p</i> = .10
Intolerance towards multi-religious, multi-racial living (I)	25	8.3 (1.5)	54	18.0 (14.4)	1.15, <i>p</i> = .31
Knowledge and skill to commit terrorist offences (K)	3	1.0 (.0)	1	.3 (.5)	2.00, <i>p</i> = .11
Redemption and the pursuit for significance (S)	11	3.6 (4.7)	0	.0 (.0)	1.34, <i>p</i> = .25
Readiness to use violence (R)	40	13.3 (1.5)	4	1.3 (1.1)	10.85, <i>p</i> = .00
Commitment to terrorist groups (C)	20	6.6 (3.5)	23	7.6 (3.5)	.34, <i>p</i> = .74
Online relationship building with like-minded individuals (OR)	36	12.0 (16.4)	1	.3 (.5)	1.22, <i>p</i> = .28
Involvement in the terrorist online community (OC)	27	9.0 (7.0)	6	2.0 (2.6)	1.62, <i>p</i> = .18

Note. The following four factors were not included in this table as the frequency count was too low for analysis: Personal uncertainty (P); negative social support (N); individual-centric protective elements (IP); online environment-centric protective elements (OP).

This sample of fighters and sympathisers posted a total of 622 tweets. After these tweets were mapped against the indicators, 334 tweets were coded, accounting for 53.6 per cent of the total number of tweets. The rest of the tweets could not be coded, as they did not fit in any of the 42 indicators. There

was also a difference in the number of tweets coded for both groups. 183 and 151 tweets were coded for the fighter and sympathiser groups, respectively.

To determine whether there was any statistical difference between the fighters and sympathisers, an independent t-test was conducted to compare the mean number of tweets of these two groups. The results of the t-test suggested that only one statistically significant finding was found. As compared to sympathisers ($M = 1.3$), foreign fighters ($M = 13.3$) created more tweets that displayed their readiness to commit violence, $t(4) = 10.85$, $p = .000$. Before interpreting the results of the t-test, there is a need to ensure that the difference between the two groups is meaningfully large, independent of whether the difference is statistically significant (Cohen, 1988). To do so, the effect size was calculated using Cohen's d and was found to be large at .983.

In other words, the foreign fighters have a higher likelihood to tweet postings such as: "Jihad is the cure for all diseases #FACT", "The moustache men in deir need to realise if needed we are not afraid to slaughter all of deir and turn its ground red if required. #Khilafa", and "Running away from jihad will not save you from death. You can die as a coward or you can die as a martyr". The identification of this factor appears to be consistent with past research on how terrorists would act on their radical beliefs and manifest the willingness to use violence to achieve their objectives in a given situation (Borum 2015a; Kebbell & Porter, 2012; Lloyd & Dean, 2015).

4. Discussion

The aim of this exploratory study was to compare ISIS foreign fighters versus sympathisers based on their social media posts on Twitter. It was revealed that the factor "readiness to use violence" can be used to distinguish

the foreign fighters from the sympathisers. This finding may hold implications for designing counter terrorism measures.

At the fundamental level, it suggests that the detection of potential foreign fighters would be improved if online screening tools were programmed to identify this factor. As previously noted, the ‘loudest’ members on social media platforms may not be the ones most likely to engage in violence, while the most passive members are not automatically the most peaceful. This endeavour to empirically test and validate a list of factors to identify and decipher between online ‘noise’ (i.e., sympathisers) and offline action (i.e., foreign fighters) represents a basis for further study and examination. It also highlights what can be done to correctly identify sympathisers, who should be treated differently from foreign fighters who will indeed use violence to further the group’s cause. Given that law enforcement agencies have finite investigative resources, the ability to distinguish foreign fighters from sympathisers will be useful for law enforcement to determine whether or not a suspected terrorism case should be prioritised for more investigation.

Currently, the Home Team Behavioural Sciences Centre at the Ministry of Home Affairs, Singapore, identifies the factor “readiness to use violence” as one of three factors that Home Team officers should be trained to use to identify potential terrorists. Officers are trained to ask respondents if they have encountered anyone who:

- Supports the use of violence as a solution to achieve their political/religious terrorist agenda?
- Expresses low tolerance and resentment towards multi-racial and multi-religious living?

- Indicates interest to travel and participate in a foreign conflict?

Furthermore, it is interesting to note that while the results were not significant, the sympathisers manifested certain individual-centric protective elements (e.g., “Read my disclaimer, I’m against terrorism and proscribed organisations”) that may have reduced their likelihood to transit from online to offline behaviours, and become foreign fighters. Thus, beyond merely grappling with when and how an individual becomes radicalised, there is also value in exploring protective factors that dissuade individuals from getting involved in the first place. This notion has been corroborated by the findings from the General Intelligence and Security Service [AIVD] of the Netherlands. In their 2012 analysis on jihadism on the internet, it was suggested that most of the people lack the willingness, the knowledge, the expertise and the connections to become a terrorist. This underscores the value of being cognizant of factors that influence one’s decision not to be involved in terrorism.

There is a dearth of terrorism studies that have adopted the use of empirical data to drive conclusions (Schoorman & Eijkman, 2013). Thus, the use of sympathisers as a comparison group against the foreign fighter sample not only increases reliability and validity as the information collected is primary data but also acts as a ‘proper’ control group. This is in comparison to many terrorism studies where the terrorists are compared against violent criminals (e.g., Cook, 2014) and students (e.g., Stankov et al., 2010). As there are distinct differences among these groups, the violent criminal and student populations may not serve as ideal comparison groups. Indeed, there are several fundamental differences to keep in mind in comparing violent criminals with terrorists. For example, although prior criminal acts have been found to predict

future offending (Monahan, 2012), no such correlation has been demonstrated among terrorists. Furthermore, most terrorists do not lack education, employment or have had troubled childhoods (Silber & Bhatt, 2007). They are, in fact, very ‘normal’ in comparison to the general population. Terrorists also generally do not have a predisposition towards aggressive behaviour, unlike other violent crime offenders (Pressman, 2009); terrorists see violence as a viable means to achieve their agenda.

However, our findings comparing sympathisers with foreign fighters have to be interpreted with caution, as the generalisability of the findings is limited. There are a few limitations that must be taken into account. Firstly, this is an exploratory study with a small sample size. There is, therefore, a need to increase the sample of foreign fighters and sympathisers for future research. Secondly, it is important to recognise that these factors offer only a snapshot of an individual’s beliefs at a particular moment in time, and regular assessment is required if law enforcement needs to portray a complete picture of the person of interest. Thirdly, such forms of online analysis are dependent on and restricted by the amount of information available (Egan et al., 2016). Thus, there is a need to move beyond Twitter and search for other social media platforms (e.g., Facebook, Instagram, Ask.fm, Tumblr, WordPress) that foreign fighters and sympathisers may use. Lastly, as Gill et al. (2017) argue:

There is no easy offline versus online violent radicalisation dichotomy to be drawn. It may be a false dichotomy. Plotters regularly engage in activities in both domains. Often their behaviours are compartmentalised across these two domains ... A preoccupation with only checking online behaviours may lead an intelligence analyst to miss crucial face-to-face components of a plot’s technical development or a perpetrators’ motivations. (p. 100)

Thus, there is an essential need to complement these online assessments with offline information gathering.

In conclusion, the current study proposes a basis for future research in the field, as it is one of the first attempts to empirically explore and compare ISIS foreign fighters versus sympathisers based on their social media postings, and provides a unique contribution to the field of terrorism.

CHAPTER FIVE: COMPARING ISIS FOREIGN FIGHTERS VERSUS SYMPATHISERS: INSIGHTS FROM THEIR SOCIAL MEDIA POSTS⁵

The goal of this chapter was to address two main implications that arose from chapter 4, which was an exploratory probe to compare the social media posts of ISIS foreign fighters and sympathisers using the 12 factors and their associated 42 indicators.

The first implication pertains to a need to boost the sample size and assemble a panoptical view of their social media footprints. The design of chapter 4 did not allow us to see beyond the postings on Twitter and was limited in terms of the measures used to illuminate the differences between the two samples. To address this implication, several enhancements were made. First, the sample size was increased. Other social media sites frequented by ISIS supporters were also surveyed in this study. Next, recognising the importance of examining the ‘radical score’ of postings (see Scrivens et al., 2018), a new criterion to identify the ‘severity’ of the coded posts was introduced. By measuring severity together with the binary categorisation of the indicators would allow us to gain a more holistic appraisal of the data in order to identify any potential differences between the fighters and sympathisers. Based on these changes, a sample of 17 foreign fighters and 19 sympathisers was gathered using purposive sampling, and a total of 22,457 social media posts was used for analysis.

The second implication raised by chapter 4 is whether the findings could be replicated using a larger sample. In this study, new types of quantitative and

⁵ This chapter was presented at the ‘Asia Pacific Association of Threat Assessment Professionals (APATAP) Conference 2020’ at Melbourne, Australia, February 26, 2020.

qualitative data analyses were introduced. To overcome the statistical issue of analysing variables that have zero occurrence (i.e., indicators were not mapped against any postings), the Fisher's exact test—which was also utilised by Egan et al. (2016) and Meloy et al. (2015) to compare between different terrorist groups—was employed. Furthermore, multidimensional scaling (MDS; see Bloombaum, 1970) was utilised to identify any potential associations among the indicators. This new approach is based on previous work on crimes (Santtila et al., 2005; Trojan & Salfati, 2010) and terrorism (Goodwill & Meloy, 2019; Horgan et al., 2018), which suggest that certain behavioural indicators would cluster together. The final refinement pertains to the identification of the 'best' indicator using logistic regression (see Peng et al., 2002). This statistical technique offers a unique opportunity to describe and test the relationship between the categorical outcome of travelling or not travelling to join ISIS, and the entire set of 42 indicators.

Based on the enhancement and refinement to the research design, the objectives of this chapter are as follows: The first objective is to differentiate ISIS fighters and ISIS sympathisers based on their social media posts, and the second objective is to identify the 'best' predictor for identifying ISIS fighters.

1. Method

The criteria and steps taken for the identification of the sample of foreign fighters and sympathisers and their social media posts are similar to that of chapter 4 unless stated otherwise.

1.1 Inclusion Criteria for Sample

A sample of ISIS supporters (foreign fighters and sympathisers) was used for case analyses and comparisons. Out of the four inclusion criteria

mentioned in chapter 4, three criteria were revised to suit the objectives of this chapter. Firstly, in addition to Twitter, other social media sites such as Facebook, Ask.fm, that were frequented by ISIS supporters were surveyed. While Twitter is known for being the preferred platform for ISIS supporters (Conway et al., 2019), it is crucial to collect as much open-source information from other social media sites. Secondly, the selected accounts can originate from any parts of the world, and not just from the United Kingdom. The selected social media accounts must also be posting in a language⁶ that I understood. The last revision concerns the time period for analysis: from 2012 to 2015. Given that ISIS social media accounts were subjected to massive takedown by social media companies and authorities in 2015 (Ceron et al., 2019), the endpoint for the sampling frame for analysis was slated to be June 2015. As for the start point, it was revised from 2013 to 2012 to capture more data about the accounts before ISIS (or its earlier iteration) gained prominence on social media in 2013 (Berger & Morgan, 2015). The only new criterion revolves around the need for each selected account to have at least ten postings to allow for meaningful exploration and analysis.

1.2 Identification of Sample

Data collection was undertaken from March to June 2015. The search methodology utilised in this study is similar to previous research that examined terrorists' social media accounts (e.g., Dillon et al., 2019; Klausen, 2015; Knight et al., 2019). An initial sample of 59 accounts was identified using purposive sampling. This sampling technique helps to identify samples that met

⁶ Accounts that post in Arabic were not considered for analysis as I lacked the proficiency to understand the language. Future studies could engage a translator to decipher Arabic accounts.

the abovementioned criteria. Twenty-three accounts (eight foreign fighters and 15 sympathisers) were excluded from further analysis due to the following reasons: lack of information to verify the travel dates for the fighter sample and status as an ISIS supporter, language barrier, and lack of postings in the social media accounts.

Table 13
Information about the Social Media Accounts of 36 ISIS Supporters (2012 to 2015)

Group	Identifier	Total number of postings across all platforms	Coded number of postings ^a (% ^b)	Time period of posting	Country
Foreign fighter	A1	2294	57 (2.4)	2013	UK
	A2	2330	39 (1.6)	2012 – 2014	UK
	A3	178	41 (23.0)	2013 – 2014	UK
	A4	3085	76 (2.4)	2012 – 2013	UK
	A5	1399	97 (6.9)	2012 – 2014	UK
	A6	731	62 (8.4)	2014	UK
	A7	361	37 (10.2)	2013 – 2014	UK
	A8	377	24 (6.2)	2014	UK
	A9	166	28 (16.8)	2013 – 2014	UK
	A10	2919	34 (1.1)	2013	UK
	A11	1168	4 (3.6)	2014	UK
	A12	35	4 (11.4)	2013	US
	A13	182	16 (8.7)	2013 – 2014	Malaysia
	A14	126	7 (5.5)	2012 – 2014	Malaysia
	A15	58	12 (20.6)	2012 – 2014	Indonesia
	A16	1550	27 (1.7)	2012 – 2014	Indonesia
	A17	246	12 (4.8)	2012 – 2014	Indonesia
Sympathiser	B1	119	52 (43.6)	2015	UK
	B2	199	30 (15.0)	2015	UK
	B3	367	34 (9.2)	2014 – 2015	UK
	B4	136	22 (16.1)	2012 – 2015	UK
	B5	111	20 (18.0)	2013 – 2015	UK
	B6	109	26 (23.8)	2015	UK
	B7	17	8 (47.0)	2015	UK
	B8	10	4 (40.0)	2015	UK
	B9	174	31 (17.8)	2012 – 2015	UK
	B10	196	30 (15.3)	2015	UK
	B11	32	7 (21.8)	2012 – 2015	UK
	B12	1847	77 (4.1)	2014	India
	B13	296	49 (16.5)	2012 – 2015	Indonesia
	B14	1038	28 (2.6)	2012 – 2015	Indonesia
	B15	155	18 (11.6)	2012 – 2014	Malaysia
	B16	322	29 (9.0)	2012 – 2015	Malaysia
	B17	54	9 (16.6)	2012 – 2015	Malaysia
	B18	59	9 (15.2)	2014	Indonesia
	B19	11	2 (18.1)	2013 – 2015	UK

Note. ^a For the foreign fighters, the analysis will be conducted on the posts taken from the time they set up their accounts or from 2012, until the date they made the travel.

^b This is the percentage of post used for analysis in relation to the total number of posts across all social media accounts.

Eventually, a sample of 36 ISIS supporters with 22,457 posts was derived. Table 13 details the information about these accounts. There were 17 foreign fighters ($M_{post} = 1,012.06$, $SD_{post} = 1,061.27$) and 19 sympathisers ($M_{post} = 276.42$, $SD_{post} = 444.73$). There were 23 (63.8%) U.K. accounts, 6 (16.7%) Indonesian accounts, 5 (13.9%) Malaysian accounts, 1 (2.7%) U.S. account, and 1 (2.7%) Indian account. The sample was predominantly from the United Kingdom; studies have shown that foreign fighters from the United Kingdom were more active on social media relative to foreign fighters from other countries (Klausen, 2015; Rowe & Saif, 2016). The names of the account holders were not disclosed, and all the online handles of the accounts were de-identified and given specific identifiers—e.g., A1 for accounts belonging to foreign fighter 1.

Open-source information was captured from the following social media platforms—Twitter (19,741; 87.9%), Facebook (2,647; 11.7%), Ask.fm (67; 0.2%), and Instagram (2, 0.0%). No data was collected from privatised communications and accounts. Similar to chapter 4, analysis of the fighters revolves around the posts that were created from the time they set up the accounts (or from 2012) to the date that they travelled to the Middle East. As for the sympathiser group, an analysis was conducted on the posts that were collected from 2012 to 2015.

1.3 Data Coding

Three independent coders, who were blind to the hypotheses of the study, coded the 36 accounts and their 22,457 postings. They were trained in the use of the codebook and were instructed to indicate the presence or absence of an indicator as well as record the frequency of their occurrence. In addition,

when there was evidence, they were told to rate the ‘severity’ of the social media posts on a range from ‘1’ (least severe) to ‘5’ (most severe) for indicators belonging to the following four factors: “perceived grievances” (PG), “redemption and the pursuit for significance” (S), “readiness to use violence” (R), and “intolerance towards multi-religious, multi-racial living” (I). These factors were chosen because they have the highest likelihood of capturing the ideological inclinations of the individual, which research suggests would differ from person to person (Scrivens et al., 2018) and vary according to the extent of their radicalisation trajectory (Holbrook & Horgan, 2019). The coders thus looked at the overall context of a coded post to discern its level of severity.

1.3.1 Interrater Reliability

To assess the consistency between the three coders, intra-class correlation (ICC; Shrout & Fleiss, 1979) was used to calculate interrater reliability. In this case, a two-way random effects model, mean of 3 coders, consistency measure of ICC was employed. Table 14 displays the ICC agreement between the three coders.

Table 14
Intra-class Correlation (ICC) Agreement Between the Three Coders

Factors	ICC ^a	95% CI
<u>Frequency Rating ^b</u>		
Perceived grievances (PG)	.80	-.00, .97
Knowledge and skill to commit terrorist offences (K)	.85	-.55, .99
Redemption and the pursuit for significance (S)	.84	.00, .99
Readiness to use violence (R)	.84	.41, .97
Commitment to terrorist groups (C)	.89	.33, .99
Intolerance towards multi-religious, multi-racial living (I)	.88	.26, .99
Online relationship building with like-minded individuals (OR)	.83	-.74, .99
Involvement in the terrorist online community (OC)	.89	.31, .99
Individual-centric protective elements (IP)	.82	-.15, .98
Online environment-centric protective elements (OP)	.91	-2.20, 1.00
<u>Severity Rating</u>		
Perceived grievances (PG)	.86	.76, .92
Redemption and the pursuit for significance (S)	.76	.54, .88
Readiness to use violence (R)	.80	.63, .90
Intolerance towards multi-religious, multi-racial living (I)	.83	.69, .91

Note. ^a ICC two-way random effects model, mean of 3 coders, consistency measure.

^b The factors of “personal uncertainty” (P) and “negative social support” (N) were not included due to insufficient ratings.

According to Koo and Li (2016), ICC values are considered to be moderate, good, and excellent if the values are between .05 and .75, between .75 and .9, and larger than .9 respectively. For the frequency ratings, the ICC values range from .80 to .91, suggesting that the coders exhibited good to excellent inter-rater reliability. For the severity ratings, there is a good degree of interrater reliability across the four factors—ICC values range from .76 to .86. With regards to the disagreements, they were resolved by having the three coders to discuss and come to a consensus.

2. Results

Out of the 22,457 posts, 1,101 (4.9%) were coded. Bivariate analyses (Fisher's exact test [FET], Mann-Whitney U test) were used to examine the differences between ISIS foreign fighters and sympathisers. In addition to this primary analysis, MDS explored how the indicators may cluster across the two samples. Following which, a binary logistic regression was computed to identify the key predictor(s) for someone to become a foreign fighter.

2.1 Differences Between ISIS Foreign Fighters and Sympathisers

2.1.1 Prevalence of Factors and Indicators Across the Two Samples

The findings indicate that whilst there is a comparatively high number of posts that evidenced the indicators across the fighter sample as compared to the sympathisers, the difference was statistically significant for only nine of them—see Table 15.

The account holders who became foreign fighters have a significantly higher likelihood of displaying the following eight indicators. First, they would post photos of weapons, and in some instances, together with the Quran on their social media (indicator K2), $p = .04$, FET. The proportion of K2 observed

amongst the fighters (.23) is 23.5% points higher than those found in the sympathiser sample (.00). Second, fighters would express the desire to migrate to the Islamic caliphate (indicator S2), $p = .03$, FET. The proportion of S2 observed in the fighter group (.35) is 30% points higher than those found in the sympathiser sample (.05). Third, fighters would express contempt for their lifestyle and behaviours (indicator S3), $p = .03$, FET. For example, one of the fighters said: “I ask myself why is it so hard to wake up for night prayer and not to get up for work? Do I fear my boss than my creator?”. The proportion of this indicator found in the fighter group (.58) is 37.7% points higher than those found amongst the sympathisers (.21). Next, they would show the desire to adopt a new worldview (indicator P1), $p = .01$, FET. The proportion of P1 seen in the fighter group (.29) is 29.4% points higher than the sympathiser sample (.00). Fifth, fighters would strongly encourage their family and friends to defend Islam by joining ISIS, $p = .01$, FET. The proportion of this indicator, R2, observed in the fighter group (.70) is 44.3% points higher than those found amongst the sympathisers (.26). One of the fighters said, “other than that \$ isn’t a necessity so brothers/sisters make movements asap and stop with the excuses and make hijra fi sabilillah”. Sixth, they would express their willingness to sacrifice their lives for ISIS (indicator R3), $p = .00$, FET. The proportion of R3 found amongst the fighters (.35) is 35.3% points higher than the sympathiser sample (.00). Next, fighters would share their intention to join ISIS in Syria, $p = .01$, FET. The proportion of this indicator, R7, that is present in the fighter group (.41) is 35.9% points higher than the R7 found in the sympathiser sample (.05). Finally, fighters would reach out to terrorists and/or known key nodes in the terrorist online communities (indicator OR1), $p = .00$, FET. The proportion

of OR1 seen in the fighter group (.47) is 41.8% points higher than the OR1 found amongst the sympathisers (.05). For instance, one of the fighters said: “wanting to migrate to #Damascus #Syria In Sh? All?h. If you’re from there, @ me with some directions. Want to move sooner rather than later”.

There seems to be a cluster of three indicators (R2, R3, R7) belonging to the factor “readiness to use violence”. This suggests that the fighters were showing their inclination towards ISIS by inciting others to fight for ISIS as well as wanting to be personally involved in fighting for ISIS. It could also well be the case that for this group of individuals, the quest to become a fighter was underlined by their desire to repent and do something meaningful, as exemplified by the indicators S2 and S3. For instance, after being influenced by the ideology of ISIS, the fighters may fixate on the need to live in a state governed only by Islamic laws: “I want to live in a world where theirs no internet, tv, mobiles, toilets, people, dogs, cold weather, pork, all I want is sand and the book”.

In contrast, the sympathisers were more likely to display ISIS symbols, such as the black flag with ISIS insignia, on their social media (indicator C2), $p = .00$, FET. The proportion of C2 that is present in the fighter group (.17) is 50.4% points lower than those observed in the sympathiser sample (.68). The lower number of fighters manifesting this indicator could be due to them not wanting to attract unwanted law enforcement attention. Alternatively, it could be attributed to the support activities that sympathisers, or what Brachman (2008) labelled as ‘jihobbyists’ are known to engage in—e.g., praising ISIS, celebrating its success, showing solidarity with the group.

Table 15*Prevalence of Factors and Indicators Across ISIS Supporters*

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Sympathiser (<i>n</i> = 19)	Overall (<i>N</i> = 36)	Foreign fighter (<i>n</i> = 17)			Sympathiser (<i>n</i> = 19)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
<u>Perceived grievances (PG)</u>									
PG1: Publicise the injustices targeted at one’s own community, faith, or belief	94.1%	78.9%	86.1%	3.35	2.71	57	3.53	3.58	67
PG2: Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice	52.9%	47.4%	50%	.71	.84	12	.89	1.32	17
PG3: Express frustration with the injustice targeted at one’s own community, faith, or belief	76.5%	63.2%	69.4%	1.88	1.99	32	1.68	2.33	32
PG4: Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice	58.8%	36.8%	47.2%	1.35	1.65	23	.63	1.01	12
PG5: Openly challenge certain group(s) of concern about the injustice	41.2%	52.6%	47.2%	.82	1.23	14	1.16	1.53	22
<u>Knowledge and skill to commit terrorist offences (K)</u>									
K1: Demonstrate an interest in learning combat skills	11.8%	15.8%	13.8%	.24	0.66	4	0.21	.53	4
K2: Showcase interest in the use of weapons and explosives	23.5% *	0%	11.1%	.29	0.58	5	.00	.00	0
K3: Have information on explosives-bomb making	0%	0%	0%	.00	.00	0	.00	.00	0
<u>Redemption and the pursuit for significance (S)</u>									
S1: Desire to partake in humanitarian activities in countries associated with terrorism opportunities	29.4%	15.8%	22.2%	.47	.80	8	.16	.37	3
S2: Desire to repent by migrating to countries associated with terrorism opportunities	35.3% **	5.3%	19.4%	.88	1.31	15	.05	.22	1
S3: Express feelings of contempt for own prior practices	58.8% **	21.1%	38.8%	1.29	1.61	22	.26	.56	5

Table 15 (continued)

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Sympathiser (<i>n</i> = 19)	Overall (<i>N</i> = 36)	Foreign fighter (<i>n</i> = 17)			Sympathiser (<i>n</i> = 19)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
S4: Intention to search for opportunity to do something meaningful	58.8%	52.6%	55.5%	1.24	1.30	21	.74	.87	14
<u>Personal uncertainty (P)</u>									
P1: Desire to explore different ideologies and beliefs—inconsistent identity	29.4% ***	0%	13.8%	.53	1.06	9	.00	.00	0
<u>Readiness to use violence (R)</u>									
R1: Voice strong support for the use of violence towards a certain group(s) of concern as a viable solution	58.8%	31.6%	44.4%	1.06	1.19	18	.37	.59	7
R2: Incite friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief	70.6% ***	26.3%	47.2%	2.47	2.18	42	0.47	1.17	9
R3: Express willingness to die for cause, and achieve martyrdom	35.3% ****	0%	16.7%	1.18	2.12	20	.00	.00	0
R4: Demonstrate a preoccupation with an individual from group(s) of concern as a potential target	35.3%	15.8%	25%	.59	.87	10	.16	.37	3
R5: Display themselves as a protector/hero of their fellow believers of the same faith, religion or belief	11.8%	0%	5.5%	.12	.33	2	.00	.00	0
R6: Perceive an urgency to act and that non-violent alternative are ineffective solutions	35.3%	15.8%	25%	.53	.80	9	.16	0.37	3
R7: Indicate their intention to travel and participate in overseas conflict	41.2% ***	5.3%	22.2%	.71	1.26	12	.05	.22	1
<u>Commitment to terrorist groups (C)</u>									
C1: Quotations from/ associations with personalities known for their radical views	52.9%	21.1%	36.1%	.71	.77	12	.53	1.42	10

Table 15 (continued)

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Sympathiser (<i>n</i> = 19)	Overall (<i>N</i> = 36)	Foreign fighter (<i>n</i> = 17)			Sympathiser (<i>n</i> = 19)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
C2: Identify with symbols of known terrorist groups on one's online profile	17.6%	68.4% ****	44.4%	.18	.39	3	1.11	1.04	21
C3: Display their public allegiance to terrorist groups	11.8%	26.3%	19.4%	.12	.33	2	.37	.68	7
C4: Praise and defend terrorist groups	58.8%	73.7%	66.6%	2.35	4.01	40	3.21	3.08	61
<u>Intolerance towards multi-religious, multi-racial living (I)</u>									
I1: Force friends, colleagues or family to distance themselves from certain group(s) or community	17.6%	42.1%	30.5%	.18	.393	3	.68	1.20	13
I2: Dehumanise group(s) of concern who hold different viewpoints/ beliefs system	35.3%	31.6%	33.3%	.59	1.00	10	.53	.90	10
I3: Dissatisfaction with local cultures, practices, values, and governance	100%	73.7%	86.1%	6.18	4.26	105	3.00	2.86	57
I4: Anti-integration messaging—exclusivity of one's own community, faith, or belief	76.5%	68.4%	72.2%	2.18	2.15	37	2.53	3.22	48
<u>Online relationship building with like-minded individuals (OR)</u>									
OR1: Attempt to reach out to terrorists	47.1% ****	5.3%	25%	1.82	2.72	31	.05	.22	1
OR2: Develop and disseminates terrorist content	0%	0%	0%	.00	.00	0	.00	.00	0
OR3: Attempt to set up physical meeting with terrorists	11.8%	0%	5.5%	.29	.98	5	.00	.00	0
<u>Involvement in the terrorist online community (OC)</u>									
OC1: Possess terrorist documents, music, videos, etc. on computer or mobile devices	41.2%	36.8%	38.8%	.59	.79	10	.42	.60	8
OC2: Host web-links to other online platforms that contain terrorist context	11.8%	31.6%	22.2%	.35	1.22	6	.79	1.54	15
OC3: Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism	35.3%	15.8%	25%	.65	1.11	11	1.26	4.59	24
OC4: A sudden increase in the user's activity	0%	0%	0%	.00	.00	0	.00	.00	0

Table 15 (continued)

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Sympathiser (<i>n</i> = 19)	Overall (<i>N</i> = 36)	Foreign fighter (<i>n</i> = 17)			Sympathiser (<i>n</i> = 19)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
<u>Negative social support (N)</u>									
N1: Presence of supportive family members and friends that encourage involvement in the terrorist online communities and/or terrorist offending	5.9%	0%	2.7%	.06	.24	1	.00	.00	0
<u>Individual-centric protective elements (IP)</u>									
IP1: Presence of supportive family members and friends that discourage terrorist offending	5.9%	5.3%	5.5%	.06	.24	1	.05	.22	1
IP2: Demonstrate willingness to engage in discussions of ideology and the use of violence	5.9%	26.3%	16.6%	.06	.24	1	.26	.45	5
IP3: Disillusioned with using violence to solve problems	0%	0%	0%	.00	.00	0	.00	.00	0
IP4: Demonstrate an appreciation for diversity	5.9%	15.8%	11.1%	.06	.24	1	.16	.37	3
<u>Online environment-centric protective elements (OP)</u>									
OP1: Inability to obtain access to the terrorist online community	0%	0%	0%	.00	.00	0	.00	.00	0
OP2: Recognise and fear the detection by law enforcement and social media companies	5.9%	5.3%	5.5%	.12	.48	2	.05	.22	1

Note. Analysis based on Fisher's exact test: * $p = .04$. ** $p = .03$. *** $p = .01$. **** $p = .00$.

Interestingly, it appears that the six protective indicators do not have the discriminatory power of differentiating the fighters from the sympathisers.

While it may sound intuitive that sympathisers should manifest more of such indicators, the results do not support such assumptions. It may be that sympathisers were very much akin to the fighters in terms of their shared common attraction towards ISIS, but were dissuaded from travelling by other variables, other than protective factors.

Of interest here are the three statistically significant indicators that exhibited a high difference in proportions: OR1 (41.8%), R2 (44.3%), and C2 (50.4%). This suggests that foreign fighters are more likely to reach out to terrorists and/or key nodes in the terrorist online communities, and encourage their family and friends to join them in defending Islam. In contrast, sympathisers tend to show their support to the ISIS' cause by overtly displaying ISIS related symbols on their social media.

2.1.2 Severity Ratings of Factors Across the Two Samples

As severity ratings are generally subjective in nature, there may be potential outliers that would skew the results. Hence, I decided to use the median of the severity ratings (instead of the mean) as the unit of measurement—see Figure 6.

The ISIS supporters who became foreign fighters had posts that were rated significantly more severe across all four factors. Fighters ($Mdn = 2.00$) have created posts espousing grievances that were rated more severe, as compared to the sympathisers ($Mdn = 2.00$), $U = 77.00$, $p = .00$, $r = -.48$. They ($Mdn = 2.00$) were also creating posts that expressed a higher level of intolerance towards communal living as compared to the sympathisers ($Mdn =$

2.00), $U = 93.50$, $p = .02$, $r = -.38$. Furthermore, the manner in which fighters ($Mdn = 2.5$) expressed their need to engage in meaningful activities was rated significantly more severe than that of sympathisers ($Mdn = 1.00$), $U = 65.00$, $p = .00$, $r = -.52$. In terms of expressing their readiness to use violence, fighters ($Mdn = 3.00$) reported significantly more severe ratings as compared to sympathisers ($Mdn = 1.00$), $U = 82.00$, $p = .01$, $r = -.42$. It is noteworthy that the effect sizes were between the range of medium to large, suggesting that fighters do express themselves more radically across these four factors. In other words, instead of simply sharing incidents of injustices, fighters are more likely to engage in downright condemnation of these incidences.

Figure 6
Median Severity Ratings Across Four Factors

Note. The number in the () represents the number of ISIS supporters (fighters or sympathisers).

* This refers to the median score for each subsample.

The foreign fighters' more radical worldviews may have led them down a 'slippery slope' trajectory in terms of their involvement with ISIS that eventually culminated in them travelling to join the group, as compared to the sympathisers who support the group through acts of activism via the internet. Alternatively, the fighters could be attempting to portray a positive image about their commitment towards ISIS and attract the attention of recruiters in the

online networks. This inference dovetails with the theory on group polarisation which posits that individuals tend to gravitate towards the extreme in their discussions, which then leave “behind a hard-core group that increasingly becomes more radicalised” (Gupta, 2011, p. 39). However, it remains to be seen whether the differences in the severity ratings amongst the ISIS supporters would be robust over time. Future research that can explore the temporal relationship between severity ratings and terrorists’ supporters is, therefore, warranted.

2.1.3 Relationships Between the Indicators Across the Two Samples

It was observed that some indicators seem to be co-occurring within the sample of fighters and sympathisers. To better understand such co-occurrence of indicators, MDS was utilised as it allows us to elucidate how the indicators are interrelated, and visualise how they may manifest differently for the two groups of ISIS supporters. Indicators that regularly co-occur would register a high level of association and be plotted closer together in a two- or three-dimension space (Bishopp & Hare, 2008; Powis et al., 2019).

For this study, Multidimensional Unfolding (PREFSCAL) in SPSS was used to produce a three-dimension space that plotted 37 indicators for all the ISIS supporters (fighters and sympathisers, $N = 36$). Five indicators that were not mapped to any posts were excluded from the analyses: K3, OR2, OC4, IP3, and OP1. To determine the model’s goodness of fit, Kruskal’s stress, which provides an index ranging from .20 to .02, was used (Kruskal, 1964). The smaller the stress value, the better the fit. The current model has a good fit, as the reported stress value was .04. While the ‘line’ used to separate and derive clusters of variables on the plot is determined by the user (i.e., subjective in

nature), researchers have recommended the use of theoretical insights to guide the location of the line (see Goodwill & Meloy, 2019).

2.1.3.1 Three Clusters of ISIS Supporters Found. Figure 7 locates the ISIS supporters on the plot. The foreign fighters ($n = 17$) are represented by green pentagons, whereas red triangles represent the sympathisers ($n = 19$). It appears that the fighters are more closely clustered together compared to the sympathisers.

Figure 7
Multidimensional Scaling Plot of ISIS Supporters

Note. Foreign fighters (green pentagon, $n = 17$) and sympathisers (red triangle, $n = 19$)

Further inspection of the plot reveals that there are three clusters of interest. Two lines were drawn onto the MDS plot to demarcate the foreign fighter cluster, the sympathiser cluster, and the 'foreign fighter-sympathiser'

cluster. For those fighters and sympathisers represented in the ‘foreign fighter-sympathiser’ cluster, their social media posts were likely mapped to similar indicators due to their close distance on the plot. This has two implications. Firstly, it could mean that the sympathisers in this cluster are very similar to some fighters, and probably have a high chance of becoming foreign fighters. Secondly, it alludes to the nature of the terrorist online communities where like-minded individuals—regardless of them being fighters or sympathisers—are closely connected to one another, and as a result, engage in many similar online activities and discussions.

2.1.3.2 Six Clusters of Indicators Found. MDS was carried out for all the 37 indicators. Six clusters of indicators were identified that broadly accord with the person-centric (“frustration”, “negative fixation”, “intention to act”), psychosocial (“strong support towards group”, “contribute to the online community”), and protective (“deterrence”) dimensions—introduced in chapter 2. Figure 8 locates these six clusters of indicators, which are represented as different coloured circles.

Four out of the six clusters were located within close proximity to one another, suggesting that the indicators within were likely to co-occur. Of particular interest here is the association amongst the “deterrence”, “negative fixation”, and “intention to act” clusters. This finding suggests that one’s likelihood to act on their radical beliefs towards a particular target is likely to be mitigated by the presence of deterrence-related indicators. This is unsurprising given that research on deradicalisation and disengagement has shown how the presence of protective factors can buffer against the risk of someone becoming radicalised (Horgan et al., 2017; Sarma, 2017).

As for the two other clusters of “contribute to the online community” and “frustration”, they are remotely positioned on the plot, suggesting a relatively low association with other clusters of indicators. In other words, the indicators within these two clusters are likely to be observed as stand-alone occurrence.

Figure 8
Multidimensional Scaling Plot of the 37 Indicators

Note. The indicators are represented by the circles and are differentiated by the different colour coding. Cluster on “contribute to the online community” constitutes the following: S4, C2, C4, and OC2. Cluster on “frustration” constitutes the following: PG1, PG3, I3, and I4. Cluster on “strong support towards group” constitutes the following: PG4, S3, R1, R2, and OR1. Cluster on “negative fixation” constitutes the following: PG2, PG5, R4, C1, I1, I2, OC1, and OC3. Cluster on “deterrence” constitutes the following: IP1, IP2, IP4, and OP2. Cluster on “intention to act” constitutes the following: K1, K2, S1, S2, P1, R3, R5, R6, R7, C3, OR3, and N1.

2.1.3.3 Overlaying the ISIS Supporters with the 37 Indicators. The

MDS analysis highlighted three behavioural typologies of ISIS supporters—see Figure 9.

Figure 9

Multidimensional Scaling Plot of ISIS Supporters and the 37 Indicators

Note. Foreign fighters (green pentagon, $n = 17$) and sympathisers (red triangle, $n = 19$). The indicators are represented by the circles and are differentiated by the different colour coding. The two black lines are used to demarcate the three clusters of ISIS supporters.

The first behavioural typology pertains to that of the ISIS sympathisers.

Located within the cluster of indicators known as “contribute to the online community”, sympathisers have a high degree of association with behaviours such as identifying with symbols of ISIS on their social media, praising and defending ISIS, and sharing ISIS propaganda via web-links. In a nutshell, these non-violent ISIS supporters may have perceived acts of contributing to the online community as a meaningful endeavour. Thus, these individuals may not have the interest to participate in physical battle and are contended to contribute in their capacity as armchair jihadist (Saifudeen, 2016) through acts of creating and disseminating ISIS-related propaganda (Knight et al., 2019).

The MDS results further suggest the presence of a second behavioural typology of foreign fighters. This group of ISIS supporters shows a strong co-occurrence with indicators from the clusters of “strong support towards group” and “frustration”. Foreign fighters are generally frustrated by the grievances they perceived, especially with their local practices. Of particular interest is the sizable congregation of fighters around one particular indicator, I3 (“dissatisfaction with local cultures, practices, values, and governance”), which has a recorded frequency of 105. Moreover, they would also espouse sentiments highlighting the exclusivity of ISIS ideology and the strong moral compass of those who adhered to it. This observation corroborates with the findings by Dawson et al. (2016), who found that many of the ISIS foreign fighters were motivated to travel to Syria by their perceived moral high ground. Such worldviews are likely shaped by the narratives propagated by ISIS (Tolis, 2019; Vergani & Bliuc, 2018).

Furthermore, there is some degree of association among the fighters and the indicators located within the “strong support towards group” cluster—albeit weaker than the association between the fighters and the indicators from the “frustration” cluster. This suggests that fighters would express hatred and endorse the use of violence towards the enemies of ISIS. There is also an increased likelihood of them reaching out to key nodes within the ISIS online community, and inciting others to join ISIS. It nonetheless makes sense that those preparing to fight would demonstrate a higher association with this cluster of indicators. This could possibly represent the behavioural indicators that fighters would engage in whilst they rationalise and reconcile their internal decision to travel to Syria.

It is also evident from the MDS analysis that some foreign fighters and sympathisers have clustered together as a separate entity forming the ‘fighter-sympathiser’ group. This group is located in close locality to the indicators from the “frustration” cluster and is further away from those belonging to the “contribute to the online community” cluster. Although there is no clear picture from the data, it does appear as if sympathiser, who starts to espouse frustration that arises from their perceived grievances, are in the process of becoming foreign fighters. However, this deduction must also be interpreted with reference to the group’s weak association with indicators from the “strong support towards group” cluster. As this cluster of indicators is not associated with the sympathiser group, the indicators within can potentially be used to distinguish the foreign fighters from the sympathisers.

There was no identifiable difference in the distance between these three groups of ISIS supporters and the indicators in the “negative fixation”, “deterrence”, “intention to act” clusters. This could be attributed to the low frequency of these indicators and/or the unconfirmed negative correlation of these indicators with that of an individual becoming a fighter or sympathiser. In other words, the social media posts of ISIS foreign fighters and sympathisers have a lower likelihood of being mapped to these indicators.

Given that the clusters of ISIS supporters and indicators were derived manually based on my interpretation (albeit guided by the framework presented in chapter 2 and my reading of the terrorism literature), it must be recognised that the findings are less useful at statistically predicting whether the presence of an indicator would indicate or suggest that an individual is becoming a fighter or sympathiser—which is the objective of the next section. Caution in

interpreting the MDS results is therefore recommended. Nevertheless, the MDS analysis does provide us with a geometric representation of how certain indicators are associated differently among the samples of foreign fighters and sympathisers, which is critical in enhancing our knowledge to detect radicalisation in social media posts.

2.2 Predictor(s) for Becoming an ISIS Foreign Fighter

As the outcome measures are binary in nature (1 = travel to ISIS—fighter, 0 = did not travel to ISIS—sympathiser), binary logistic regression (see Long, 1997) is the most appropriate statistical tool to identify the indicator(s) that can predict an individual's likelihood of becoming a foreign fighter. Thirty-eight indicators were input into the regression model to determine the strength of their predictive value across 22,457 social media postings. Four indicators (K3, OC4, IP4, OP1) were removed due to their low correlation values (see Kinnear & Gray, 2006).

The regression model was significant, $X^2(38, N = 22457) = 481.65, p = .00$, and it correctly classified 77.1% of posts that belong to the foreign fighters. The R^2 value was about .03, which means that the model was only able to explain 3.2% of the variation in predicting an ISIS foreign fighter. This low R^2 value is expected as the topic of analysis is a low base-rate event; in this case, out of the 22,457 postings, only 1,101 (4.9%) were coded. Furthermore, it can be attributed to the presence of other offline predictors on the online radicalisation process (Gill et al., 2017), which were not accounted for in this study. Nevertheless, despite that, 19 indicators were found to be significant predictors, as shown in Table 16. Thus, useful insights can still be drawn from these results.

Table 16*Logistic Regression Model for Predicting Who Becomes a Foreign Fighter*

Indicator	B (SE)	95% CI for odds ratio		
		Lower	Exp (B)	Upper
PG1: Publicise the injustices targeted at one's own community, faith, or belief	-1.41 (.18) **	.17	.24	.34
PG2: Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice	-1.59 (.37) **	.09	.20	.42
PG3: Express frustration with the injustice targeted at one's own community, faith, or belief	-1.25 (.25) **	.17	.28	.46
PG5: Openly challenge certain group(s) of concern about the injustice	-1.69 (.34) **	.09	.18	.35
S4: Intention to search for opportunity to do something meaningful	-.84 (.34) *	.21	.43	.84
C1: Quotations from/ associations with personalities known for their radical views	-1.06 (.42) *	.14	.34	.79
C2: Identify with symbols of known terrorist groups on one's online profile	-3.19 (.61) **	.01	.04	.13
C3: Display their public allegiance to terrorist groups	-2.50 (.80) **	.01	.08	.39
C4: Praise and defend terrorist groups	-1.66 (.20) **	.12	.18	.28
I1: Force friends, colleagues or family to distance themselves from certain group(s) or community	-2.71 (.64) **	.01	.06	.23
I2: Dehumanise group(s) of concern who hold different viewpoints/ beliefs system	-1.24 (.44) **	.12	.28	.69
I3: Dissatisfaction with local cultures, practices, values, and governance	-.71 (.16) **	.35	.48	.67
I4: Anti-integration messaging—exclusivity of one's own community, faith, or belief	-1.43 (.21) **	.15	.23	.36
OR1: Attempt to reach out to terrorists	2.21 (1.01) *	1.25	9.19	67.29
OC1: Possess terrorist documents, music, videos etc. on computer or mobile devices	-1.13 (.48) *	.12	.32	.83
OC2: Host web-links to other online platforms that contain terrorist context	-3.95 (1.03) **	.00	.01	.14
OC3: Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism	-2.12 (.37) **	.05	.12	.25
IP2: Demonstrate willingness to engage in discussions of ideology and the use of violence	-2.85 (1.09) **	.00	.05	.49
IP4: Demonstrate an appreciation for diversity	-2.34 (1.15) *	.01	.09	.92
Constant	1.24 (.01) **		3.48	

Note. B = regression coefficient; Exp (B) = odds ratio.

Postings are coded as 1 for 'travel to ISIS' and 0 for 'did not travel to ISIS'.

$R^2 = .03$; -2 Log likelihood = 23947.48; $N = 22457$

* $p < .05$. ** $p < .01$.

There were 18 significant negative indicators. These indicators do not predict the likelihood of an individual becoming a fighter, but instead, reduce

the odds of them doing so. ISIS supporters who have posts that are mapped to these 18 indicators would be less likely to travel to join ISIS, and their odds ratios range from .01 to .48 times of not travelling.

Only one significant positive indicator (OR1: “attempts to reach out to terrorists”) was found. In other words, a social media post that is mapped onto this indicator would increase the likelihood of the post creator to travel to Syria by 9.2 times (95% CI: 1.25, 67.29). This underscores just how important efforts to establish contacts with key nodes within the ISIS online communities play in propelling an ISIS supporter to become a foreign fighter. There are several potential explanations. It may be a deliberate move by aspirant travellers to elicit more practical information about how to make the journey into Syria, or simply just to receive words of encouragement from those who have already made the journey. Previous research has underlined the importance of establishing social networks on the radicalisation process. Based on their analysis of far-right groups, Caspi et al. (2012) found that the more connections a group has, the higher the risk of them engaging in acts of violence. In terms of ISIS, other studies have found similar results in that an individual’s connections to those who have already travelled, is a key determinant for them to become a foreign fighter (Holman, 2016; Reynolds & Hafez, 2019; Speckhard & Ellenberg, 2020).

Furthermore, these results lend weight to the earlier findings of this chapter. For example, OR1 is part of the “strong support towards group” cluster from the MDS plot, which was found to be associated with the foreign fighters. This suggests that attempts to detect OR1 could be enhanced if authorities were to also keep a lookout for other indicators within that cluster—i.e., PG4, S3,

R1, R2. In terms of its relation to the findings of the Fisher's exact test, OR1 is one of the three indicators that exhibited a high difference in proportions between the fighters (47%) and sympathisers (5.3%).

3. Discussion

Using a mix of bivariate and multivariate statistical analyses, this chapter built upon the research design from chapter 4 and examined how open-source materials can be used to differentiate two groups of ISIS supporters (foreign fighters and sympathisers), and identify which indicator(s) can be used to predict who will become a foreign fighter. This current work joins a growing literature (e.g., Dillon et al., 2019; Gruenewald et al., 2013), which utilised open-source data to generate empirical insights about terrorism.

This chapter found several significant differences between the two groups. Findings from the Fisher's exact test showed that fighters and sympathisers differ in how their social media postings were mapped against the indicators. For a start, most of the fighters were positive on 88% of the indicators, whereas most of the sympathisers were positive on 73% of them. This suggests some level of face validity as the factors and indicators were able to capture observable cyber behaviours and linguistic expressions created by the ISIS supporters. There were three significant differences with large effects. Foreign fighters tend to show their support to the ISIS' cause by expressing interest to perform acts of martyrdom and reaching out to like-minded others, whereas sympathisers tend to show their support towards ISIS by displaying insignia related to ISIS on their social media accounts.

Next, foreign fighters' posts were ascertained to be rated significantly more severe as compared to those made by the sympathisers across four factors, based on the Mann-Whitney U test.

To build a picture that reflects the full spectrum of indicators that may be associated with the online behaviours and expressions of the fighters and sympathisers, MDS was used to visualise how the indicators may cluster differently for these two groups. The results highlight the presence of three behavioural typologies. The first behavioural typology is that of the foreign fighters—they would engage in online behaviours that underline their frustration and strong support towards ISIS, in the build-up to their departure to Syria. Sympathisers, which is the second behavioural profile, are more inclined to perform 'outreach' efforts (e.g., sharing web-links) to the wider online community. Surprisingly, there is a third behavioural typology which comprises a mix of foreign fighters and sympathisers. Individuals in this group are located in close locality to the indicators from the "frustration" cluster (i.e., associated with the foreign fighters), and are further away from those belonging to the "contribute to the online community" cluster (i.e., associated with the sympathisers).

Finally, one key indicator was identified by the logistic regression model. The indicator (OR1: "attempts to reach out to terrorists") under the factor "online relationship building with like-minded individual" was found to increase the likelihood of the post creator to travel to Syria by 9.2 times. Thus, the findings do demonstrate some degree of postdictive validity in discriminating between those who travelled and those who did not.

This chapter was, however, unable to replicate the findings from the pilot study in chapter 4, where the factor “readiness to use violence” was found to be a significant factor in differentiating between ISIS foreign fighters and sympathisers. Given that this current chapter is an enhancement of the previous one (with a larger sample size as well as the adoption of new statistical techniques), the findings derived from this study should be viewed with more confidence. These new statistical analyses allow us to better examine the posts of the ISIS supporters in order to enhance our knowledge about detecting radicalisation in social media posts.

It must be recognised, however, that due to the small sample size (i.e., in relation to the entire spectrum of ISIS supporters), any sort of attempts to overgeneralise the findings should therefore err on the side of caution. From an online risk assessment perspective, this means using the entire set of factors and their indicators as an investigative template for screening suspicious social media accounts, and to then place more emphasis on the identified predictor of OR1 and its associated clusters of indicators (PG4, S3, R1, R2). Central to this is the recognition that many of these indicators described herein may be insignificant on their own in elucidating whether the threat is real.

3.1 Limitations

There are three limitations of interest. Firstly, the current dataset is a convenience sample of 36 ISIS supporters and hence is by no means representative of the larger corpus of ISIS supporters. Secondly, some of the supporters may not have publicised all their online engagements (i.e., they may engage in private chats), making it plausible that a proportion of their online behaviours and expressions have eluded empirical observation. While the

findings may not be generalisable to the entire terrorist population, it does help to further our understanding of this under-research population using primary data and provide some form of postdictive validity in the detection of radicalisation in social media posts. An additional limitation stems from the need to track changes in online behaviour or expression over time, which is an important area of research highlighted by other terrorism researchers (e.g., Goodwill & Meloy, 2019). In this study, it is unclear how the online behaviours and expressions of the ISIS supporters have changed over time. In light of this, future research should establish some form of temporal relationship so that a baseline from which deviations in terms of the online behaviours and expressions could be measured.

These limitations notwithstanding, the attempt to test the 12 factors and their associated 42 indicators does presents itself as a worthwhile endeavour to further our insights on detecting online radicalisation. A potential way forth is to validate these factors and indicators with a different group of foreign fighters, such as the anti-ISIS foreign fighters (Tuck et al., 2016). This will provide new avenues to investigate the external generalisability of the factors and indicators using a similar yet different set of foreign fighters.

CHAPTER SIX: COMPARING ISIS FOREIGN FIGHTERS VERSUS KURDISH FOREIGN FIGHTERS: INSIGHTS FROM THEIR SOCIAL MEDIA POSTS⁷

The goal of the study, detailed in this chapter, was to extend the findings of chapter 5, and investigate the external generalisability of the factors and indicators with other types of terrorists' supporters. In the current chapter, further evidence was sought using a group of terrorists' supporters who had joined the conflict in the Middle East. These are individuals (hereafter denoted as Kurdish foreign fighters) who made the journey from their home countries to join Kurdish militia groups to fight against ISIS (Bakker & Singleton, 2016; van Wilgenburg, 2015). Most of them voluntarily made requests to join the fight via the social media pages of Kurdish militia groups (Costello, 2016), and started travelling from Western countries such as the United States in 2014 (Orton, 2017). The nature of how they were being recruited via the internet, which is similar to the ISIS foreign fighters examined in chapter 5, therefore makes the Kurdish foreign fighters an ideal comparison group for the purpose of this chapter.

1. Background about Kurdish Foreign Fighters

Many of the Kurdish fighters travelled to join groups such as the Iraqi Kurdish Peshmerga, the Kurdish People's Defence Units (YPG), and the Dwekh Nawsha (Patin, 2015). In Syria, the main Kurdish group fighting against ISIS is the YPG. The YPG is affiliated to the Kurdistan Workers Party (PKK), which is recognised as a terrorist organisation by many countries and entities

⁷ An earlier version of this chapter was presented at the '2019 Asian Conference of Criminal & Operations Psychology (ACCOP)' at Singapore, July 10, 2019.

such as the European Union (Orton, 2017). Besides fighting against ISIS, the main agenda of the YPG is to seize territory and establish a self-declared autonomous Kurdish region in northern Syria, commonly known as Rojava. The Peshmerga is the armed forces of the Kurdish Regional Government in Iraq, who has been granted autonomy in 1992 to govern the northern part of Iraq, also known as Iraqi Kurdistan (van Wilgenburg, 2015). As for the Dwekh Nawsha, it is a Christian militia group that was established in 2014 to defend Iraq's Assyrian population from ISIS (Tuck et al., 2016). These militia groups have been instrumental in waging war against ISIS. In fact, the YPG and Peshmerga have been highlighted within the Dabiq magazine as ISIS most important adversaries on the ground (van Wilgenburg, 2015).

Several researchers have attempted to decipher the underlying motivations of the Kurdish foreign fighters. A recurring theme is their altruistic desire to help and protect persecuted Kurds from the atrocities committed by ISIS (Jayakumar, 2019). Some have cited frustration with their home country's foreign policy and the limited international response towards the plight of the Kurds (Bell, 2014), while others have sought the feeling of solidarity or adventurism (Morin, 2016). Interestingly, some of them were veterans who missed the lifestyle associated with a military career and have trouble adapting back to civilian lives (Orton, 2017). Notwithstanding the wide range of motivations, the consensus is that these motivations do overlap with some of those observed amongst the ISIS foreign fighters, leading researchers such as Fritz and Young (2017, p. 12) to remark that "anti-ISIS foreign fighters are reflections of jihadist foreign fighters".

1.1 Online Recruitment of Kurdish Foreign Fighters

While the recruitment materials and commentaries of Kurdish online communities may not be as sophisticated as that of ISIS (Koch, 2019), they still play an essential role in publicising of the Kurdish cause and in recruiting foreign fighters. One of the most prominent platforms is ‘The Lions of Rojava’ Facebook page, which is affiliated with the YPG. This Facebook page features images of heavily armed Kurdish soldiers and foreign fighters working together to defeat ISIS. It has garnered more than 20,000 likes and served as a rudimentary ‘cheerleading’ facility, where Kurdish sympathisers would post their messages of support (Johnson, 2015). Besides the publicity gained from this Facebook page, the YPG has also created a dedicated website (<http://thelionsofrojava.com/>) and made appearances on various social media sites, such as Reddit, to elicit support for its cause. It is important to note that these online platforms provide interested individuals with an opportunity to network with recruiters and like-minded others. These platforms become a cause for concern when individuals—who frequented them—become influenced by the propaganda materials disseminated by the Kurdish militia groups, and in some cases, start to espouse anti-Muslims sentiments in response to the actions of ISIS (Tuck et al., 2016). This is similar to how other terrorist online communities have operated in their attempts to recruit and radicalise new supporters (Bowman-Grieve, 2009; Torok, 2013). As a result, some of the Kurdish sympathisers have been mobilised and travelled to the Middle East to become Kurdish foreign fighters.

1.2 Objectives of Study

This chapter uses the same research methodology as chapter 5 and compares the social media posts of 17 ISIS fighters with that of 23 Kurdish

fighters. This study will not only attempt to distinguish between these two groups of foreign fighters using the identified factors and indicators (from chapter 3) but also identify the predictor(s) for someone to become an ISIS foreign fighter. This would build on the findings from chapter 5 and enhance the generalisability of the factors and indicators.

2. Method

The data for the 17 ISIS fighters from chapter 5 was used for comparison with the Kurdish fighters. This section will focus on the identification of Kurdish fighters to be included in the analyses. The inclusion criteria and steps taken for the data collection and coding are identical to the previous chapter.

2.1 Identification of Kurdish Foreign Fighters

Data collection was undertaken from January to February 2017. I used my social media accounts to find potential Kurdish foreign fighters. The search was informed by insights gathered from sources such as the Centre of Excellence for National Security (CENS)'s Kurdish foreign fighter database (see Jayakumar, 2019), reports released by research think tanks, news stories, scholarly literature on Kurdish foreign fighters, and recommendation algorithms by social media sites. An initial sample of 104 accounts was identified using purposive sampling. Eighty-one accounts (77.9%) were excluded from further analysis due to the following reasons: the lack of information to verify the travel dates, and the lack of posts in the social media accounts. Only 23 accounts with 6,753 postings were used for analysis.

There were 17 (73.9%) U.S. accounts, 3 (13%) Canadian accounts, 2 (8.6%) U.K. accounts, and 1 (4.3%) Australian account. The sample was

predominantly from the United States, as many studies have shown that many of the Kurdish fighters came from this country (Orton, 2017; Patin, 2015). The names of the account holders were not disclosed, and all the online handles of the accounts were de-identified and given specific identifiers—e.g., C1 for accounts belonging to Kurdish foreign fighter 1.

2.2 Consolidation of Sample Containing both ISIS and Kurdish Fighters

Eventually, a sample of 40 foreign fighters with 23,958 posts was derived. Table 17 details the information about these accounts. There are 17 ISIS fighters ($M_{post} = 1,012.06$, $SD_{post} = 1,061.27$) and 23 Kurdish fighters ($M_{post} = 293.61$, $SD_{post} = 270.75$). Open-source information was captured from the following social media platforms—Twitter (16,633; 69.4%), Facebook (7,256; 30.2%), Ask.fm (67; 0.2%), and Instagram (2, 0.0%). No data was collected from privatised communications and/or accounts.

Table 17

Information about the Social Media Accounts of 40 Foreign Fighters (2012 to 2015)

Group	Identifier	Total number of postings across all platforms	Coded number of postings ^a (% ^b)	Time period of posting	Country
ISIS foreign fighter	A1	2294	57 (2.4)	2013	UK
	A2	2330	39 (1.6)	2012 – 2014	UK
	A3	178	41 (23.0)	2013 – 2014	UK
	A4	3085	76 (2.4)	2012 – 2013	UK
	A5	1399	97 (6.9)	2012 – 2014	UK
	A6	731	62 (8.4)	2014	UK
	A7	361	37 (10.2)	2013 – 2014	UK
	A8	377	24 (6.2)	2014	UK
	A9	166	28 (16.8)	2013 – 2014	UK
	A10	2919	34 (1.1)	2013	UK
	A11	1168	4 (3.6)	2014	UK
	A12	35	4 (11.4)	2013	US
	A13	182	16 (8.7)	2013 – 2014	Malaysia
	A14	126	7 (5.5)	2012 – 2014	Malaysia
	A15	58	12 (20.6)	2012 – 2014	Indonesia
	A16	1550	27 (1.7)	2012 – 2014	Indonesia
	A17	246	12 (4.8)	2012 – 2014	Indonesia
Kurdish foreign fighter	C1	52	11 (21.1)	2013 – 2015	Canada
	C2	742	15 (2.0)	2012 – 2015	US
	C3	69	3 (4.3)	2012 – 2015	US
	C4	199	9 (4.5)	2012 – 2015	US
	C5	423	30 (7.0)	2012 – 2015	US
	C6	157	7 (4.4)	2012 – 2015	Australia

Table 17 (continued)

Group	Identifier	Total number of postings across all platforms	Coded number of postings ^a (% ^b)	Time period of posting	Country
Kurdish foreign fighter	C7	506	15 (2.9)	2012 – 2015	US
	C8	527	19 (3.6)	2012 – 2015	US
	C9	73	2 (2.7)	2012 – 2015	UK
	C10	1099	27 (2.4)	2012 – 2015	Canada
	C11	109	3 (2.7)	2012 – 2015	US
	C12	107	2 (1.8)	2012 – 2015	US
	C13	107	2 (1.8)	2012 – 2015	US
	C14	240	8 (3.3)	2012 – 2015	US
	C15	108	15 (13.8)	2015	US
	C16	10	4 (40)	2015	US
	C17	253	10 (3.9)	2012 – 2015	US
	C18	46	4 (8.6)	2012 – 2015	Canada
	C19	181	32 (17.6)	2014 – 2015	US
	C20	408	7 (1.7)	2012 – 2015	US
	C21	217	3 (1.3)	2012 – 2015	UK
	C22	602	23 (3.8)	2014 – 2015	US
	C23	518	17 (3.2)	2012 – 2015	US

Note. ^a Analysis will be conducted on the posts taken from the time they set up their accounts or from 2012, until the date they made the travel. ^b This is the percentage of post used for analysis in relation to the total number of posts across all social media accounts.

2.3 Data Coding

Three independent coders, who were blind to the hypotheses of the study, coded 6,753 posts that were obtained from the 23 Kurdish fighters' social media accounts. The same three coders had already completed the coding of the social media posts of the ISIS fighters in chapter 5.

Table 18

Intra-class Correlation (ICC) Agreement Between the Three Coders

Factors	ICC ^a	95% CI
<u>Frequency Rating^b</u>		
Perceived grievances (PG)	.86	.30, .98
Knowledge and skill to commit terrorist offences (K)	.87	-.31, .99
Redemption and the pursuit for significance (S)	.82	-.16, .98
Readiness to use violence (R)	.88	.58, .97
Commitment to terrorist groups (C)	.87	.14, .99
Intolerance towards multi-religious, multi-racial living (I)	.88	.25, .99
Online relationship building with like-minded individuals (OR)	.87	-.31, .99
Involvement in the terrorist online community (OC)	.87	.14, .99
Individual-centric protective elements (IP)	.81	-.23, .98
Online environment-centric protective elements (OP)	.93	-1.40, 1.00
<u>Severity Rating</u>		
Perceived grievances (PG)	.72	.49, .86
Redemption and the pursuit for significance (S)	.87	.74, .93
Readiness to use violence (R)	.85	.72, .92
Intolerance towards multi-religious, multi-racial living (I)	.80	.62, .90

Note. ^a ICC two-way random effects model, mean of 3 coders, consistency measure.

^b The factors of "personal uncertainty" (P) and "negative social support" (N) were not included due to insufficient ratings.

A two-way random effects model, mean of 3 coders, consistency measure of ICC was employed (see Shrout & Fleiss, 1979). Table 18 displays the ICC agreement between the three coders. For the frequency ratings, the ICC values range from .81 to .93, suggesting that the coders exhibited good to excellent inter-rater reliability. For the severity ratings, there is a good degree of interrater reliability across the four factors, with ICC values ranging from .72 to .87. Disagreements between coders were resolved by discussion.

3. Results

3.1 Differences Between ISIS and Kurdish Foreign Fighters

Out of the 23,958 posts, 884 (3.6%) were coded. Similar to chapter 5, the differences between ISIS and Kurdish foreign fighters were examined using bivariate and multivariate analyses.

3.1.1 Prevalence of Factors and Indicator Across the Two Samples

Most of the ISIS fighters were positive on 88% of the 42 indicators, whereas most of the Kurdish fighters were positive on 76% of them. 16 out of the 42 indicators (38%) were found to be statistically significant in terms of the differences between the two groups—see Table 19. However, upon taking into account the difference of proportions ($>.40$), the number of significant indicators dropped to ten.

The account holders who became ISIS fighters have a significantly higher likelihood of displaying the following nine indicators. First, they would publicise the injustices targeted at the Muslim communities (indicator PG1), $p = .00$, FET. The proportion of PG1 observed amongst the ISIS fighters (.94) is 59.3% points higher than those found in the Kurdish sample (.34). Second, ISIS fighters would demonstrate a preoccupation with those who were responsible

for causing the injustice (indicator PG2), $p = .00$, FET. The proportion of PG2 observed in the ISIS group (.52) is 44.2% points higher than those found in the Kurdish sample (.08). Third, fighters from ISIS would express frustration about the injustice (indicator PG3), $p = .00$, FET. The proportion of this indicator found in the ISIS group (.76) is 63.5% points higher than those found amongst the Kurdish sample (.13). Next, they would express a strong sense of hatred towards those responsible for the injustice (indicator PG4), $p = .00$, FET. The proportion of PG4 seen in the fighter group (.58) is 50.1% points higher than the Kurdish sample (.08). Fifth, ISIS fighters would strongly encourage their family and friends to defend Islam by joining ISIS, $p = .00$, FET. The proportion of this indicator, R2, observed in this group (.70) is 61.9% points higher than those found amongst the Kurdish group (.08). Sixth, they would quote personalities known for their radical views (indicator C1), $p = .00$, FET. The proportion of C1 found amongst the ISIS fighters (.52) is 48.6% points higher than the Kurdish sample (.04). Seventh, ISIS fighters would express dissatisfaction with their home countries' culture and governance, $p = .00$, FET. The proportion of this indicator, I3, that is present in the ISIS group (1.00) is 52.2% points higher than the I3 found in the Kurdish sample (.47). Next, they would also highlight how Islam and the Islamic caliphate were superior to other religion and governance systems (indicator I4), $p = .00$, FET. The proportion of I4 found amongst the ISIS fighters (.76) is 76.5% points higher than the Kurdish sample (.00). Finally, ISIS fighters would reach out to terrorists and/or key nodes in the terrorist online communities (indicator OR1), $p = .00$, FET. The proportion of OR1 seen in the ISIS group (.47) is 42.8% points higher than the OR1 found amongst the Kurdish fighters (.04).

This suggests that ISIS fighters are more likely than their Kurdish counterparts to highlight grievances affecting the group, express a higher level of intolerance towards others, and reach out to like-minded individuals. It could well be the case that for this particular group of ISIS fighters, the quest to become a fighter is underlined mainly by the perceived grievance they felt, as exemplified by a large representation of indicators under the factor “perceived grievances”—PG1, PG2, PG3, and PG4. In contrast, this factor and its indicators were not featured prominently within the Kurdish sample.

To make sense of these findings, it is vital to understand how ISIS and Kurdish militia groups conduct their online recruitment campaigns. ISIS places more emphasis in its outreach campaigns, as reflected by the sheer number and range of propaganda materials produced by the group (Berger & Morgan, 2015; Cohen & Kaati, 2018). Furthermore, ISIS makes concerted efforts to proactively reach out to and groom potential supporters via its online platforms (Carter et al., 2014). This makes it easier for ISIS supporters to come into contact with radical content, and make connections and engage in online discussions with like-minded others. On the other hand, there is a conspicuous lack of effort by Kurdish militia groups to mass-produce propaganda materials or actively groom potential supporters (Tuck et al., 2016). Instead of a huge repository of online platforms, these Kurdish groups mostly rely on standalone websites and social media pages for any potential supporters to contact them. Thus, what stands out in particular for the Kurdish fighters is the self-driven nature of their radicalisation process and how it leads them to travel to Syria. This observation is corroborated by Jayakumar (2019). In an analysis of 500 Kurdish foreign fighters, he observed that many of them did not post any

content relating to the conflict and only “in a few cases the decision to make the journey to the conflict zone is preceded by the posting of content relating to the Kurdish cause, key battles or atrocities carried out by ISIS” (p. 14). In other words, Kurdish fighters have a lower likelihood of airing their thoughts about becoming a foreign fighter or their views about the conflict on social media and instead may have communicated directly via private messaging to the Kurdish militias’ social media pages.

Out of the ten significant indicators, one of them is related to the Kurdish fighters. Compared to their ISIS counterparts, Kurdish fighters were more likely to post photos of weapons and explosives on their social media (indicator K2), $p = .01$, FET. The proportion of K2 observed amongst the ISIS fighters (.23) is 41.7% points lower than those found in the Kurdish sample (.65). This supports a general observation that the Kurdish cohort may espouse certain sensational interest in weapons, which research suggest is a risk factor for violence (Meloy et al., 2008). For example, Barlas and Egan (2006) found that adolescents that have an interest in weapons are more likely to display aggressive behaviours. However, more research is required before concluding that this finding could be generalised to all Kurdish fighters. Alternatively, it could be attributed to the fact that many of the Kurdish fighters had previously served in the military (Jayakumar, 2019; Patin, 2015), and by that extension, are comfortable in displaying images of them engaging in weapons training (during their military career) or at a rifle range.

Table 19*Prevalence of Factors and Indicators Across ISIS Fighters and Kurdish Fighters*

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Kurdish fighter (<i>n</i> = 23)	Overall (<i>N</i> = 40)	ISIS fighter (<i>n</i> = 17)			Kurdish fighter (<i>n</i> = 23)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
<u>Perceived grievances (PG)</u>									
PG1: Publicise the injustices targeted at one’s own community, faith, or belief	94.1% ***	34.8%	60%	3.35	2.71	57	.87	1.48	20
PG2: Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice	52.9% ***	8.7%	27.5%	.71	.84	12	.09	.28	2
PG3: Express frustration with the injustice targeted at one’s own community, faith, or belief	76.5% ***	13%	40%	1.88	1.99	32	.13	.34	3
PG4: Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice	58.8% ***	8.7%	30%	1.35	1.65	23	.09	.28	2
PG5: Openly challenge certain group(s) of concern about the injustice	41.2%	39.1%	40%	.82	1.23	14	.57	.94	13
<u>Knowledge and skill to commit terrorist offences (K)</u>									
K1: Demonstrate an interest in learning combat skills	11.8%	21.7%	17.5%	.24	0.66	4	.22	.42	5
K2: Showcase interest in the use of weapons and explosives	23.5%	65.2% **	47.5%	.29	0.58	5	2.26	2.78	52
K3: Have information on explosives-bomb making	0%	0%	0%	.00	.00	0	.00	.00	0
<u>Redemption and the pursuit for significance (S)</u>									
S1: Desire to partake in humanitarian activities in countries associated with terrorism opportunities	29.4%	26.1%	27.5%	.47	.80	8	.39	.78	9
S2: Desire to repent by migrating to countries associated with terrorism opportunities	35.3% ***	0%	15%	.88	1.31	15	.00	.00	0
S3: Express feelings of contempt for own prior practices	58.8% *	21.7%	37.5%	1.29	1.61	22	.43	.94	10

Table 19 (continued)

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Kurdish fighter (<i>n</i> = 23)	Overall (<i>N</i> = 40)	ISIS fighter (<i>n</i> = 17)			Kurdish fighter (<i>n</i> = 23)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
S4: Intention to search for opportunity to do something meaningful	58.8%	43.5%	50%	1.24	1.30	21	1.00	1.78	23
<u>Personal uncertainty (P)</u>									
P1: Desire to explore different ideologies and beliefs—inconsistent identity	29.4%	13%	20%	.53	1.06	9	.17	.49	4
<u>Readiness to use violence (R)</u>									
R1: Voice strong support for the use of violence towards a certain group(s) of concern as a viable solution	58.8% *	21.7%	37.5%	1.06	1.19	18	.26	.54	6
R2: Incite friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief	70.6% ***	8.7%	35%	2.47	2.18	42	.13	.45	3
R3: Express willingness to die for cause, and achieve martyrdom	35.3% *	4.3%	17.5%	1.18	2.12	20	.04	.20	1
R4: Demonstrate a preoccupation with an individual from group(s) of concern as a potential target	35.3%	17.4%	25%	.59	.87	10	.26	.68	6
R5: Display themselves as a protector/hero of their fellow believers of the same faith, religion or belief	11.8%	26.1%	20%	.12	.33	2	.26	.44	6
R6: Perceive an urgency to act and that non-violent alternative are ineffective solutions	35.3% *	4.3%	17.5%	.53	.80	9	.04	.20	1
R7: Indicate their intention to travel and participate in overseas conflict	41.2%	21.7%	30%	.71	1.26	12	.35	.88	8
<u>Commitment to terrorist groups (C)</u>									
C1: Quotations from/ associations with personalities known for their radical views	52.9% ***	4.3%	25%	.71	.77	12	.04	.20	1

Table 19 (continued)

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Kurdish fighter (<i>n</i> = 23)	Overall (<i>N</i> = 40)	ISIS fighter (<i>n</i> = 17)			Kurdish fighter (<i>n</i> = 23)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
C2: Identify with symbols of known terrorist groups on one's online profile	17.6%	21.7%	20%	.18	.39	3	.61	1.75	14
C3: Display their public allegiance to terrorist groups	11.8%	8.7%	10%	.12	.33	2	.13	.45	3
C4: Praise and defend terrorist groups	58.8%	30.4%	42.5%	2.35	4.01	40	.43	.78	10
<u>Intolerance towards multi-religious, multi-racial living (I)</u>									
I1: Force friends, colleagues or family to distance themselves from certain group(s) or community	17.6%	0%	7.5%	.18	.393	3	.00	.00	0
I2: Dehumanise group(s) of concern who hold different viewpoints/ beliefs system	35.3%	8.7%	20%	.59	1.00	10	.09	.28	2
I3: Dissatisfaction with local cultures, practices, values, and governance	100% ***	47.8%	70%	6.18	4.26	105	1.17	1.80	27
I4: Anti-integration messaging—exclusivity of one's own community, faith, or belief	76.5% ***	0%	32.5%	2.18	2.15	37	.00	.00	0
<u>Online relationship building with like-minded individuals (OR)</u>									
OR1: Attempt to reach out to terrorists	47.1% ***	4.3%	22.5%	1.82	2.72	31	.17	.83	4
OR2: Develop and disseminates terrorist content	0%	8.7%	5%	.00	.00	0	.43	1.87	10
OR3: Attempt to set up physical meeting with terrorists	11.8%	0%	5%	.29	.98	5	.00	.00	0
<u>Involvement in the terrorist online community (OC)</u>									
OC1: Possess terrorist documents, music, videos, etc. on computer or mobile devices	41.2% *	8.7%	22.5%	.59	.79	10	.09	.28	2
OC2: Host web-links to other online platforms that contain terrorist context	11.8%	21.7%	17.5%	.35	1.22	6	.57	1.53	13
OC3: Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism	35.3%	8.7%	20%	.65	1.11	11	.09	.28	2
OC4: A sudden increase in the user's activity	0%	0%	0%	.00	.00	0	.00	.00	0

Table 19 (continued)

Indicators	Prevalence (%)			Frequency of occurrence					
	Foreign fighter (<i>n</i> = 17)	Kurdish fighter (<i>n</i> = 23)	Overall (<i>N</i> = 40)	ISIS fighter (<i>n</i> = 17)			Kurdish fighter (<i>n</i> = 23)		
				<i>M</i>	<i>SD</i>	Total	<i>M</i>	<i>SD</i>	Total
<u>Negative social support (N)</u>									
N1: Presence of supportive family members and friends that encourage involvement in the terrorist online communities and/or terrorist offending	5.9%	13%	10%	.06	.24	1	.13	.34	0
<u>Individual-centric protective elements (IP)</u>									
IP1: Presence of supportive family members and friends that discourage terrorist offending	5.9%	0%	2.5%	.06	.24	1	.00	.00	0
IP2: Demonstrate willingness to engage in discussions of ideology and the use of violence	5.9%	0%	2.5%	.06	.24	1	.00	.00	0
IP3: Disillusioned with using violence to solve problems	0%	4.3%	2.5%	.00	.00	0	.04	.20	1
IP4: Demonstrate an appreciation for diversity	5.9%	4.3%	5%	.06	.24	1	.09	.41	2
<u>Online environment-centric protective elements (OP)</u>									
OP1: Inability to obtain access to the terrorist online community	0%	0%	0%	.00	.00	0	.00	.00	0
OP2: Recognise and fear the detection by law enforcement and social media companies	5.9%	0%	2.5%	.12	.48	2	.00	.00	0

Note. Analysis based on Fisher's exact test: * $p = .02$. ** $p = .01$. *** $p = .00$.

3.1.2 Severity Ratings of Factors Across the Two Samples

The coded posts across four factors (see Figure 10)—“perceived grievances” (PG); “redemption and the pursuit for significance” (S); “readiness to use violence” (R); “intolerance towards multi-religious, multi-racial living” (I)—were analysed using the Mann-Whitney U Test. There were two significant findings.

Figure 10
Median Severity Ratings Across Four Factors

Note. The number in the () represents the number of foreign fighters (ISIS or Kurdish).

* This refers to the median score for each subsample.

ISIS fighters ($Mdn = 2.00$) have created posts espousing grievances that were rated more severe, as compared to the Kurdish fighters ($Mdn = 2.00$), $U = 114.00$, $p = .02$, $r = -.36$. While the median values are equal, the difference in the sum of ranks of the two groups is sufficient enough for the comparison to be statistically significant. They ($Mdn = 2.00$) were also creating posts that expressed a higher level of intolerance towards communal living as compared to their Kurdish counterparts ($Mdn = .00$), $U = 52.00$, $p = .00$, $r = -.64$. It is noteworthy that the effect sizes were between the range of medium to large, suggesting that ISIS fighters do express themselves more radically across these

two factors. There was, however, no significant difference found in the other two factors of S and R.

These results provide additional support to the earlier observations that ISIS fighters were more expressive online by highlighting that they were also more severe in the way they expressed their grievances and intolerance for the out-group. The active online communities that are propagating ISIS rhetoric serve as echo chambers to normalise and reinforce the radical worldviews of the ISIS fighters, may have contributed to the higher severity ratings of their posts. Conversely, such sentiments were not observed within the Kurdish sample as they may be less likely to publicly air their views before they travel (Fritz & Young, 2017), and they may also have fewer online platforms available to them—i.e., in comparison to ISIS fighters.

3.1.3 Relationships Between the Indicators Across the Two Samples

Multidimensional scaling (MDS) was used to measure how the indicators are interrelated and visualise how they may manifest differently for the two groups of foreign fighters. In this case, Multidimensional Unfolding (PREFSCAL) in SPSS was employed to produce a three-dimension space that plotted 39 indicators for all the foreign fighters (ISIS and Kurdish fighters, $N = 40$). Three indicators that were not mapped to any posts were excluded from the analyses: K3, OC4, and OP1. To determine the model's goodness of fit, Kruskal's stress was used (Kruskal, 1964). The current model has a reported good fit as the stress value is .03.

Figure 11 locates the foreign fighters on the MDS plot. The Kurdish fighters ($n = 23$) are represented by red triangles, whereas green pentagons

represent the ISIS fighters ($n = 17$). There appears to be a clear demarcation between these two groups as they were neatly separated on the plot.

Figure 11

Multidimensional Scaling Plot of Foreign Fighters

Note. Kurdish fighters (red triangle, $n = 23$) and ISIS fighters (green pentagon, $n = 17$)

3.1.3.1 Five Clusters of Indicators Found. MDS was carried out for all the 39 indicators. Five clusters of indicators were identified that broadly accord with the person-centric (“frustration”, “sensational interest”, “intention to act”) and psychosocial (“strong identification with group”, “willingness to use violence”) dimensions—introduced in chapter 2. Figure 12 locates these five clusters of indicators, which are represented as different coloured circles.

Of particular interest here is the close proximity of the “intention to act” cluster with the “willingness to use violence” cluster, suggesting a high

likelihood of the indicators within them to co-occur. Although the specific relationship at work eludes us, these indicators seem to represent an essential psychological milestone that individuals need to surpass in order to conduct physical acts of violence. As for the other three clusters, the likelihood of their indicators co-occurring is relatively low due to the low degree of association between them—i.e., they are remotely located from one another. In other words, the indicators within these three clusters are likely to be observed as stand-alone occurrence.

Figure 12
Multidimensional Scaling Plot of the 39 Indicators

Note. The indicators are represented by the circles and are differentiated by the different colour coding. Cluster on “strong identification with group” constitutes the following: S1, C4, and OC2. Cluster on “frustration” constitutes the following: PG1, PG3, I3, I4, and R2. Cluster on “sensational interest” constitutes the following: K2. Cluster on “intention to act” constitutes the following: PG5, K1, S4, P1, R4, R5, C2, C3, OR2, N1, IP1, IP2, IP3, IP4, and OP2. Cluster on “willingness to use violence” constitutes the following: PG2, PG4, S2, S3, R1, R3, R6, R7, C1, I1, I2, OR1, OR3, OC1, and OC3.

3.1.3.2 Overlaying the Foreign Fighters with the 39 Indicators. The

MDS analysis has highlighted two behavioural typologies of foreign fighters (see Figure 13).

The first behavioural typology pertains to that of the Kurdish fighters. While they were primarily situated within the cluster known as “sensational interest”, some Kurdish fighters also exhibited some degree of association with the “frustration” cluster of indicators. In a nutshell, this group of fighters were generally interested in weapons and explosives and were feeling dissatisfied with their local government and/or cultural practices. This is not surprising given that Fritz and Young (2017) and Tuck et al. (2016) found that some Kurdish fighters are former army veterans, who are frustrated with the inaction of Western governments in responding to the atrocities perpetrated by ISIS. For some, they missed the thrills of participating in combat and have difficulties transiting from military service to a civilian lifestyle (Orton, 2017). For others, they were motivated to continue what they have done previously during their combat tours to fight terrorism in the Middle East (Jayakumar, 2019).

The MDS results further suggest the presence of a second behavioural typology of ISIS fighters. This group of individuals showed a strong co-occurrence with indicators from the “frustration” cluster. The ISIS fighters were generally frustrated by the grievances they perceived, especially with their local practices. Of particular interest is the sizable congregation of fighters around one particular indicator, I3 (“dissatisfaction with local cultures, practices, values, and governance”), which has a recorded frequency of 105. This observation lends support to the arguments put forth by van Dyke and Soule (2002) on how perceived grievances can be used to mobilise individuals to participate in militia movements, even when their grievances are not fully aligned to the movements’ agenda.

Figure 13

Multidimensional Scaling Plot of Foreign Fighters and the 39 Indicators

Note. Kurdish fighters (red triangle, $n = 23$) and ISIS fighters (green pentagon, $n = 17$). The indicators are represented by the circles and are differentiated by the different colour coding. The black line is used to demarcate the two clusters of foreign fighters.

There was no discernible difference in the distance between the two cohorts of foreign fighters and the indicators in the “intention to act”, “strong identification with group”, and “willingness to use violence” clusters. This could be attributed to the low frequency of these indicators and/or the unconfirmed negative correlation of these indicators with that of an individual becoming an ISIS fighter or Kurdish fighter. In other words, the social media posts of ISIS and Kurdish fighters have a lower likelihood of being mapped against these indicators.

3.2 Predictor(s) for Becoming an ISIS Foreign Fighter

Thirty-nine indicators across 23,958 social media posts were input into the logistics regression model to predict who would become an ISIS foreign

fighter (1 = ISIS fighter, 0 = Kurdish fighter). Three indicators (K3, OC4, OP1) were removed due to their low correlation values (see Kinnear & Gray, 2006).

The regression model was significant, $X^2(39, N = 23958) = 303.39, p = .00$, and it correctly classified 72.2% of posts that belong to the ISIS fighters. The R^2 value was about .01, which means that the model was only able to explain 1.8% of the variation in predicting an ISIS fighter. This low R^2 value is expected as the topic of investigation is a low base-rate event; in this case, out of the 23,958 postings, only 884 (3.6%) were coded. Furthermore, it can be attributed to the presence of other offline predictors on the radicalisation process (Gill et al., 2017), which were not accounted for in this study. But, despite that, 13 indicators were found to be significant predictors, as shown in Table 20. Thus, useful insights can still be drawn from the findings.

There were eight negative and significant indicators. These indicators do not predict the likelihood of an individual becoming an ISIS fighter, but instead, reduce the odds of them doing so. In other words, individuals who have posts that are mapped to these eight indicators would be less likely to become an ISIS fighter, and their odds ratios range from .03 to .42 times of not becoming an ISIS fighter.

When considering the positive indicators for becoming an ISIS fighter, five significant indicators were found. ISIS fighters were significantly more likely to create posts—before they travelled—that expressed their frustration about injustice (4.16 [95% CI: 1.27, 13.6] times more likely to be an ISIS fighter), voice their hatred towards those responsible for the injustice (4.49 [95% CI: 1.05, 19.0] times more likely), incite their family and friends to join ISIS (5.47 [95% CI: 1.69, 17.6] times more likely), indicate their willingness to

die for ISIS (7.81 [95% CI: 1.04, 58.2] times more likely), and attempt to establish contacts with key nodes within the ISIS online community (3.12 [95% CI: 1.10, 8.84] times more likely).

Table 20

Logistic Regression Model for Predicting Who Becomes an ISIS Foreign Fighter

Indicator	B (SE)	95% CI for odds ratio		
		Lower	Exp (B)	Upper
PG3: Express frustration with the injustice targeted at one's own community, faith, or belief	1.42 (.60) *	1.27	4.16	13.6
PG4: Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice	1.50 (.73) *	1.05	4.49	19.0
PG5: Openly challenge certain group(s) of concern about the injustice	-0.86 (.38) *	.19	0.42	.89
K2: Showcase interest in the use of weapons and explosives	-3.28 (.46) **	.01	0.03	.09
S1: Desire to partake in humanitarian activities in countries associated with terrorism opportunities	-1.05 (.48) *	.13	0.34	.90
S4: Intention to search for opportunity to do something meaningful	-1.03 (.30) **	.19	0.35	.64
R2: Incite friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief	1.70 (.59) **	1.69	5.47	17.6
R3: Express willingness to die for cause, and achieve martyrdom	2.05 (1.02) *	1.04	7.81	58.2
R5: Display themselves as a protector/hero of their fellow believers of the same faith, religion or belief	-2.03 (.81) *	.02	0.13	.64
C2: Identify with symbols of known terrorist groups on one's online profile	-2.48 (.63) **	.02	0.08	.29
OR1: Attempt to reach out to terrorists	1.14 (.53) *	1.10	3.12	8.84
OR2: Develop and disseminates terrorist content	-1.63 (.54) **	.06	0.19	.57
OC2: Host web-links to other online platforms that contain terrorist context	-3.50 (1.03) *	.00	0.03	.23
Constant	.94 (.01) **		2.55	

Note. B = regression coefficient; Exp (B) = odds ratio.

Postings are coded as 1 for 'ISIS fighter' and 0 for 'Kurdish fighter'.

$R^2 = .01$; $-2 \text{ Log likelihood} = 28192.69$; $N = 23958$

* $p < .05$. ** $p < .00$.

These results underscore the essential role that terrorist online communities plays in cultivating partisanship and providing the necessary sounding boards for potential ISIS fighters to voice their radical views (e.g., frustration about injustice, intention to die as a martyr) and be reinforced by others, and to connect their budding intentions to contribute to the ISIS' cause with a plan of action (i.e., travel to Syria).

4. Discussion

This chapter replicated the research design from chapter 5 to investigate the external generalisability of the factors and indicators in distinguishing two groups of foreign fighters: ISIS fighters and Kurdish fighters. The contributions of the current chapter to the thesis are twofold. First, it extends research on terrorists' online activities by studying the manifestation of online radicalisation indicators using social media posts of ISIS and Kurdish fighters. It deviates from the usual focus on ISIS social media activity (see Conway et al., 2019), and highlights the largely overlooked phenomenon of Kurdish foreign fighters. While both cohorts of fighters were recruited via social media, there are not many studies that utilised primary data to study the Kurdish foreign fighters (Fritz & Young, 2017), let alone to compare them against the ISIS fighters using their online posts before either of the groups made the travel.

Second, the results suggest that there are differences between the two groups of foreign fighters. Findings from the Fisher's exact test showed that ISIS fighters tend to lend their support for ISIS by highlighting grievances affecting the group and the Muslim communities, expressing a higher level of intolerance towards the out-group, and reaching out to more like-minded others. Kurdish fighters, on the other hand, tend to showcase their interest in weapons and combat. The analysis of the severity of the postings revealed that ISIS fighters tend to create posts that are rated more severe for the factors of "perceived grievances" and "intolerance towards multi-religious, multi-racial living". The results of the MDS indicated that the ISIS fighters tend to express their frustration online, as compared to Kurdish fighters, who are more inclined to showcase their interest in weapons and combat. Finally, the logistic

regression model found five indicators that increase the likelihood of a post creator to be an ISIS fighter: “express willingness to die for cause, and achieve martyrdom” by 7.8 times; “express frustration with the injustice targeted at one’s own community, faith, or belief” by 4.1 times; “express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice” by 4.5 times; “incites friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief” by 5.4 times; and “attempts to reach out to terrorists” by 3.1 times. These results add another level of postdictive validity for the factors and indicators.

Results of this chapter have replicated some of the findings found in chapter 5 for the ISIS fighters using a different comparison group, i.e., Kurdish fighters. The indicator OR1 was found to be a significant predictor of someone becoming an ISIS fighter in both studies. The only difference, in this chapter, is the addition of four more predictors. From an online risk assessment perspective, these indicators have the potential to be used as an investigative template for screening suspicious social media accounts. This approach not only enables us to use the statistically derived predictors (from logistics regression) for a granular level of examination, but it also allows us to triangulate any identified indicators with other indicators that are highly associated with them (based on the MDS findings). This provides a more holistic approach to detect online radicalisation in social media posts. It is essential to recognise that there are some indicators (K3, OC4, OP1) that were not coded for across both samples and their utility need to be explored in future research. Nonetheless, these findings have buttressed our understanding about the mechanisms underlying online radicalisation as we focus on one of its

extreme manifestations whereby an individual transits from the online to the offline realm and becomes a foreign fighter.

4.1 Limitations

In addition to the limitations (e.g., the use of purposive sampling) already highlighted in chapter 5, there is one new limitation to discuss. For the vast majority of the Kurdish fighters, information about which militia groups that they had joined is hard to ascertain. While many have been recruited via ‘The Lions of Rojava’ Facebook page, the group that they eventually joined may not be the YPG. In addition, it is a common occurrence for Kurdish fighters to switch allegiance when they are in Syria and Iraq (Orton, 2017). However, in this chapter, all the Kurdish fighters were analysed as a single entity—instead of segregating them according to the groups they joined—because the main objective was to use them as a comparison group for the ISIS fighters. Hence, I felt that this approach was a reasonable step to take.

In conclusion, this chapter’s attempt to further test the factors and indicators—by mapping them to two groups of foreign fighters—does present itself as a worthwhile endeavour to further our insights on detecting online radicalisation. While it is important to derive empirically derived insights about how terrorists and their supporters use the internet, it is equally important to obtain a ‘baseline’ perception of how the mainstream population view the above-mentioned factors and indicators. As the social media posts by terrorists and their supporters may be chanced upon by members of the community, it is, therefore, useful to understand their level of understanding about the indicators that can be used to detect online radicalisation.

**CHAPTER SEVEN: UNDERSTANDING COMMUNITY'S
PERCEPTIONS TOWARDS RADICALISATION VIA THE INTERNET
AND TERRORISM⁸**

Given the growing threat of online radicalisation, it is unrealistic that the onus to detect the warning signs resides solely under the purview of law enforcement. Due to the massive amount of available data that intelligence agencies had to sieve through (Skillicorn, 2008) and the recognition that members of the community have reported cases of self-radicalised individuals to the authorities (Neo et al., 2019), observers have recommended the importance for law enforcement to work closely with the community that they are trying to protect (Shaftoe et al., 2007) in order to mitigate the threat of online radicalisation. Specifically, community members are key partners as they have the opportunity to observe expressions and behaviours associated with online radicalisation on their social media accounts. It is thus relevant to the current research learn more about what the members of the general online community know and think about the warning signs of online radicalisation.

In chapters 5 and 6, indicators that could predict an individual's likelihood of becoming an ISIS foreign fighter were identified. To complement the earlier findings, this chapter is intended to contribute knowledge about community perceptions towards these indicators, and hereby to the discussion of how such insights can be utilised by law enforcement to formulate relevant counter terrorism strategies. To the best of my knowledge, there is a lack of

⁸ This study was awarded the Ministry of Home Affairs (MHA)'s research grant titled 'Home Team Behavioural Sciences Centre Student Research Award' in 2019, and was second runner-up for the Singapore Psychological Society (SPS)'s Student Research Award 2020.

research that examines how the community perceives indicators of radicalisation, especially within the context of the cyber realm.

1. The Important Role of the Community in Countering Radicalisation

The media's portrayal of attacks and the perpetrators behind them have shaped how people react to and formulate opinions about radicalisation and terrorism. Previous research has shown how the lack of or incorrect knowledge about terrorism has led the community to develop negative attitudes towards specific segments of the community (Abdul Rahman, 2019). For example, on July 22, 2011, an attack occurred in Norway where 77 people were killed. Even before the perpetrator was arrested, the media was quick to assume that the attack was motivated by Al-Qaeda. Many mainstream media were drawing this link without any conclusive evidence—e.g., the newspaper “The Sun” carried the headline “Al-Qaeda Massacre: Norway’s 9/11”. Eventually, investigations revealed that the perpetrator was not an Al-Qaeda supporter and instead was a right-wing terrorist, Anders Behring Breivik (Sehgal, 2011). In itself, such media framing risks the likelihood of people associating certain religion with terrorism (von Sikorski et al., 2017) and influences how they would identify terrorist threats.

In the context of jihad attacks, such perceptions may increase the occurrence of Islamophobia (Abdelkader, 2016) and reinforce unwanted stereotypes of Muslims. This can lead to dangerous outcomes where individuals are harmed or traumatised due to their affiliation to certain groups. As Cameron et al. (2013) write,

Beards and rucksacks (as seen in video images of the bombers) became symbols of suspicions; everyday actions, such as taking a seat on the train or going out, could

activate potential terrorism stories, reinforced by internalised voices of fearful parents or relations. (p. 9)

Similarly, such stereotypical and biased mindset may manifest in the cyber domain in the form of verbal abuse and/or unnecessary reporting of accounts—belonging to certain groups of individuals—to the authorities and social media companies. This, therefore, prompts a critical need to rethink about how one's experiences and knowledge on online radicalisation would impact our opinions about what kind of online content is deemed radical and who are considered dangerous.

It may be pertinent to appraise the level of knowledge and potential misunderstanding that the community may have regarding how radicalisation occurs and its associated markers (Hussain, 2018). Awan and Guru (2017) remark that many community members do not have a good grasp of the radicalisation process, let alone its warning signs. They may, in some instances, interpret a practising Muslim as a potential terrorist. This is notable as community members are uniquely positioned to detect potential warning signs amongst their family and friends (see Neo et al., 2019). Thus, the lack of knowledge about radicalisation indicators may either result in the missed opportunities for community members to flag them and for authorities to assess and intervene (if necessary), or in the worst case, lead to the unnecessary activation of law enforcement resources to investigate bias reporting.

1.1 Objectives of Study

This chapter has two objectives. First, it seeks to gain an understanding about the community's perceptions towards the 42 indicators—from chapter 3—by asking participants to rate the relevance of the indicators in the detection of radicalisation in social media posts. The findings will then be compared to

the results from chapters 5 and 6 to gauge the participants' knowledge level about the relevant indicators. Second, participants' perceptions on the threat of online radicalisation and terrorism will be measured to obtain a 'situational understanding' of their knowledge, and identify potential areas of concerns. To ensure the generalisability of the findings and examine any potential cultural influence on the perceptions, the survey was conducted on samples from Singapore (NTU psychology undergraduates) and the United States (MTurk workers).

2. Methods

2.1 Participants

This study⁹ was advertised as an electronic survey that aimed to understand the perceptions that the community may have towards online radicalisation and terrorism. The participants ($N = 320$) consisted of community members from the Nanyang Technological University (NTU; $n = 160$) and Amazon Mechanical Turk (MTurk; $n = 160$). The NTU sample was recruited via the SONA system from the pool of psychology undergraduate students, who received one course credit for their participation. The MTurk sample was recruited via the Amazon MTurk website in return for a payment of US\$2. MTurk workers were chosen for this study as research has found them to be a good comparison group for undergraduate sample (Buhrmester et al., 2016). The gender distribution within the NTU sample was 102 females (63.7%) and 58 males (36.3%), whereas, in the MTurk sample, there was 49 females (30.6%) and 111 males (69.4%). In terms of their age range, NTU participants

⁹ This study was approved by the NTU's Institutional Review Board (IRB), and the data was collected between August and October 2019. The IRB reference number is IRB- 2019-02-035.

were largely in the '18-22 age' group ($n = 129$; 80.6%) and '23-27 age' group ($n = 31$; 19.4%). For the MTurk participants, the corresponding figures were 26 in the '23-27 age' group (16.3%), 32 in the '28-32 age' group (20%), 37 in the '33-37 age' group (23.1%), 20 in the '38-42 age' group (12.5%), 19 in the '43-47 age' group (11.8%), and finally 26 in the ' ≥ 48 age' group (16.3%).

2.2 Measures

A 74-item survey comprising three sections was administered to the participants. In addition to the first section on demographic-related questions (5 items), the participants were asked for their opinions about online radicalisation indicators in the second section (42 items), and about their general awareness regarding terrorism and online radicalisation in the third section (27 items). For the second section, participants were provided with 42 indicators—from chapter 3—and were instructed to rate their relevance for detecting radicalisation in social media posts, on a 5-point Likert scale (1 = “strongly disagree”, 5 = “strongly agree”).

For the third section, participants' perceptions in five topics related to online radicalisation and terrorism were elicited. These topics were adapted from Samuel (2018), and contained the following: Five statements that examined the sources of information where participants derived their knowledge on terrorism (e.g., “where do you obtain information on terrorism?”); three statements that explored their views on the definition of terrorism (e.g., “what is terrorism?”); two statements about the role that the internet plays in facilitating radicalisation and terrorism (e.g., “terrorism needs the internet to grow”); eight statements regarding their views on counter terrorism measures (e.g., “the government is capable of handling the threat of

terrorism”); and nine statements about their opinions on how an individual can become radicalised (e.g., “a terrorist usually starts out by having violent radical ideas”). These statements were measured on a 5-point Likert scale (1 = “strongly disagree”, 5 = “strongly agree”), forced-choice options, or open-ended option, wherever appropriate. For the open-ended responses, they were thematically coded by two independent coders to identify the common themes. The entire survey is presented in Appendix D.

2.3 Procedures

Once the participants had given their consent for participation, they were given a perception survey via Qualtrics to complete. They were informed that they can withdraw from the study at any point in time and that their participation is voluntary in nature. Participants provided their opinions on the 42 indicators before completing the section that measured their views on online radicalisation and terrorism. They were then asked to input their demographic information. The entire survey took approximately 15 minutes to complete, and a complete debriefing was provided to the participants upon completion of the survey.

3. Results and Discussion

The results section is presented in three parts. Part 1 presents the descriptive statistics for both the NTU and MTurk samples about their ratings of the indicators. Part 2 showcases the outcome of a factor analysis conducted on the ratings of the indicators. Part 3 then presents the findings on their perceptions of online radicalisation and terrorism.

3.1 Group Differences Between NTU and MTurk Samples

To identify the group differences between the NTU and MTurk samples, the mean ratings across the 42 indicators were used for analysis.

3.1.1 Top Five Indicators Across Each Sample

This part focuses on the top 10% (i.e., top five indicators) of the 42 indicators. Results revealed that the top five indicators rated by the NTU sample to be relevant for detecting online radicalisation were: OR3 (“attempt to set up physical meeting with terrorists” [$M = 4.57, SD = .97$]), OR2 (“develop and disseminates terrorist content” [$M = 4.54, SD = .91$]), OR1 (“attempt to reach out to terrorist” [$M = 4.53, SD = .98$]), C4 (“praise and defend terrorist groups” [$M = 4.44, SD = 1.00$]), and C3 (“display their public allegiance to terrorist groups” [$M = 4.50, SD = .93$]).

The corresponding top five indicators for the MTurk sample were: PG4 (“express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice” [$M = 4.43, SD = .96$]), OR3 (“attempt to set up physical meeting with terrorists” [$M = 4.30, SD = 1.09$]), R2 (“incite friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief” [$M = 4.27, SD = 1.01$]), R3 (“express willingness to die for cause, and achieve martyrdom” [$M = 4.25, SD = 1.03$]), and C3 (“display their public allegiance to terrorist groups” [$M = 4.25, SD = 1.10$]). In comparison to the common finding from chapters 5 and 6 that OR1 is a significant predictor for someone to become an ISIS foreign fighter, it seems that the NTU sample had flagged the same indicator as a key cause of concern within their top five ratings. For the MTurk sample, it was not deemed as equally important; this indicator was featured only within the top ten ratings.

3.1.2 Significant Differences Between the Samples

Seventeen indicators were found to be significantly different between the two groups—see Table 21. Out of these indicators, the MTurk sample scored significantly lower on ten of them. However, one should not over-interpret the findings as there were differences in terms of age and gender across the two samples. Despite this, it is noteworthy that there were two indicators (K1, IP3) where a large effect size was observed. MTurk participants ($M = 3.46$, $SE = .09$) perceived interest in learning combat skills to be more of a concern as compared to their NTU counterparts ($M = 2.60$, $SE = .09$). This may be attributed to the easier access to weapons and combat training that an individual residing in the United States has as compared to the Singapore's participants where firearms are prohibited, and military training lies within the purview of the authorities.

Table 21
Differences Between NTU and MTurk Participants in their Ratings of the Indicators

Indicator	MTurk		NTU		<i>t</i>	<i>r</i>
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>		
K1: Demonstrate an interest in learning combat skills	3.46	1.24	2.60	1.16	6.44**	.71
K2: Showcase interest in the use of weapons and explosives	3.91	1.19	3.50	1.23	3.08*	.33
S4: Intention to search for opportunity to do something meaningful	2.71	1.35	2.40	1.12	2.24*	.24
P1: Desire to explore different ideologies and beliefs— inconsistent identity	2.91	1.25	2.53	1.06	2.96*	.32
C1: Quotations from/ associations with personalities known for their radical views	3.71	1.08	3.96	1.02	-2.12*	.32
C3: Display their public allegiance to terrorist groups	4.25	1.10	4.50	0.93	-2.19*	.24
C4: Praise and defend terrorist groups	4.08	1.23	4.44	1.00	-2.87**	.32
OR1: Attempt to reach out to terrorists	4.21	1.25	4.53	0.98	-2.58*	.28
OR2: Develop and disseminates terrorist content	4.20	1.11	4.54	0.91	-2.96**	.33
OR3: Attempt to set up physical meeting with terrorists	4.30	1.09	4.57	0.97	-2.36*	.26
OC1: Possess terrorist documents, music, videos, etc. on computer or mobile devices	4.01	1.15	4.32	1.01	-2.57*	.28

Table 21 (continued)

Indicator	MTurk		NTU		<i>t</i>	<i>r</i>
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>		
OC2: Host web-links to other online platforms that contain terrorist context	3.97	1.13	4.38	0.97	-3.44**	.38
OC3: Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism	4.06	1.08	4.31	0.99	-2.09*	.24
OC4: A sudden increase in the user's activity	3.03	1.20	2.68	1.03	2.83**	.31
IP3: Disillusioned with using violence to solve problems	3.01	1.38	3.86	1.08	-6.14**	.68
IP4: Demonstrate an appreciation for diversity	2.48	1.43	2.00	1.08	3.38**	.37
OP2: Recognise and fear the detection by law enforcement and social media companies	3.45	1.12	3.18	1.08	2.17*	.24

Note. * $p < .05$. ** $p < .00$.

The full list of the mean and standard deviation for the 42 indicators can be found in Appendix E.

Participants from MTurk ($M = 3.01$, $SE = .10$) perceived disillusionment with the use of violence to be less of a concern as compared to the NTU participants ($M = 3.86$, $SE = .08$). This is a surprising result considering that the literature (Bjørge & Horgan, 2009; Pressman & Flockton, 2012) found that disillusionment with the use of violence to be a protective factor against one's involvement in terrorism. In the same vein, I expected the mean score to be within the category of “disagree” or “neutral”. While the MTurk participants' mean response was rated as neutral, those of their NTU counterparts were more inclined towards “agree”. This finding could be interpreted as that the NTU sample either did not understand the wording of this indicator or that they were referring to the ‘inverse’ usage of this indicator—i.e., seen as a protective element that if present, would reduce the likelihood of an individual becoming radicalised. However, a conclusive explanation cannot yet be derived due to the lack of information, and future research can explore this finding.

3.2 Factor Analysis of the Ratings of the Indicators

To explore how the participants have rated the indicators, a factor analysis was conducted. The principal components analysis with oblique (oblimin) rotation in SPSS was run separately for both the NTU ($n = 160$) and MTurk ($n = 160$) samples. The oblique rotation was chosen (see Field, 2005) because the indicators were theoretically related. Both the Bartlett's test of sphericity and the Kaiser-Meyer-Olkin (KMO) test confirmed that the two samples were adequate for factor analyses: for NTU, $KMO = .90$, $X^2(861) = 5177.89$, $p = .00$; for MTurk, $KMO = .87$, $X^2(861) = 4407.26$, $p = .00$. Factor loadings of .50 and above were considered for further analysis.

Based on a parallel analysis (O'Connor, 2000), a four-factor structure was identified for the NTU sample, accounting for 58% of the total variance. In contrast, the MTurk sample yielded a three-factor structure, which accounted for 51.5% of the total variance. Table 22 presents the result of the factor analyses, as well as the eigenvalues and percentage of accounted variance. The results showed that there were differences in how the NTU participants detect radicalisation in social media posts as compared to their MTurk counterparts.

Table 22*Factor Analysis of the Ratings of the 42 Indicators*

Indicator	NTU				MTurk		
	1	2	3	4	1	2	3
OR2: Develop and disseminates terrorist content	.93				.58		
C3: Display their public allegiance to terrorist groups	.93				.73		
OR1: Attempt to reach out to terrorists	.92				.59		
OC2: Host web-links to other online platforms that contain terrorist context	.86				.68		
OC1: Possess terrorist documents, music, videos, etc. on computer or mobile devices	.85				.67		
C2: Identify with symbols of known terrorist groups on one's online profile	.84				.76		
C4: Praise and defend terrorist groups	.83				.73		
OR3: Attempt to set up physical meeting with terrorists	.83						
OC3: Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism	.73				.63		
R7: Indicate their intention to travel and participate in overseas conflict	.57						
K1: Demonstrate an interest in learning combat skills		.79					
K2: Showcase interest in the use of weapons and explosives		.65					
P1: Desire to explore different ideologies and beliefs—inconsistent identity		.61				.56	
PG3: Express frustration with the injustice targeted at one's own community, faith, or belief			-.87				
PG1: Publicise the injustices targeted at one's own community, faith, or belief			-.86				
PG2: Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice			-.70				.61
PG4: Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice			-.62			-.50	
IP1: Presence of supportive family members and friends that discourage terrorist offending				.70		.80	
OP1: Inability to obtain access to the terrorist online community				.69		.77	
IP4: Demonstrate an appreciation for diversity				.58		.77	
S4: Intention to search for opportunity to do something meaningful						.61	
OC4: A sudden increase in the user's activity						.60	
IP3: Disillusioned with using violence to solve problems						.53	

Table 22 (continued)

Indicator	NTU				MTurk		
	1	2	3	4	1	2	3
S3: Express feelings of contempt for own prior practices						.52	
I1: Force friends, colleagues or family to distance themselves from certain group(s) or community							.81
I2: Dehumanise group(s) of concern who hold different viewpoints/ beliefs system							.53
Eigenvalue	15.00	4.35	2.69	2.33	12.37	6.57	2.68
% of explained variance	35.7%	10.3%	6.4%	5.5%	29.4%	15.6%	6.4%

Note. Extraction method: Principal Component Analysis. Rotation method: Oblimin with Kaiser Normalisation. Only factor loadings larger than .50 are featured.

For NTU sample: (1) Involvement in terrorist online communities; (2) weapons; (3) frustration; and (4) protective element.

For MTurk sample: (1) Involvement in terrorist online communities; (2) protective element; and (3) intolerance towards others.

3.2.1 Commonalities Across the Two Samples

Both samples were largely in agreement in relation to the first factor of “involvement in terrorist online communities”. The indicators nested within this factor include cyber behaviours that radicalised or becoming radicalised individuals would exhibit in their attempts to reach out to like-minded others in the terrorist online communities. As one may expect, these are online behaviours that can be easily observed and straightforward in nature.

The next common factor across both samples is that of “protective elements”. The indicators, which defined this factor, revolve around the attitudes and circumstances that reduce the risk of an individual becoming radicalised. However, this factor seems to contain two contradicting themes within the MTurk sample. First, the majority of the indicators were neatly nested within the label of protective elements. It is perhaps the case that the MTurk participants recognised the importance of indicators that would disengage or dissuade radicalising individuals from becoming even more entrenched in their radical ideas. Second, there were three indicators within this factor that focused on identifying individuals who are searching for purpose and significance in their lives. These indicators are recognised within the terrorism literature to be key motivations for joining terrorist groups (Kruglanski et al., 2018; Muluk et al., 2020). Thus, it is essential to note that these three indicators do not exactly serve as protective barriers against terrorism. In other words, for the MTurk sample, there may be a need to divide this factor on “protective elements” into two discrete subparts in order to better capture the essence of these three indicators.

3.2.2 Differences Across the Two Samples

3.2.2.1 Present only within the NTU Sample. Factor 2 of the NTU sample has been labelled as “weapons” due to the loading of indicators that focus on one’s interest in weapons and combat. These are potential indications that the radicalising individual is preparing for an attack, and as such, may feature prominently as red-flags for the participants. It is surprising that this factor was not featured amongst the MTurk sample because of the easier access to weapons and firearms in the United States. Recent trends in the United States suggest that there are many incidents of radicalised individuals purchasing weapons and undergoing target practice at rifle ranges before conducting the attacks (e.g., Omar Mateen in the 2016 Orlando Pulse Nightclub Shooting; Alter, 2016).

Another factor that was featured only within the NTU sample was “frustration”. This factor contained indicators that highlight the perceived grievances that radicalising individuals may express online. Interestingly, these four indicators were all negatively loaded, implying that the participants may perceive the absence of these indicators as a cause of concern instead. There is no straightforward answer to account for the negative loadings. The most viable explanation would correspond to how Hussain (2018) describes these perceived grievances as ‘common experiences’ that everyone is also subjected to, and therefore not unique to the terrorist population. In other words, radicalising individuals may be perceived to have a higher tendency to ‘walk the talk’ rather than spend effort trying to publicise their grievances.

3.2.2.2 Present only within the MTurk Sample. Factor 3 of the MTurk sample was “intolerance towards others”. The indicators with salient loadings on this factor focused on the negative sentiments that radicalising

individuals would use to depict the out-group. Research has shown that the online rhetoric that dehumanised the out-groups—created and propagated by right-wing terrorist groups—have led to an increase in the number of hate crimes committed against the out-groups (Abdul Rahman, 2019). Thus, the high occurrence of hate-related incidents in the United States (260,000 cases of hate crime occurring annually; Giannasi, 2015) may have influenced the MTurk participants to associate such expression of intolerance with online radicalisation.

In sum, the results of the factor analysis can be understood in many different ways, including the fact that all the participants have prioritised the identification of OR1 under the first factor of “involvement in terrorist online communities”. This indicates that both samples would identify a person-of-interest based on this indicator that was found to differentiate violent ISIS foreign fighters from the non-violent ISIS sympathisers (see chapter 5). It also means that they would be looking for individuals who are attempting to reach out to terrorists and/or personalities known for their radical views. The implications are that more knowledge is needed about who these terrorists or radical personalities are, and whether such a list can be routinely updated and communicated to the community. However, this may have the unwanted repercussion of intensifying monitoring efforts on certain segments of the population—especially if the list of names is closely tied to a particular race or religion (Abbas, 2019). It may also result in message fatigue as the community is overwhelmed by the large number of advisories provided by the authorities (Neo, 2019).

Beyond that, the rest of the identified factors revealed how the two samples differ in terms of their perceptions towards the detection of radicalisation in social media posts. One explanation for this could be that the participants were influenced by the information they learned from media reporting and/or from their personal experience (Alakoc, 2019). In this sense, they may have developed certain preconceived opinions about who the terrorists are and how they would behave, and this inevitably impacted their ratings of the indicators. Thus, the next section will attempt to decipher the participants' general awareness of online radicalisation and terrorism.

3.3 Group Differences on General Awareness of Online Radicalisation and Terrorism

3.3.1 Source of Information on Terrorism

The majority of the participants from both samples reported that they learnt about terrorism mostly from the internet ($n = 304$, 30.1%), followed by more traditional information sources such as television ($n = 256$, 25.3%), newspapers ($n = 206$, 20.4%), radio ($n = 82$, 8.1%), research seminars ($n = 58$, 5.8%), books ($n = 56$, 5.6%), and magazines ($n = 46$, 4.6%). While the emphasis of this chapter is on online radicalisation, the results imply that outreach messages about the threats of online radicalisation should not be disseminated solely through the internet and neglect traditional information sources.

Further analyses revealed some differences between the two samples—see Figure 14. NTU participants were more likely to get information from attending research seminars and reading newspapers. This could be attributed to the profile of the participants who were mostly students that have attended

courses on terrorism in their university. On the contrary, the MTurk sample gathered more information from magazines as compared to their NTU counterparts.

Figure 14

Source of Information on Terrorism

Note. The participants can choose more than one option.

On average, MTurk participants ($M = 3.63$, $SE = .08$) agreed to a lesser extent that the media has conveniently associated terrorism with Islam, as compared to the NTU participants ($M = 3.90$, $SE = .07$), $t(381) = -2.45$, $p = .01$. Given that the Singapore government has invested many resources in promoting racial harmony as well as working closely with various religious organisations to counter terrorism (Khader et al., 2019), it may have imbued its citizens with the knowledge that terrorism is not related to any single religion; hence, accounting for the higher ratings. Alternatively, it could perhaps be the case of the MTurk participants being normalised to such an association. As the rates of Islamophobia is higher in the United States as compared to Singapore, MTurk participants were more likely to have come across such pieces of reporting and over time, might have become habituated to them.

The MTurk sample ($M = 3.20$, $SE = .08$) was also more likely to believe that the media has provided sufficient reporting on terrorism, as compared to

the NTU participants ($M = 2.91$, $SE = .08$), $t(381) = -2.28$, $p = .02$. This is not surprising as there are more cases of terrorist attacks in the United States, which tend to hog the headlines of media outlets. Lastly, there is a similar trend across both samples, where the participants perceived their knowledge on terrorism ($M_{MTurk} = 3.49$; $M_{NTU} = 3.01$) to be lower than that of their fellow citizens ($M_{MTurk} = 3.71$; $M_{NTU} = 3.18$). The differences between both samples across these two questions were found to be statistically significant. The lower ratings for the NTU participants could be attributed to the lack of actual attacks occurring in Singapore, thereby making it harder for them to relate to the threat of terrorism—i.e., complacency (Neo, 2019). However, it must be noted that the effect size of these findings is small—see Table 23.

Table 23
Group Differences on Questions Relating to Information Source

Indicator	MTurk		NTU		<i>t</i>	<i>r</i>
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>		
The media conveniently links terrorism with Islam	3.63	1.04	3.90	0.95	-2.45*	.13
There is sufficient fair coverage on terrorism in the media	3.20	1.13	2.91	1.11	2.28*	.12
I have sufficient knowledge on the threat of terrorism in my country	3.49	0.97	3.01	1.07	4.14**	.22
My fellow citizens are aware of the threat of terrorism	3.71	0.97	3.18	1.04	4.68**	.25

Note. * $p < .05$. ** $p < .00$.

3.3.2 Definition of Terrorism

While it is impossible to decide if the participants had a clear sense of what terrorism means, what emerged was that there is no one distinct definitional element that they chose to define the term. The breakdown of the findings—see Figure 15—is as follows: hijacking ($n = 260$, 23.9%), killing of civilians ($n = 222$, 20.4%), murder ($n = 214$, 19.6%), rape ($n = 115$, 10.6%), armed robbery ($n = 110$, 10.1%), riots ($n = 106$, 9.7%), and street demonstrations ($n = 47$, 4.3%). There were 16 entries under the ‘other’

category, and based on a thematic analysis, two general themes emerged. They were “to further radical ideology” ($n = 12$, 1.1%) and “instil fear and panic” ($n = 4$, .4%). In terms of major differences, the findings indicate that the NTU sample perceived acts of killing civilians to be a key component of terrorism as compared to their MTurk counterparts.

Figure 15
Definitional Elements of Terrorism

Note. The participants can choose more than one option.

Both samples ($M_{MTurk} = 4.45$; $M_{NTU} = 4.53$) strongly agreed that terrorism is illegal and unethical, and no significant difference between them was found. In terms of the likelihood of an attack occurring in their home country, MTurk participants ($M = 3.79$, $SE = .07$) rated significantly higher than the NTU sample ($M = 3.38$, $SE = .07$), $t(381) = -3.78$, $p = .00$, $r = .20$. The many terrorist attacks (e.g., 9/11, Orlando shooting) that had happened in the United States may have predisposed the MTurk participants to recognise that the likelihood of an attack occurring is real. As for the NTU sample, the lower ratings could be explained by what Khader et al. (2019, p. xliii) describe as a “superficial sense of security” due to the absence of attacks in Singapore, leading many of its citizens to perceive Singapore to be a safe country. Despite that, further analysis revealed that 52.5% of the participants acknowledged that

an attack is imminent, which is similar to the survey findings conducted by the Ministry of Home Affairs (MHA; 2019) in 2018.

3.3.3 Role of the Internet

Statistical analysis revealed two interesting findings of the role of the internet. Firstly, the participants were generally neutral in their ratings about the internet as a facilitator for terrorism. This is in stark contrast to what the terrorism literature has been emphasising (Conway, 2017; von Behr et al., 2013; Weimann, 2010), suggesting a potential lack of knowledge about the said topic. Between the two groups, a significant difference was found. Participants from MTurk ($M = 3.01$, $SE = .09$) showed a lower rating on this item as compared to the NTU cohort ($M = 3.67$, $SE = .08$), $t(381) = -4.97$, $p = .00$, $r = .26$. Secondly, the overall ratings increased when it comes to the ease with which an individual can be radicalised via the internet. A significant difference between the MTurk sample ($M = 3.68$, $SE = .07$) and NTU sample ($M = 4.13$, $SE = .06$) was found, $t(381) = -4.46$, $p = .00$, $r = .24$. To account for the higher ratings observed in the NTU sample, there is a need to recognise that the majority of the recent arrests in Singapore are individuals who were self-radicalised via the internet (Loke, 2017).

3.3.4 Counter Terrorism Measures

There was a strong consensus amongst the whole group ($M_{MTurk} = 4.00$; $M_{NTU} = 4.54$) that the community has a role to play in countering terrorism. There is a significant difference between the samples on this item, $t(381) = -7.07$, $p = .00$, $r = .36$. One potential reason underlying the higher ratings of the NTU sample could be due to the recent nationwide SGSecure campaign launched by the Singapore government to prepare and inoculate the community

against terrorism (MHA, 2019). Given the positive response for the previous item, it is therefore not surprising that the participants also recognised their role in reporting suspicious characters ($M_{MTurk} = 3.99$; $M_{NTU} = 4.29$). Similarly, the NTU sample provided a higher rating on the need to engage in such behaviours, $t(381) = -3.48, p = .00, r = .19$. This finding is also consistent with the above-mentioned survey conducted by MHA (2019).

Figure 16
Channels to Report Suspicious Behaviours

However, all the participants reported slightly neutral ratings when it comes to their knowledge about the appropriate channels for reporting suspicious behaviours ($M_{MTurk} = 3.54$; $M_{NTU} = 3.43$), and no significant difference between the samples was found. Further probing led to the identification of a wide range of options that they would report to—see Figure 16. Across both samples, the top three channels, which accounted for 80.5% ($n = 305$) of the overall responses, were the “police”, “government agencies”, and “anti-terrorism unit”. However, it is noteworthy that some participants did not have a clear idea of where to report suspicious behaviours—options of “not sure”, “google”, “non-emergencies services”, and “courts” were recorded, and they accounted for 6.4% ($n = 24$) of the responses. While the numbers are

small, it is still vital to ensure that every member of the community knows where to report suspicious behaviours.

In terms of interventions to counter terrorism, such as through the use of military actions, both samples reported a neutral stance. Having said that, MTurk participants ($M = 3.30$, $SE = .10$) rated significantly higher than the NTU sample ($M = 3.01$, $SE = .08$), $t(381) = 2.24$, $p = .02$, $r = .12$. Analysis of the participants' views about the capability of their governments in handling the threat of terrorism found no significant difference between the two samples ($M_{MTurk} = 3.45$; $M_{NTU} = 3.50$). Table 24 summaries these findings.

Table 24
Questions Relating to Countering Terrorism Measures

Indicator	MTurk		NTU		<i>t</i>	<i>r</i>
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>		
The community plays an important role in countering terrorism	4.00	0.79	4.54	0.53	-7.07**	.36
Military action is the most effective way in dealing with terrorism	3.30	1.26	3.01	1.05	2.24*	.12
The government is capable of handling the threat of terrorism	3.45	1.14	3.50	0.89	-.49	.02
I have a role to play in preventing a terrorist attack in my country	3.07	1.21	4.06	0.84	-8.48**	.42
I am responsible for reporting individuals whom I suspect to be radicalised to the authorities	3.99	0.90	4.29	0.61	-3.48**	.19
I know who to report to if I suspect that an individual is radicalised	3.54	1.05	3.43	1.20	.88	.04

Note. * $p < .05$. ** $p < .00$.

When it comes to their role in preventing an attack, MTurk participants ($M = 3.07$, $SE = .09$) rated significantly lower than the NTU sample ($M = 4.06$, $SE = .06$), $t(381) = -8.48$, $p = .00$, $r = .42$. The higher ratings for the NTU participants could be due to the success of the SGSecure movement (Seow, 2019), where citizens were equipped with the knowledge and skills to protect themselves during an attack. Otherwise, it could perhaps be due to the presence of certain barriers that evoke a tendency for inaction. To better understand these

barriers, an open-ended question was asked of the participants about what “would prevent someone from reporting people to the authorities if they observed them showing signs of radicalisation”. Based on a thematic analysis, several general themes were derived—see Figure 17. The top five reasons, which accounted for 78.4% ($n = 316$) of the overall responses, were: fear of reprisal ($n = 124$, 30.8%), fear of ruining close relationships with the person ($n = 89$, 22.1%), fear of reporting wrong information ($n = 39$, 9.7%), cannot be bothered to do anything ($n = 34$, 8.4%), and fear of getting themselves in trouble ($n = 30$, 7.4%). These findings corroborated what MHA (2019) and Neo et al. (2019) have found from their research.

Figure 17
Reasons for Not Reporting

Two particular differences were noted amongst the two groups. Firstly, the NTU sample has identified the fear of ruining close relationships as the primary barrier ($n = 74$) as compared to what the MTurk participants felt ($n = 15$). Secondly, the MTurk sample was more concerned about the fear of reprisal ($n = 72$) as compared to their NTU counterparts ($n = 52$). The participants’ cultural practices could influence their perceptions. Cultural psychology research found that members of individualist cultures (e.g., the United States, which is represented by the MTurk sample) would place a greater emphasis

one's positive sense of self and to have personal control over their lives (Balçetis et al., 2008). This could have led the MTurk participants to worry about how the acts of reporting would negatively affect their own lives. Inversely, members of collectivistic cultures (e.g., Singapore, which is represented by the NTU sample) would place more emphasis on maintaining social harmony and looking out for others (Ozdemir & Hewett, 2010). This could have influenced the NTU participants' decision to perceive the possibility of damaging the close relationships that they have with the person-of-interest as a major barrier.

3.3.5 Radicalisation

It appeared that both samples ($M_{MTurk} = 3.52$; $M_{NTU} = 3.30$) were relatively ambivalent in terms of their opinions that a terrorist must be motivated by radical ideology, and no significant difference between them was found. While they ($M_{MTurk} = 3.82$; $M_{NTU} = 3.89$; no significant difference was found) agreed that an individual could espouse radical ideals without resorting to violence, they disagreed on the extent to which it is considered permissible. MTurk participants ($M = 2.91$, $SE = .09$) expressed less disagreement as compared to the NTU sample ($M = 2.42$, $SE = .08$), $t(381) = 3.97$, $p = .00$, $r = .21$. This could be attributed to the importance that U.S. citizens placed on their freedom of speech—it is considered a birth-right to be able to speak one's mind (Downs & Cowan, 2012). Alternatively, it could be that the NTU participants were more concerned about having radical ideologies being propagated within the community as they recognised the dangers associated with it. This explanation was reinforced by the subsequent analysis regarding the participants' perception that individuals with radical ideas would progress on to conduct physical acts of

violence. It was found that MTurk participants ($M = 4.31$, $SE = .06$) rated lower on this item as compared to the NTU sample ($M = 4.55$, $SE = .04$), $t(381) = -3.03$, $p = .00$, $r = .16$.

Table 25
Questions Relating to Radicalisation

Indicator	MTurk		NTU		<i>t</i>	<i>r</i>
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>		
A terrorist usually starts out by having violent radical ideas	3.52	1.12	3.30	1.18	1.74	.09
It is possible to have violent radical ideas without resorting to terrorism	3.82	1.03	3.89	0.74	-.68	.03
It is not wrong to have violent radical ideas just as long as you do not engage in terrorism	2.91	1.18	2.42	1.03	3.97**	.21
It is possible to move from having violent radical ideas to actually conducting violent acts such as terrorism	4.31	0.81	4.55	0.55	-3.03**	.16
To what extent do you agree or disagree that terrorists are:						
Mentally ill	3.59	1.09	2.93	1.07	5.45**	.29
Religious	3.53	1.07	3.66	1.13	-1.06	.05
From low-income families	3.20	1.13	2.73	1.09	3.81**	.20
Heroic	2.02	1.36	2.06	1.19	-.26	.01
Male	3.65	0.93	2.85	1.13	6.87**	.35

Note. * $p < .05$. ** $p < .00$.

In terms of their opinions about the profile of a terrorist, several significant differences were noted. MTurk participants were more likely to view terrorists as mentally ill ($M_{MTurk} = 3.59$; $M_{NTU} = 2.93$; $t(381) = 5.45$, $p = .00$, $r = .29$), from low-income families ($M_{MTurk} = 3.20$; $M_{NTU} = 2.73$; $t(381) = 3.81$, $p = .00$, $r = .20$), and are male ($M_{MTurk} = 3.65$; $M_{NTU} = 2.85$; $t(381) = 6.87$, $p = .00$, $r = .35$). This implies that the participants from MTurk espoused certain misconceptions about radicalisation, given that the literature (de Bie et al., 2015; Dernevik et al., 2009) has found no profile fitting what the MTurk sample felt was relevant. No significant difference was found for the other two items: terrorists being religious ($M_{MTurk} = 3.53$; $M_{NTU} = 3.66$) and heroic ($M_{MTurk} = 2.02$; $M_{NTU} = 2.06$). These findings are summarised in Table 25.

4. Conclusion

The implementation of any counter terrorism measures needs to account for the potential impact on the community if the authorities want to avoid any harmful consequences. In the case of identifying indicators to detect radicalisation in social media posts, concerted efforts have to be made to situate any empirically derived findings within the context of the community. As community members play an essential role in reporting any inappropriate online content and/or person, it makes practical sense to understand their knowledge and views regarding online radicalisation indicators. Their ability to detect and subsequently report the observed indicators would assist law enforcement in their counter terrorism efforts. Furthermore, the derived insights about the community's general awareness of terrorism and online radicalisation could be used to unearth areas of concern that law enforcement agencies need to pay attention to.

This chapter showed that there were differences in the way NTU and MTurk participants viewed the indicators as well as their level of awareness about online radicalisation and terrorism. The findings indicated that both groups prioritised the identification of the common key predictor found in chapters 5 and 6 (OR1: "attempts to reach out to terrorists"). Nevertheless, results highlighted the need to address certain misconceptions that community members may have about terrorists, and to encourage them to overcome their reluctance to report signs of online radicalisation. There is also the need to remind and impress upon the community members the significance of not associating certain segments of the population—based on their racial and religious affiliations—with terrorism.

Having said that, there are two limitations of interest. Firstly, this study only captured the participants' opinions about the indicators and is therefore not an exact test of their ability to detect them. In other words, it is not an accurate measure of their knowledge of detecting online radicalisation. In order to generalise the findings, future research could consider an experimental setup to observe how individuals would detect indicators from actual terrorists' social media posts. Secondly, it is essential to note that the two samples chosen for this study may not be representative of the 'communities' from which foreign fighters were recruited. Thus, future studies could approach communities that have been identified as sources of foreign fighters (i.e., certain communities in Belgium, the Netherlands, the United Kingdom for the case of ISIS), and conduct this survey among members of these communities. This would increase the relevancy of the survey findings for law enforcement agencies.

In conclusion, I hope that the findings from this chapter have provided preliminary insights about how community members would perceive online radicalisation indicators, and served as a foundation for future studies on community's perceptions towards online radicalisation.

CHAPTER EIGHT: GENERAL DISCUSSION

The internet has become one of the most important arenas for terrorist groups of different affiliations (jihadi, right-wing, left-wing, etc.) to spread their messages and radicalise new supporters. It is, therefore, critical to develop a metric that can assist law enforcement to detect signs of radicalisation based on an individual's digital footprints. To address this concern, this thesis investigated the literature on online radicalisation and risk assessment to identify markers that can be used to detect radicalisation in social media posts.

In chapter 2, a theoretical framework (person-centric, psychosocial, and protective dimensions) within which relevant factors and indicators can be derived, was introduced. To identify these relevant variables, a concurrent approach of a modified Delphi technique and in-depth literature review was conducted in chapter 3 (i.e., study 1). For the modified Delphi technique, seven local SMEs were asked to evaluate a list of factors collated from six terrorism risk assessment tools (MLG, TRAP-18, ERG 22+, VERA-2, IVP, and Cyber-VERA) and identify those that have the greatest relevance for detecting radicalisation via the internet. This was complemented by a literature review conducted in parallel on online radicalisation and led to the creation of 12 person-centric and psychosocial risk factors, and protective factors, and their 42 associated indicators.

In many cases, the terrorists' supporters were radicalised enough to be mobilised from the online realm to the real-world context, and some became foreign fighters—a phenomenon that gained massive attention with the rise of ISIS (Reed et al., 2017). There are also cases where individuals went on to initiate attacks in their home countries after being influenced by the radical

ideologies that they had consumed online (Jerard, 2017). This then begs the question: how can we better assess the risk of those—based on their online activities—who will go on to conduct physical acts of violence? Yet, despite its importance, there is a paucity of empirical research that can address this question and shed light on the difference between violent and non-violent terrorists' supporters. For these reasons, chapters 4 to 6 investigated whether the identified factors and indicators can distinguish between three groups of terrorists' supporters.

In chapter 4 (i.e., study 2), a significant factor was found to distinguish between two groups of ISIS supporters: violent foreign fighters (travelled to join ISIS) and non-violent sympathisers (did not travel to join ISIS). Fighters were found to create more posts that showcased their readiness to commit violence. As a pilot study, study 2 shows the feasibility in using the factors and indicators derived in study 1 to detect signs of online radicalisation, and serves as a model for comparing ISIS fighters with the ISIS sympathisers. The study also provided valuable insights on how to improve the research methodology of subsequent studies in this research.

Chapter 5 (i.e., study 3) extended chapter 4 in two ways. First, the sample size of the ISIS foreign fighters and sympathisers was increased. Second, new criteria for coding and statistical methods for data analysis were adopted. As a result, more distinct differences between the two samples of ISIS supporters were observed. In particular, attempts to reach out to terrorists and/or key nodes within the terrorist online community (i.e., OR1) was found to be the key predictor to identify which ISIS supporters would become foreign fighters. The creation of such posts is linked to a 9.2-time increased in

likelihood for the post creator to travel and become a fighter. While I recognised that the findings might not be generalisable to the larger corpus of the terrorist or ISIS population, they did help to increase our knowledge about detecting markers of online radicalisation using primary data, and in doing so, provided some degree of postdictive validity.

Using the same research methodology as in study 3, chapter 6 (i.e., study 4) compared ISIS fighters against Kurdish fighters. Both groups of terrorists' supporters were influenced by radical online propaganda and left their home countries to join terrorist groups in Syria and Iraq—ISIS fighters join ISIS, whereas Kurdish fighters join Kurdish militia groups. Several differences were observed across the two groups, and the results demonstrated that ISIS fighters were significantly more likely to create posts—before they travelled—that express their frustration about injustice (PG3: 4.16 times more likely), voice their hatred towards those responsible for the injustice (PG4: 4.49 times more likely), incite family and friends to join ISIS (R2: 5.47 times more likely), indicate their willingness to die for ISIS (R3: 7.81 times more likely), and attempt to establish contacts with key nodes within the ISIS online community (OR1: 3.12 times more likely). One common indicator underlying the findings of chapters 5 and 6 is that of OR1, which was found to be a significant predictor of someone becoming an ISIS foreign fighter. This, in turn, helps to increase our understanding about how the online radicalisation process can culminate into acts of real-world violence.

Finally, in chapter 7 (i.e., study 5), the community's perceptions of the above-mentioned 42 indicators, and also their general understanding of online radicalisation and terrorism were surveyed. A 74-item survey was administered

to 160 NTU psychology undergraduates and 160 MTurk workers. The key predictor of OR1—found in earlier chapters—was featured within the top ten rated indicators for both samples, suggesting that the participants have an inclination on what to look out for. Differences between their perceptions were found, and factor analyses uncovered a four-factor and three-factor structure for the NTU and MTurk samples, respectively. These findings revealed valuable insights about what guide the community members in their detection of online radicalisation indicators. As community members are an essential ally in identifying and reporting suspicious behaviours (online or offline), the findings would contribute to the discussion of how law enforcement could better engage and work together with the community members to detect terrorist threats. For example, the results highlighted the need to address certain misconceptions about radicalisation, and to encourage community members to overcome their reluctance to report signs of radicalisation.

Taken together, these studies aim to provide law enforcement officials, policymakers, and academics with a set of factors and indicators that can supplement their work and/or research, and contribute to efforts that mitigate the threat of online radicalisation. Although the studied samples are considered small (as a result, the findings should not be overstated), this research still offers useful insights into the patterns of online behaviours and expressions that would be of interest to practitioners and researchers who are studying the phenomenon of online radicalisation. Table 26 summarises the key findings of this thesis. This last chapter will identify the practical, methodological, and theoretical implications of this research.

Table 26*Summary of Studies Conducted*

Study	Objective	Method	Sample	Key findings
Study 1 (chapter 3)	<ul style="list-style-type: none"> To construct a list of person-centric and psychosocial risk factors, and protective factors, and their associated indicators. 	<ul style="list-style-type: none"> Combination of a modified Delphi technique with a literature review on risk factors for online radicalisation. 	<ul style="list-style-type: none"> A three-round modified Delphi technique with 7 local SMEs, who were asked to evaluate factors—obtained from six terrorism risk assessment tools (MLG, TRAP-18, ERG 22+, VERA-2, IVP, Cyber-VERA)—that are relevant to the endeavour of identifying individuals who may be radicalised via the internet. Literature review in three major databases (PsycINFO, SAGE, ScienceDirect) using the keywords: ‘internet’, ‘radicalisation’, and ‘risk assessment’. Hand searching of relevant literature was also conducted. 	<ul style="list-style-type: none"> 12 person-centric and psychosocial risk factors, and protective factors, and their associated 42 indicators were identified.
Study 2 (chapter 4)	<ul style="list-style-type: none"> Pilot study. To distinguish ISIS foreign fighters from ISIS sympathisers using their Twitter postings. 	<ul style="list-style-type: none"> Content analysis: Mapping of tweets to factors and indicators. T-test was used to measure the differences in the frequency of the coded indicators. 	<ul style="list-style-type: none"> $N = 6$ 3 fighters, 3 sympathisers 622 Tweets Range of kappa values = .78 to .86 	<ul style="list-style-type: none"> Factor “readiness to use violence” can be used to distinguish ISIS fighters from ISIS sympathisers. Suggestions to improve the research methodology were identified.
Study 3 (chapter 5)	<ul style="list-style-type: none"> To build on from study 2 To differentiate between ISIS foreign fighters and ISIS sympathisers using their social media posts. 	<ul style="list-style-type: none"> Content analysis: Mapping of posts to factors and indicators. Fisher’s exact test was used to measure the differences in the presence and absence of the coded indicators. 	<ul style="list-style-type: none"> $N = 36$ 17 fighters, 19 sympathisers 22,457 posts from various social media sites Range of ICC values (frequency) = .80 to .91 Range of ICC values (severity) = .76 to .86 	<ul style="list-style-type: none"> Fighters were more likely to reach out to terrorists and/or key nodes within the terrorist online communities (OR1), and encourage their family and friends to join them in defending Islam (R2). In contrast, sympathisers tend to show their support to ISIS by displaying ISIS related symbols on their social media (C2). Fighters’ postings were rated to be significantly more severe as compared to the sympathisers.

Table 26 (continued)

Study	Objective	Method	Sample	Key findings
Study 3 (cont.)	<ul style="list-style-type: none"> To identify the predictor(s) that could be used to identify ISIS foreign fighters. 	<ul style="list-style-type: none"> Mann-Whitney U test was utilised to measure the differences in the severity ratings of the coded indicators. MDS (PREFSCAL) was employed to explore how the indicators may cluster across the fighters and sympathisers. Binary logistic regression was utilised to identify predictor(s) for someone to become an ISIS foreign fighter. 		<ul style="list-style-type: none"> Three behavioural typologies were found: sympathisers (located within the cluster of indicators known as “contribute to the online community”), foreign fighters (located within the clusters of indicators known as “strong support towards group” and “frustration”), and ‘fighter-sympathiser’ group (located close to the indicators from the “frustration” cluster, and is further away from those belonging to the “contribute to the online community” cluster). One significant predictor (OR1) was found. A post that mapped onto this indicator would increase the likelihood of the post creator to travel to Syria by 9.2 times. Demonstrated some degree of postdictive validity.
Study 4 (chapter 6)	<ul style="list-style-type: none"> To investigate the external generalisability of the factors and indicators using a different comparison group. To differentiate between ISIS fighters and Kurdish fighters using their social media posts. To identify the predictor(s) that could be used to identify ISIS foreign fighters. 	<ul style="list-style-type: none"> Content analysis: Mapping of posts to factors and indicators. Fisher’s exact test was used to measure the differences in the presence and absence of the coded indicators. Mann-Whitney U test was utilised to measure the differences in the severity ratings of the coded indicators. MDS (PREFSCAL) was employed to explore how the indicators may cluster across the ISIS fighters and Kurdish fighters. 	<ul style="list-style-type: none"> $N = 40$ 17 ISIS fighters, 23 Kurdish fighters 23,958 posts from various social media sites Range of ICC values (frequency) = .81 to .93 Range of ICC values (severity) = .72 to .87 	<ul style="list-style-type: none"> ISIS fighters were more likely than their Kurdish counterparts to highlight grievances affecting the group (PG1, PG2, PG3, PG4), express a higher level of intolerance towards others (I3, I4), and reach out to like-minded individuals (C1, OR1). As compared to ISIS fighters, Kurdish fighters were more likely to post photos of weapons and combat on their social media (K2). ISIS fighters’ postings were rated to be significantly more severe for topics on grievances and intolerance towards communal living, as compared to the Kurdish fighters. Two behavioural typologies were found: Kurdish fighters (situated within the cluster known as “sensational interest”; some Kurdish fighters also exhibited some degree of association with the “frustration” cluster), and ISIS fighters (located within the cluster of indicators known as “frustration”).

Table 26 (continued)

Study	Objective	Method	Sample	Key findings
Study 4 (cont.)		<ul style="list-style-type: none"> Binary logistic regression was utilised to identify predictor(s) for someone to become an ISIS fighter. 		<ul style="list-style-type: none"> Five significant predictors were found. ISIS fighters were significantly more likely to have posts that express their frustration about injustice (PG3: 4.16 times more likely), voice their hatred towards those responsible for the injustice (PG4: 4.49 times more likely), incite family and friends to join ISIS (R2: 5.47 times more likely), indicate their willingness to die for ISIS (R3: 7.81 times more likely), and attempt to establish contacts with key nodes within the ISIS online community (OR1: 3.12 times more likely). Demonstrated some degree of postdictive validity. OR1 (common predictor from studies 3 and 4) was featured within the top ten rated indicators for both samples. A four-factor structure was identified for the NTU sample: (1) Involvement in terrorist online communities; (2) weapons; (3) frustration; and (4) protective element. A three-factor structure was yielded for MTurk sample: (1) Involvement in terrorist online communities; (2) protective element; and (3) intolerance towards others. There were differences between the two samples with regards to their awareness of online radicalisation and terrorism. Results highlighted the need to address certain misconceptions about radicalisation, and to encourage community members to overcome their reluctance to report signs of radicalisation.
Study 5 (chapter 7)	<ul style="list-style-type: none"> To gain an understanding of the community's perceptions towards the indicators. To obtain a 'situational understanding' of their awareness of online radicalisation and terrorism. 	<ul style="list-style-type: none"> A 74-item survey was administered. T-test was used to measure the differences in the ratings of the items. Factor analysis using principal components analysis with oblique (oblimin) rotation was conducted. Parallel analysis was utilised to prevent over-factoring. Thematic analysis was employed to identify themes for the open-ended responses. 	<ul style="list-style-type: none"> $N = 320$ 160 NTU undergraduates, 160 MTurk workers 	

1. The Detection of Online Radicalisation

The studies presented above offer a new perspective on circumventing the threat of online radicalisation in a way that considers the influence of person-centric and psychosocial risk factors, and protective factors on an individual's online behaviours and expressions. Specifically, it examines whether the individuals' online activities can be used to provide any signs of progression of their online radicalisation pathway, which in this case, means becoming foreign fighters; and if so, what are these indicators.

The idea of investigating online activities and their ascribed meaning emerged from social sciences literature, which argues that an individual's belief systems, values, motivations, etc. can be inferred from their online activities (Golbeck et al., 2011), and are correlated with their real-world behaviours (Kosinski et al., 2013). Recognising the feasibility of identifying and assessing terrorist online activities, there has been a growing trend where researchers have harnessed the online information collected from terrorists and subjected it to empirical inquiry (Cohen et al., 2014; Kalpakis et al., 2018). For example, Pressman and Ivan (2016) developed the Cyber-VERA tool to assess cyber behaviours that encourage and/or support terrorism-related activities, and demonstrated the utility of the tool using a case study analysis on Emerson Winfield Begolly.

While these studies strengthened our understanding of how terrorist online networks operate, they, however, focused more on either examining the entire online ecosystem in general, or adopting a single case study methodology. From a law enforcement perspective, these research endeavours

may not shed much insights in differentiating between potential non-violent and violent terrorists' supporters. As Taylor and Horgan (2006) contend,

Individual terrorists do not appear 'fully fledged' as terrorists; they become terrorists through involvement in terrorism, they have to be trained both in terms of what they do (the mechanics of their trade as it were) and in terms of how they make sense of what they do (ideological formation). The aspirant terrorist comes from somewhere physically and psychologically, and he belongs in a social context that is outside of terrorist life (if only by virtue of not having "crossed the boundary" to illegality). (p. 595)

In short, many of the online terrorists' supporters are not what Taylor and Horgan (2006) would describe as full-fledged terrorists, but this, of course, does not dictate that they would not become terrorists in the future. Some of them have been known to transition offline and became foreign fighters or conducted attacks in their home countries. The rest would remain as strong advocates for terrorist groups and continue proselytising on behalf of the groups (Klausen et al., 2012). The fear of incarceration (Mascini, 2006) and the lack of motivation or capability (Knight et al., 2019) are common reasons preventing supporters' radicalisation into violence, despite them adhering to the same radical worldviews as terrorists. Taking that into account, the studies conducted in this thesis represent a stepping stone to highlight what can be done to harness open-source information to predict which terrorists' supporters are most likely to 'tip-over' and engage in more extreme behaviours.

The present findings, therefore, add to the general terrorism literature by being one of the first few empirical attempts to examine the online activities of terrorists' supporters and identify those who would go on to perpetrate violence—i.e., become a foreign fighter. The critical point in this thesis is the

use of social media posts of the foreign fighters before they made their travel to the conflict zone. This approach will provide a valuable glimpse into their cognitions and behaviours before they tipped over into violence, and allow for meaningful comparison with the sympathisers—who are seen as avid supporters of terrorist groups but did not travel to the conflict zone. Furthermore, by doing so, we can better aggregate and identify the online behaviours and expressions that demand the authorities' attention.

A deliberate decision was made to move beyond the detailed enumeration of warning indicators (cf. National Counter Terrorism Center, 2011) to also direct research attention on the potential co-occurrence of the indicators. This is predicated on the fact that terrorism behavioural indicators are known to cluster together (Goodwill & Meloy, 2019). Correspondingly, the present results highlighted several behavioural profiles associated with the three groups of terrorists' supporters. For example, ISIS foreign fighters tend to show a stronger co-occurrence with indicators that belonged to the clusters labelled as “strong support towards groups” and “frustrations”—see chapter 5. Furthermore, the research has highlighted key predictors that could be used to identify who would become an ISIS fighter. The violent ISIS foreign fighter sample was compared against the non-violent ISIS supporters (deriving the indicator OR1), and violent Kurdish foreign fighters (deriving five indicators: PG3, PG4, R2, R3, and OR1).

These are several implications of this thesis' work for the detection of online radicalisation. Besides allowing us to demonstrate some degree of postdictive validity (through the use of binary logistic regression to identify key predictors of someone becoming an ISIS fighter), the findings have also

highlighted common characteristics exhibited by the three groups of terrorists' supporters. In other words, there are grounds to position the identified set of factors and indicators as an 'operationally relevant research' (see Borum, 2015b) that practitioners and academics can utilise to guide the collection and interpretation of online behaviours and expressions.

Figure 18

Assessment of Risk using the Indicators

At the same time, the results indicate that there could be the possibility of creating conditional rules, which Davis et al. (2013) argue is a superior means of assessing risk. In this context, upon the detection of a particular indicator, the user should also keep a lookout for other indicators that are known to co-occur. This means using the entire set of factors and their indicators to triangulate the assessment (see Figure 18) in order to gain greater confidence in determining whether law enforcement should probe further. Central to this is the recognition that many of these indicators described herein may be insignificant on their own in elucidating whether the threat is real. Nevertheless, one must be careful not to go too far down the path of creating conditional rules given that predictions and expectations of future human behaviours often fail in reality. Hence, any standardised approach to use the

findings for investigation should be tempered with a contextual, case-by-case qualitative assessment.

Finally, it is not necessarily the case that terrorists' supporters would conduct all their behaviours in the cyber realm (von Behr et al., 2013), and there is the possibility that no discernible patterns of online behaviour and expression could be found. This point was succinctly made by Jayakumar (2019) in his analysis of the Kurdish foreign fighters,

It is difficult, however, to attempt any estimates as to how many individuals had their thinking (and their decisions to travel to the conflict zone) shaped primarily through social media. Suffice to say that while social media played a role in influencing many individuals (and also in facilitating contacts either with individuals already in the conflict zone or with those who could assist in their travel), a great deal takes place in channels beyond public Facebook profiles. Any attempt to shed light on individual decision-making is further complicated by the fact that a great deal of the evolution of the individual's psyche and mental make-up, particularly in the crucial weeks or months before making the decision to go to Syria or Iraq, has probably taken place offline (or, in private online spaces). (p. 14)

Thus, there is a need to be mindful of the developments in the physical realm and their influence on the individual. With that in mind, we should view the factors and indicators as an online-centric metric that adds to the overall picture of risk assessment—e.g., complement other terrorism risk assessment tools.

2. Implications for Online Risk Assessment

Practitioners and researchers have utilised various risk assessment approaches such as clinical, actuarial, and structured professional judgement to assess and make predictions about the likelihood of an individual reoffending (Monahan, 2012; Powis et al., 2019; Pressman, 2009). Although interest in risk assessment for online radicalisation is relatively recent, many terrorism-specific

risk assessment tools have been constructed. Recognising the potential utility of extrapolating insights from these existing terrorism risk assessment tools, a modified Delphi technique was conducted—in chapter 3—with seven local SMEs to identify factors (collated from six extant tools) that are suitable for assessing the risk for online radicalisation. The initial list of factors derived from the modified Delphi technique was then analysed in conjunction with an in-depth literature review on online radicalisation to construct the final set of 12 person-centric and psychosocial risk factors, and protective factors, and their associated 42 indicators. While the research was informed by the risk assessment literature (due to the use of the six terrorism risk assessment tools and literature review), I do not profess that the identified set of factors and indicators to be a clinical, actuarial, nor structured professional judgement tool because of the lack of validation. Instead, the factors and indicators are best used as an investigative template for users to collect and triangulate open-source information.

Nonetheless, the current set of studies do contribute important insights to the field of online risk assessment. First, it joins the growing list of empirical terrorism studies that focus on the online sphere. Specifically, it found significant predictors that can be used to identify ISIS fighters before they travelled to Syria. Second, it underscores the vital role that a proper control group (i.e., ISIS sympathisers, Kurdish foreign fighters) can play in ascertaining indicators that may precede acts of violence, and marks a significant step towards testing and validating the indicators, which is a critical component of risk assessment. While I acknowledged that the findings might not be generalisable to the entire terrorist population, they did help to further our

knowledge and capacity to distinguish terrorists' supporters who would engage in violence from their non-violent counterparts. This section will discuss two areas of research where the findings can contribute to the sciences of online risk assessment.

2.1 Mapping of Indicators to Radicalisation Models

One of the suggested future directions from chapter 5 was to explore how the changes in online behaviours or expressions could be tracked over time. With that in mind, the proposed solution is to map the factors and indicators onto an online radicalisation model. Similar endeavour has been made by the “Countering online Violent Extremism Research (CoVER) program” at Curtin University (cited in Aly, 2017, p. 73). The researchers from CoVER incorporated warning signs of individuals engaging with radical online materials into the online radicalisation model created by Weimann and von Knop (2008; see section 2.2.1 of chapter 2), and five behavioural profiles were created.

In this case, for the purpose of illustration, the factors identified in chapter 3 are mapped to the RECRO model (Neo, 2016; see Table 27). While some individuals may radicalise slowly over many months, the process can take weeks for others. However, what can be ascertained is that one's involvement in online radicalisation is a process by which individuals move from socially normative opinions and perspectives towards more extreme ones, or where the intensity of their attachment to radical ideas grows evermore zealous. Thus, the different phases of the RECRO model present themselves as milestones to capture and examine how each factor may manifest at each phase and influence the subsequent radicalisation phases. In other words, it allows for the

identification and comparison of the changes in relative risk from person to person (based on the phases and the detection of the factors within), despite differences in the timescale of their radicalisation trajectories.

Table 27

Mapping the Factors to RECRO

Phase	Description	Factor
Reflection	The triggers, needs, and vulnerabilities that an individual may have, which increase their receptiveness towards alternative belief systems.	<ul style="list-style-type: none"> • “Personal uncertainty” (P)
Exploration	The period where the individual begins making sense of the online information put forth by terrorists.	<ul style="list-style-type: none"> • “Online relationship building with like-minded individuals” (OR) • “Perceived grievances” (PG) • “Redemption and the pursuit for significance” (S)
Connection	The influence of like-minded individuals within the terrorist online community.	<ul style="list-style-type: none"> • “Negative social support” (N) • “Intolerance towards multi-religious, multi-racial living (I)” • “Involvement in the terrorist online community” (OC)
Resolution	The period during which the individual gains the momentum to translate one’s radical beliefs into action.	<ul style="list-style-type: none"> • “Commitment to terrorist groups” (C)
Operational	The period during which the individual is ready to commit violence to further the group’s cause both online and/or offline.	<ul style="list-style-type: none"> • “Readiness to use violence” (R) • “Knowledge and skill to commit terrorist offences” (K)

Note. The two protective factors (“Individual-centric protective elements” [IP], “Online environment-centric protective elements” [OP]) are not included as their influence may transcend across the phases. Adapted from “An internet-mediated pathway for online radicalisation: RECRO”, L. S. Neo, 2016, In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era*, pp. 197-224, (<https://doi.org/10.4018/978-1-5225-0156-5.ch01>). Copyright 2016 by IGI Global.

2.2 Automating the Screening Process

Traditional methods of data collection have limitations in detecting and stopping foreign fighters before they can travel to the conflict zones, due to the shorter time taken for them to be radicalised and subsequently mobilised into action. This leaves law enforcement agencies with limited time to respond. In addition, the increasing amount of available data that intelligence agencies need to monitor and sieve through makes manual analysis a daunting task (Davis et

al., 2013). To this end, the findings from this thesis can be used as a starting point for efforts to automate the screening process and assist users such as intelligence officers and analysts to narrow down the data that they need to focus on.

Recent advancements have been made in the computational field to detect signs of online radicalisation (Camacho et al., 2016), screen radical forums and identify acts of cyber recruitment (Scanlon & Gerber, 2014), and identify lone-wolf terrorists based on weak online signals (Brynielsson et al., 2013). Similarly, in my professional capacity, I have also collaborated with the School of Electrical and Electronic Engineering (EEE) in NTU to develop an electronic screening tool—based on machine learning technology—that can flag radical propaganda videos, using some of the insights derived from this thesis. The intention of such collaborations between behavioural sciences and computational informatics is not to replace humans, but rather to supplement and enhance our ability to address the threat of online radicalisation.

3. Broader Implications and Future Directions

With the rapid increase in internet usage worldwide, research on terrorism will have to pander in the same direction. Despite abundant research on terrorism since 9/11, researchers have recently started to explore the field of risk assessment for online radicalisation. The current thesis, therefore, represents a step forth by offering a framework of factors and indicators to detect radicalisation in social media posts and opening multiple avenues for further research within the field. This section will discuss five broad implications that this thesis has on the field of online radicalisation and terrorism.

3.1 Research Design for Terrorism Studies

In a recent review of the terrorism literature, Schuurman (2018) concluded that most terrorism studies—from 2007 to 2016—do not use primary data to derive empirically informed solutions for understanding and countering terrorism. While he acknowledged how this had affected the quality of research, at the same time, he noticed a growing effort by researchers to adopt new data-gathering methods to collect primary data and to conduct advanced statistical analyses on the collected data.

Recognising the need to adopt an empirically-based approach for studying terrorism, this thesis utilised an innovative mixed-method research design to derive a set of factors and indicators, and to analyse social media posts of terrorists' supporters. First, a modified Delphi technique (not commonly utilised in the field of terrorism) was used to elicit the knowledge from SMEs. The derived insights were used in conjunction with an in-depth literature review to identify relevant factors and indicators. Second, in addition to the use of bivariate statistical analyses such as Fisher's exact test and Mann-Whitney U test, multivariate tools such as multidimensional scaling and binary logistic regression were utilised to better elucidate the subtle nuances between the samples of terrorists' supporters—based on the social media posts that were mapped onto the factors and indicators. Lastly, as highlighted earlier, one of the strengths of this thesis is the identification of an appropriate control group (e.g., ISIS sympathisers for the ISIS foreign fighters). This increases our confidence in the findings obtained from this research.

More importantly, the results can help corroborate extant theories such as the 'three pillars of radicalisation: needs, narratives, and networks' by

Kruglanski et al. (2019). In this case, the current findings provide further justification about the importance of ‘needs’ and ‘narratives’ for someone to become radicalised. Future studies could explore how the identified factors and indicators of this thesis can also help elucidate insights about the importance of ‘networks’ in online radicalisation.

It should also be noted that there are some limitations associated with social media research. The inconsistent occurrence of posts across various online platforms (i.e., some terrorists’ supporters prefer one platform over the other, making it hard to compare across platforms), as well as the difficulty in finding the ‘right’ type of data for analysis, are some challenges faced by researchers—including this thesis. While researchers obsess about the quality and quantity of the data, it would be useful for future studies to not only enhance the data collection and coding process but also to identify relevant statistical tools for distilling the nuances across the variables. One potential avenue of overcoming these difficulties is to borrow insights from adjacent fields, such as criminology and internet addiction, which have amassed knowledge about online risk assessment through their research on online vices. There have also been recent efforts to improve the way researchers conduct terrorism research. Some have attempted to develop base rates for risk factors and indicators (Clemmow et al., 2020), whereas others have implemented a systematic approach to measure the severity of an online forum (Scrivens et al., 2018). There were also efforts to utilise social network analysis to identify leaders or key nodes in terrorist networks (Choudhary et al., 2019). These new developments will pave the path for others to build on and inform practical outcomes for countering terrorism.

In sum, some important questions that practitioners, policymakers, and academics should consider are:

- How can we enhance our coding procedures in order to distil the best nuances from the online data?
- What sort of statistical tools are best suited for analysing low base-rate phenomena such as terrorism and online radicalisation?
- What research design can we learnt from adjacent fields, such as internet addiction, to enhance our ability to do conduct online risk assessment?

3.2 Ethical Issues

The second implication pertains to the ethical considerations surrounding the collection of online data. The harvesting of personal data from social media platforms entails many ethical and privacy concerns, which is best illustrated by the recent Cambridge Analytica scandal (Watkin, 2019). In some jurisdictions, the collection and usage of big data could conflict with data privacy laws or laws regulating search and surveillance. It could also raise ethical issues of using users' data for purposes which they had not consented to (Gstrein et al., 2019). In this thesis, the names of the social media account holders were not disclosed, and all the online handles of the accounts were de-identified and given specific identifiers—e.g., A1 for accounts belonging to foreign fighter 1. Arguably, more should be done if the stream of research in this direction is expected to increase. For example, terrorism researchers can consider creating an ethical guideline to inform the data collection process.

Furthermore, based on available published research (Kipane, 2019; Torres-Soriano, 2019), there is the possibility that terrorists have employed

tactics to conceal their online identity, or to mislead investigators. This could have negative implications if the findings—based on the collected data—were used to infer attributes associated with online radicalisation, resulting in a potential case of misidentification of the terrorist threat. Thus, researchers and practitioners have an ethical obligation to recognise this possibility, and that there is some factual uncertainty attached to attribution of indicators with features of online radicalisation when they are weighing evidence.

In sum, some important questions that practitioners, policymakers, and academics should consider are:

- Who should be entitled to harvest data from the internet?
- Is there a need for a code of ethics (to inform data collection) amongst terrorist researchers?
- How can terrorist researchers work better with social media companies without infringing on ethical and privacy concerns?

3.3 Terrorists' Learning Capability

The question of how and why terrorists are able to circumvent counter measures by authorities have a direct connection to a much broader question about their learning capability (see Jackson et al., 2005). Researchers have observed that terrorists and their supporters have grown more circumspect and displayed an increased level of security awareness. For example, Jayakumar (2019) notes how terrorists' supporters have assumed fake social media identities and posted less information about themselves online. In many occasions, some whose Facebook or Twitter accounts were suspended have moved on to alternative platforms, such as the dark web (Hussain & Saltman, 2014), VKontakte (Banerjee, 2015), and Telegram (Bloom & Daymon, 2018).

These developments, therefore, increase the challenges facing researchers who are trying to collect relevant data about terrorists' online activities. Following this train of thought, the indicators identified in this thesis may become obsolete once terrorists and their supporters changed the way they operate and communicate online. Thus, there is a need for future research to keep abreast of the latest developments concerning terrorists' usage of online platforms and continue to explore how their cyber behaviours and expressions may have changed.

In sum, some important questions that practitioners, policymakers, and academics should consider are:

- What are the up-and-coming online platforms that terrorists may exploit?
- How much do we know about the dark web and the extent to which terrorists are using it?
- How can we interfere in the learning capability of terrorists?

3.4 Generalising the Findings to Different Terrorists' Supporters

Another implication relates to the generalisability of the present findings to other types of terrorists' supporters. The small sample size and limited range of comparison done (ISIS fighters versus ISIS sympathisers in chapters 4 and 5; ISIS fighter versus Kurdish fighters in chapter 6) in the current thesis make it challenging to generalise the findings. Nevertheless, based on the studied samples, key observations and predictors have emerged from the analyses. Future work should continue to test these factors and indicators with other samples of terrorists and their supporters. For example, we can compare the social media posts of terrorists' supporters from different countries and/or

gender as previous works have highlighted different motivations underlying the recruitment process (Gan et al., 2019; Pearson, 2018; Schulze & Liow, 2019).

Some important questions that practitioners, policymakers, and academics should consider are:

- What are the vulnerable groups that terrorists would target for recruitment via the internet?
- Is there a cultural influence on the radicalisation process?
- Where is the next conflict zone and who is most likely to be mobilised via the internet?

3.5 Inoculate the Community Against Online Radicalisation

Given that terrorist groups are increasingly proficient in making their presence felt online, it is necessary to equip our community members with the ability to discern information that they consumed on the internet. For example, Chen et al. (2020) recommend imbuing community members with fact-checking skills and educating them about the types of cognitive biases that can affect their decision making. Likewise, Vito (2017) urges that community members, with youths, in particular, should be provided with the best media literacy education, in schools and other educational outlets, in order to counter the increasing amount of radical online propaganda.

It is also necessary to ensure that the community is adequately supplied with knowledge about the threat of online radicalisation, its associated warning indicators, and what community members should do to protect and prepare themselves. Such campaigns (e.g., SGSecure movement in Singapore) should aim to debunk any common misconceptions or myths that the community has and to emphasise that everyone has a crucial role to play in the fight against

terrorism. The authorities have to enlist trusted facilitators or known influencers, who can better resonate with the local community, to deliver such outreach messages if they want to avoid any unwanted consequences—e.g., community members viewing the outreach messages as government propaganda. Experiences from the United Kingdom showed that the distrust of the British government had minimised the credibility and impact of government-run programmes to counter the threat of terrorism (Shabi, 2016).

In sum, some important questions that practitioners, policymakers, and academics should consider are:

- Who should be the one conducting the outreach campaign?
- What key messages should be highlighted during the outreach campaign?
- How can we measure the success of such outreach campaigns?

4. Conclusion

Living in the digital age can be daunting, especially for the law enforcement agencies who are trying their utmost best to keep the society safe and secure. The affordances bestowed by the internet have led to the huge mobilisation of foreign fighters into the Middle East (Stern & Berger, 2015), a rise in self-radicalised cases (Neo, 2016), spates of lone-wolf terrorist attacks in many countries (Weimann, 2012), the continued exposure of the community to radical online propaganda (Reeve, 2019), concerns of terrorists assimilating techniques of cybercrime to conduct acts of sabotage (Dillon, 2016), and a growing terrorist online presence (Conway, 2017). The list of threat will continue to grow as new technological advances come into the picture.

Moreover, the rise and fall of the Islamic State in Iraq and Syria serves as a warning against the naïve thinking that the threat of ISIS would simply disappear. It is not the first conflict that attracts foreign fighters, and it will not be the last. Such ill-informed thinking would occur at the expense of asking more relevant questions that could be used to predict the next conflicts or upcoming threats. In the real world, the continued online propagation of radical ideas by different types of terrorist groups meant that the threat of online radicalisation does not reside solely in the domain of jihadi terrorism. Right-wing foreign fighters, for instance, have travelled to participate in the conflict in Ukraine after consuming the radical rhetoric that they read online (Koch, 2019). Furthermore, the ability of terrorist groups to exploit new technological advancements creates the support infrastructure for radical ideas to take root, and this could make the radical ideas equally dangerous as (if not more than) the actual violence itself. While the manifestation of the threats may change, the underlying principles governing the online radicalisation process remains the same.

Collectively, these developments gave a glimpse of a future where it is bleak and gloomy as the security threats are innumerable. That is not to say that we are helpless against it either. So how can practitioners, policymakers, and academics deal with the threats?

As such, I hope that the set of factors and indicators identified in this thesis can help in the early identification of radicalised individuals. The series of studies have attempted to identify and test the factors and indicators with different samples of terrorists' supporters, as well as to understand the community's perceptions towards them. More importantly, this thesis presents

how psychology can contribute to the field of terrorism by merging social psychology research on group behaviours with personality psychology research on individual characteristics, and risk assessment research to enhance our capability to detect radicalisation in social media posts. In closing, a quote from the Singapore President, Ms Halimah Yacob, is relevant:

We will not see the last of Singaporeans being influenced by what they read and who they meet online. We will likely see more cases of foreign religious teachers preaching hate, or preachers exhorting followers to stay away from those who do not share the same faith. (cited in Lee, 2018, para. 6)

This comment greatly echoes my personal belief that we need to raise our capability to detect radical online propaganda and malicious actors in advance and to raise our level of preparedness against the threat of online radicalisation.

References

- Abbas, M. S. (2019). Producing 'internal suspect bodies': Divisive effects of UK counter-terrorism measures on Muslim communities in Leeds and Bradford. *The British journal of sociology*, 70(1), 261-282.
<https://doi.org/10.1111/1468-4446.12366>
- Abdelkader, E. (2016). *When Islamophobia turns violent: The 2016 U.S presidential elections*. <http://bridge.georgetown.edu/wp-content/uploads/2016/05/When-Islamophobia-Turns-Violent.pdf>
- Abdul Rahman, N. A. (2019). How can right-wing extremism exacerbate Islamophobia after a jihadi attack? Insights from Europe. In M, Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 549-569). World Scientific.
https://doi.org/10.1142/9789813275447_0029
- Adler, M. & Ziglio, E. (1996). *Gazing into the oracle: The Delphi method and its application to social policy and public health*. Jessica Kingsley Publishers.
- Agarwal, S., & Sureka, A. (2015). Using knn and svm based one-class classifier for detecting online radicalization on Twitter. In R. Natarajan, G. Barua, & M. R. Patra (Eds.), *International Conference on Distributed Computing and Internet Technology* (pp. 431-442). Springer.
https://doi.org/10.1007/978-3-319-14977-6_47
- Alakoc, B. P. (2019). Terror in the classroom: Teaching terrorism without terrorizing. *Journal of Political Science Education*, 15(2), 218-236.
<https://doi.org/10.1080/15512169.2018.1470002>
- Alam, F., Stepanov, E. A., & Riccardi, G. (2013, June). Personality traits recognition on social network-Facebook. In *Seventh International AAAI Conference on Weblogs and Social Media*.
<https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/view/6167/6307>
- Ali, M. B. (2014). 'Jihad' in Syria: Fallacies of ISIS' end time prophecies. RSIS Commentaries (149/2014). S. Rajaratnam School of International Studies. <https://dr.ntu.edu.sg/bitstream/10356/103199/1/RSIS1492014.pdf>

- Allport, G. W. (1961). *Pattern and growth in personality*. Holt, Rinehart & Winston.
- Alter, C. (2016, June 14). Orlando shooter bought gun legally, gun owner says. *TIME*. <http://time.com/4367592/orlando-shooting-gun-store-owner/>
- Aly, A. (2017). Brothers, believers, brave mujahideen: Focusing attention on the audience of violent jihadist preachers. *Studies in Conflict & Terrorism*, 40(1), 62-76. <https://doi.org/10.1080/1057610X.2016.1157407>
- Aly, A., Weimann-Saks, D., & Weimann, G. (2014). Making ‘noise’ online: An analysis of the say no to terror online campaign. *Perspective on Terrorism*, 8(5), 33-47.
<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/376>
- Andre, V. (2012). ‘Neojihadism’ and YouTube: Patani militant propaganda dissemination and radicalization. *Asian security*, 8(1), 27-53.
<https://doi.org/10.1080/14799855.2012.669207>
- Archetti, C. (2015). Terrorism, communication and new media: Explaining radicalisation in the digital age. *Perspective on Terrorism*, 9(1), 49-59.
<https://www.jstor.org/stable/26297326>
- Awan, I., & Guru, S. (2017). Parents of foreign “terrorist” fighters in Syria – will they report their young? *Ethnic and Racial Studies*, 40(1), 24-42.
<https://doi.org/10.1080/01419870.2016.1206588>
- Back, M. D., Stopfer, J. M., Vazire, S., Gaddis, S., Schmukle, S. C., Egloff, B., & Gosling, S. D. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological science*, 21(3), 372-374.
<https://doi.org/10.1177%2F0956797609360756>
- Badawy, A., & Ferrara, E. (2018). The rise of jihadist propaganda on social networks. *Journal of Computational Social Science*, 1(2), 453-470.
<https://doi.org/10.1007/s42001-018-0015-z>
- Baines, P. R., O’Shaughnessy, N. J., Moloney, K., Richards, B., Butler, S., & Gill, M. (2010). The dark side of political marketing: Islamist propaganda, Reversal Theory and British Muslims. *European Journal of Marketing*, 44(3-4), 478-495.
<https://doi.org/10.1108/03090561011020543>

- Bakker, E., & Singleton, M. (2016). Foreign fighters in the Syria and Iraq conflict: Statistics and characteristics of a rapidly growing phenomenon. In A. de Guttery, F. Capone, & C. Paulussen (Eds.), *Foreign fighters under international law and beyond* (pp. 9–25). Asser Press.
- Balcutis, E., Dunning, D., & Miller, R. L. (2008). Do collectivists know themselves better than individualists? Cross-cultural studies of the holier than thou phenomenon. *Journal of Personality and Social Psychology*, 95(6), 1252-1267. <https://doi.org/10.1037/a0013195>
- Bandura, A. (2004). The role of selective moral disengagement in terrorism and counterterrorism. In F. M. Moghaddam, & A. J. Marsella (Eds.), *Understanding terrorism: Psychosocial roots, causes and consequences* (pp. 121-150). American Psychological Association. <https://doi.org/10.1037/10621-006>
- Banerjee, S. (2015, May 31). Jihadists' social-media recruitment sparks online battle. *CBC News*. <http://www.cbc.ca/news/canada/montreal/jihadists-socialmedia-recruitment-sparks-online-battle-1.3094600>
- Barlas, J., & Egan, V. (2006). Weapons carrying in British teenagers: The role of personality, delinquency, sensational interests, and mating effort. *The Journal of Forensic Psychiatry & Psychology*, 17(1), 53-72. <https://doi.org/10.1080/14789940500407692>
- Barnes, B. (2012). Confronting the one-man wolf pack: Adapting law enforcement and prosecution responses to the threat of lone wolf terrorism. *Boston University Law Review*, 92, 1613-1662. <https://ssrn.com/abstract=2177295>
- Barrelle, K. (2015). Pro-integration: disengagement from and life after extremism. *Behavioral Sciences of Terrorism and Political Aggression*, 7(2), 129-142. <https://doi.org/10.1080/19434472.2014.988165>
- Bartlett, J., & Miller, C. (2013). *The state of the art: A literature review of social media intelligence capabilities for counter-terrorism*. DEMOS. <https://www.publicsafety.gc.ca/lbrr/archives/cn28613-eng.pdf>
- Baumgarten, N. (2017). Othering practice in a right-wing extremist online forum. *Language@ Internet*, 14(1). <https://www.languageatinternet.org/articles/2017/baumgarten>

- Bayerl, P. S., Sahar, A., & Akhgar, B. (2020). The radicalisation-factor model (RFM): Proposing a framework for the systematic investigation and modelling of online radicalisation. In B. Akhgar, D. Wells, & J. M. Blanco (Eds.), *Investigating radicalization trends: Case studies in Europe and Asia* (pp. 29-39). Springer.
- Bell, S. (2014, November 25). More than 100 Canadians have offered to join Kurds in fight against ISIS. *National Post*.
<http://news.nationalpost.com/news/more-than-100-canadians-have-offered-to-join-kurds-in-fight-against-isis>
- Benmelech, E., & Klor, E. F. (2018). What explains the flow of foreign fighters to ISIS? *Terrorism and Political Violence*, 1-24.
<https://doi.org/10.1080/09546553.2018.1482214>
- Berger, J. M. (2018). *Extremism*. MIT Press.
- Berger, J. M., & Morgan, J. (2015). *The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter*. The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper #20.
https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf
- Bergin, A., Osman, S., Ungerer, C., & Yasin, N. A. M. (2009). *Countering Internet radicalisation in Southeast Asia*. Special Report. Australian Strategic Policy Institute. <https://www.aspi.org.au/report/special-report-issue-22-countering-internet-radicalisation-southeast-asia>
- Bhui, K., & Ibrahim, Y. (2013). Marketing the “radical”: Symbolic communication and persuasive technologies in jihadist websites. *Transcultural Psychiatry*, 50(2), 216-234.
<https://doi.org/10.1177/1363461513479329>
- Bishopp, D., & Hare, R. D. (2008). A multidimensional scaling analysis of the Hare PCL-R: Unfolding the structure of psychopathy. *Psychology, Crime & Law*, 14(2), 117-132. <https://doi.org/10.1080/10683160701483484>
- Bjørger, T. (2009). Processes of disengagement from violent groups and the extreme right. In J. Horgan, & T. Bjørger (Eds.), *Leaving terrorism behind: Individual and collective disengagement* (pp. 30-48). Routledge.
- Bjørger, T., & Horgan, J. (2009). *Leaving terrorism behind: Individual and collective disengagement*. Routledge.

- Bloom, M., & Daymon, C. (2018). Assessing the future threat: ISIS's virtual caliphate. *Orbis*, 62(3), 372-388.
<https://doi.org/10.1016/j.orbis.2018.05.007>
- Bloombaum, M. (1970). Doing smallest space analysis. *Journal of Conflict Resolution*, 14(3), 409-416. <https://www.jstor.org/stable/173520>
- Böckler, N., Hoffmann, J., & Zick, A. (2015). The Frankfurt airport attack: A case study on the radicalization of a lone-actor terrorist. *Journal of Threat Assessment and Management*, 2(3-4), 153-163.
<https://psycnet.apa.org/doi/10.1037/tam0000045>
- Bodine-Baron, E., Helmus, T. C., Magnuson, M., & Winkelman, Z. (2016). *Examining ISIS Support and Opposition Networks on Twitter*. RAND.
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/R1328/RAND_RR1328.pdf
- Borum, R. (2011a). Radicalisation into violent extremism I: A review of social science theories. *Journal of Strategic Security*, 4(4), 7-36.
<http://dx.doi.org/10.5038/1944-0472.4.4.1>
- Borum, R. (2011b). Radicalization into violent extremism II: A review of conceptual models and empirical research. *Journal of Strategic Security*, 4(4), 37-62. <http://dx.doi.org/10.5038/1944-0472.4.4.2>
- Borum, R. (2014). Psychological vulnerabilities and propensities for involvement in violent extremism. *Behavioral Sciences & the Law*, 32(3), 286-305. <https://doi.org/10.1002/bsl.2110>
- Borum, R. (2015a). Assessing risk for terrorism involvement. *Journal of Threat Assessment and Management*, 2(2), 63-87.
<http://dx.doi.org/10.1037/10930-005>
- Borum, R. (2015b). Operationally relevant research and practice in terrorism threat assessments. *Journal of Threat Assessment and Management*, 2(3-4), 192-194. <https://doi.org/10.1037/tam0000046>
- Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. *Behavioral Sciences & the Law*, 17(3), 323-337. [https://doi.org/10.1002/\(SICI\)1099-0798\(199907/09\)17:3<323::AID-BSL349>3.0.CO;2-G](https://doi.org/10.1002/(SICI)1099-0798(199907/09)17:3<323::AID-BSL349>3.0.CO;2-G)

- Boulkedid, R., Abdoul, H., Loustau, M., Sibony, O., & Alberti, C. (2011). Using and reporting the Delphi method for selecting healthcare quality indicators: a systematic review. *PloS one*, 6(6).
<https://dx.doi.org/10.1371/journal.pone.0020476>
- Bowman-Grieve, L. (2009). Exploring “Stormfront”: A virtual community of radical right. *Studies in Conflict & Terrorism*, 32(11), 989-1007.
<https://doi.org/10.1080/10576100903259951>
- Bowman-Grieve, L. (2013). A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment. *Security Informatics*, 2(9), 1-5. <https://doi.org/10.1186/2190-8532-2-9>
- Bowman-Grieve, L. (2015). Cyberterrorism and moral panics: A reflection on the discourse of cyberterrorism. In L. Jarvis, S. Macdonald, & T. M. Chen (Eds.), *Terrorism online: Politics, law and technology* (pp. 86-106). Routledge.
- Boyd, R. L., Wilson, S. R., Pennebaker, J. W., Kosinski, M., Stillwell, D. J., & Mihalcea, R. (2015, April). Values in words: Using language to evaluate and understand personal values. In *Ninth International AAAI Conference on Web and Social Media*.
<https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10482/10486>
- Brachman, J. M. (2008). *Global jihadism: Theory and practice*. Routledge.
- Brachman, J. M., & Levine, A. N. (2011). You too can be awlaki!. *The Fletcher Forum of World Affairs*, 35(1), 25-46. <https://www.voxpol.eu/wpfb-file/you-too-can-be-awlaki-pdf/>
- Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C., & Svenson, P. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics*, 2(1), 11.
<https://doi.org/10.1186/2190-8532-2-11>
- Buhrmester, M., Kwang, T., & Gosling, S. D. (2016). *Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality data?* In A. E. Kazdin (Ed.), *Methodological issues and strategies in clinical research* (pp. 133–139). American Psychological Association.
<https://doi.org/10.1037/14805-009>

- Byman, D. (2017, July 13). Frustrated foreign fighters. *Lawfare*.
<https://lawfareblog.com/frustrated-foreign-fighters>
- Caiani, M., & Kröll, P. (2015). The transnationalization of the extreme right and the use of the Internet. *International Journal of Comparative and Applied Criminal Justice*, 39(4), 331-351.
<https://doi.org/10.1080/01924036.2014.973050>
- Callimachi, R. (2015, June 27). ISIS and the lonely young American. *New York Times*. https://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html?mcubz_1
- Camacho, D., Gilpérez-López, I., Gonzalez-Pardo, A., Ortigosa, A., & Urruela, C. (2016, November). *CEUR Workshop Proceedings*. Retrieved from <http://ceur-ws.org/Vol-1794/afcai16-paper5.pdf>
- Cameron, L., Maslen, R., & Todd, Z. (2013). The dialogic construction of self and other in response to terrorism. *Peace and Conflict: Journal of Peace Psychology*, 19(1), 3-22. <https://doi.org/10.1037/a0031471>
- Carter, J. A., Maher, S., & Neumann, P. R. (2014). *#Greenbirds: measuring importance and influence in Syrian foreign fighter networks*. The International Centre for the Study of Radicalisation and Political Violence. <https://icsr.info/2014/04/22/icsr-report-inspires-syrian-foreign-fighters/>
- Carver, C. S., & Scheier, M. F. (2014). *Perspectives on personality* (7th ed). Pearson Education.
- Caspi, D. J., Freilich, J. D., & Chermak, S. M. (2012). Worst of the bad: Violent white supremacist groups and lethality. *Dynamics of Asymmetric Conflict*, 5(1), 1-17. <https://doi.org/10.1080/17467586.2012.679664>
- Ceron, A., Curini, L., & Iacus, S. M. (2019). ISIS at its apogee: the Arabic discourse on Twitter and what we can learn from that about ISIS support and Foreign Fighters. *Sage open*, 9(1).
<https://doi.org/10.1177/2158244018789229>.
- Chen, J., Hsieh, G., Mahmud, J. U., & Nichols, J. (2014, February). Understanding individuals' personal values from social media word use. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing* (pp. 405-414).
<https://doi.org/10.1145/2531602.2531608>

- Chen, X., Yu, J., Goh, P., Neo, L. S., Er, V., & Khader, M. (2020). Crime-fake news nexus. In M. Khosrow-Pour (Ed.), *Encyclopaedia of criminal activities and the deep web* (pp. 52-65). IGI Global.
<https://doi.org/10.4018/978-1-5225-9715-5.ch004>
- Cheong, D. (2017). Radicalised female infant care assistant from PCF Sparkletots detained under ISA for pro-ISIS activities. *The Straits Times*.
<https://www.straitstimes.com/singapore/radicalised-female-infantcare-assistant-from-pcf-sparkletots-detained-under-isa-for-pro>
- Choudhary, P., Singh, U., Dalal, S., & Bisen, D. (2019, February). Social network analysis (SNA): A vision for counter-terrorism approach in modern Indian Defence Sector. In *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3349028
- Cilluffo, F. J., Cozzens, J. B., & Ranstorp, M. (2010). *Foreign fighters: Trends, trajectories and conflict zones*. Homeland Security Policy Institute.
<http://www.diva-portal.org/smash/get/diva2:380558/FULLTEXT01.pdf>
- Clemmow, C., Schumann, S., Salman, N. L. & Gill, P. (2020). The base rate study: Developing base rates for risk factors and indicators for engagement in violent extremism. *Journal of Forensic Sciences*, 1-17.
<https://doi.org/10.1111/1556-4029.14282>
- Cohen, J. (1988). *Statistical power analysis for the behavioural sciences* (2nd ed). Academic Press.
- Cohen, K., & Kaati, L. (2018). *Digital jihad: Propaganda from the Islamic State*. Swedish Defence Research Agency (FOI).
- Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting linguistic markers for radical violence in social media. *Terrorism and Political Violence*, 26(1), 246-256. <https://doi.org/10.1080/09546553.2014.849948>
- Cole, J., Alison, E., Cole, B., & Alison, L. (2010). *Guidance for identifying people vulnerable to recruitment into violent extremism*. University of Liverpool, School of Psychology.
https://www.safecampuscommunities.ac.uk/uploads/editor/files/IVP_Guidance_Draft_v0.3_web_version.pdf
- Combating Violent Extremism. (2016). *Twitter Blogs*.
<https://blog.twitter.com/2016/combating-violent-extremism>

- Community Oriented Policing Services. (2014). *Online radicalisation to violent extremism: Awareness brief*.
<https://www.theiacp.org/sites/default/files/2018-07/RadicalizationtoViolentExtremismAwarenessBrief.pdf>
- Conway, M. (2007). Terrorist use of the Internet and the challenges of governing cyberspace. In D. Myriam, V. Mauer, & F. Krishna-Hensel (Eds.), *Power and security in the information age: Investigating the role of the state in cyberspace* (pp. 95-127). Ashgate.
- Conway, M. (2012). Introduction: terrorism and contemporary mediascapes – reanimating research on media and terrorism. *Critical Studies on Terrorism*, 5(3), 445-453. <https://doi.org/10.1080/17539153.2012.725979>
- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77-89.
<https://doi.org/10.1080/1057610X.2016.1157408>
- Conway, M., & McInerney, L. (2008). Jihadi video & auto-radicalisation: evidence from an exploratory YouTube study. 5376, 108-118. In D. Ortiz-Arroyo, H. L. Larsen, D. D. Zeng, D. Hicks, & G. Wagner (Eds), *Intelligence and security informatics*. (pp. 108-118). Springer.
https://doi.org/10.1007/978-3-540-89900-6_13
- Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2019). Disrupting Daesh: Measuring takedown of online terrorist material and its impact. *Studies in Conflict & Terrorism*, 42(1-2), 141-160. <https://doi.org/10.1080/1057610X.2018.1513984>
- Cook, A. N. (2014). *Risk assessment and management of group-based violence* (Doctoral dissertation, Simon Fraser University).
http://summit.sfu.ca/system/files/iritems1/14289/etd8437_ACook.pdf
- Cook, J., & Vale, G. (2018). *From daesh to 'diaspora': Tracing the women and minors of Islamic State*. The International Centre for the Study of Radicalisation. https://icsr.info/wp-content/uploads/2018/07/Women-in-ISIS-report_20180719_web.pdf
- Corera, G. (2008, January 16). The world's most wanted cyber-jihadist. *BBC News*. <http://news.bbc.co.uk/2/hi/americas/7191248.stm>

- Costello, M., Barrett-Fox, R., Bernatzky, C., Hawdon, J., & Mendes, K. (2018). Predictors of viewing online extremism among America's youth. *Youth & Society*, 52(5), 710-727. <https://doi.org/10.1177/0044118X18768115>
- Costello, N. (2016, May 21). War on Isis: Western fighters joining Kurds to fight terror group in Iraq and Syria. *Independent*.
<http://www.independent.co.uk/news/world/middle-east/western-fighters-joining-the-kurds-to-fight-isis-in-iraq-and-syria-a7041136.html>
- Cragin, R. K. (2014). Resisting violent extremism: A conceptual model for non-radicalization. *Terrorism and Political Violence*, 26(2), 337-353.
<https://doi.org/10.1080/09546553.2012.714820>
- Crosset, V., Tanner, S., & Campana, A. (2018). Researching far right groups on Twitter: Methodological challenges 2.0. *New Media & Society*, 1–23.
<https://doi.org/10.1177%2F1461444818817306>
- Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science*, 9(3), 458-467.
<https://doi.org/10.1287/mnsc.9.3.458>
- Dauber, C. E., & Winkler, C. K. (2014). Radical visual propaganda in the online environment: An introduction. In C. K. Winkler, & C. E. Dauber (Eds.), *Visual propaganda and extremism in the online environment* (pp.1-30). The US Army war college.
<https://www.hsdl.org/?view&did=756464>
- Davis, P. K., Perry, W. L., Brown, R. A., Yeung, D., Roshan, P., & Voorhies, P. (2013). *Using behavioral indicators to help detect potential violent acts: A review of the science base*. RAND Corporation.
- Dawson, L. L., Amarasingam, A., & Bain, A. (2016). *Talking to foreign fighters: Socio-economic push versus existential pull factors* (Working paper series, no.16-14). TSAS Canadian network for research on terrorism, security and society. <https://www.tsas.ca/publications/talking-to-foreign-fighters/>
- de Bie, J. L., de Poot, C. J., & van der Leun, J. P. (2015). Shifting modus operandi of Jihadist foreign fighters from the Netherlands between 2000 and 2013: A crime script analysis. *Terrorism and Political Violence*, 27(3), 416-440. <https://doi.org/10.1080/09546553.2015.1021038>

- de Ruiter, C., & Nicholls, T. (2011). Protective factors in forensic mental health: A new frontier. *The International Journal of Forensic Mental Health*, 10, 160–170. <http://dx.doi.org/10.1080/14999013.2011.600602>
- Dean, G. (2014). *Neurocognitive risk assessment for the early detection of violent extremists*. Springer.
- Dernevik, M., Beck, A., Grann, M., Hogue, T., & McGuire, J. (2009). The use of psychiatric and psychological evidence in the assessment of terrorist offenders. *The Journal of Forensic Psychiatry & Psychology*, 20(4), 508-525. <https://doi.org/10.1080/13501760902771217>
- Desmarais, S. L., Simons-Rudolph, J., Brugh, C. S., Schilling, E., & Hoggan, C. (2017). The state of scientific knowledge regarding factors associated with terrorism. *Journal of Threat Assessment and Management*, 4(4), 180-209. <https://doi.org/10.1037/tam0000090>
- Dillon, L. (2016). *Cyberterrorism: Using the internet as a weapon of destruction*. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 426-451). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch021>
- Dillon, L., Neo, L. S., & Freilich, J. D. (2019). A comparison of ISIS foreign fighters and supporters social media posts: An exploratory mixed-method content analysis. *Behavioral Sciences of Terrorism and Political Aggression*, 1-24. <https://doi.org/10.1080/19434472.2019.1690544>
- Dillon, L., Neo, L. S., & Khader, M. (2017). The psychology of violent extremism: what we know and what else we need to do. In H. C. Chan, & S. M. Y. Ho (Eds.), *Psycho-criminological perspective of criminal justice in Asia: Research and practices in Hong Kong, Singapore, and beyond* (pp. 252-273). Routledge Academic.
- Donnelly, M. G., Sanderson, T. M., & Fellman, Z. (2017). Foreign fighters in history. *Center for Strategic International Studies*, 5. <https://www.csis.org/analysis/foreign-fighters-history>
- Doosje, B., Loseman, A., & van Den Bos, K. (2013). Determinants of radicalization of Islamic youth in the Netherlands: Personal uncertainty, perceived injustice, and perceived group threat. *Journal of Social Issues*, 69(3), 586-604. <https://doi.org/10.1111/josi.12030>

- Downs, D. M., & Cowan, G. (2012). Predicting the importance of freedom of speech and the perceived harm of hate speech. *Journal of Applied Social Psychology*, 42(6), 1353-1375. <https://doi.org/10.1111/j.1559-1816.2012.00902.x>
- Droogan, J., Waldek, L., & Blackhall, R. (2018). Innovation and terror: An analysis of the use of social media by terror-related groups in the Asia Pacific. *The Journal of Policing, Intelligence and Counter Terrorism*, 13(2), 170-184. <https://doi.org/10.1080/18335330.2018.1476773>
- Ducol, B. (2012). Uncovering the French-speaking jihadisphere: An exploratory analysis. *Media, War & Conflict*, 5(1), 51-70. <https://doi.org/10.1177%2F1750635211434366>
- Duncan, N. B. (1995). Capturing flexibility of information technology infrastructure: A study of resource characteristics and their measure. *Journal of Management Information systems*, 12(2), 37-57. <https://doi.org/10.1080/07421222.1995.11518080>
- Edwards, C., & Gribbon, L. (2013). Pathways to violent extremism in the digital era. *The RUSI Journal*, 158(5), 40-47. <https://doi.org/10.1080/03071847.2013.847714>
- Egan, V., Cole, J., Cole, B., Alison, L., Alison, E., Waring, S., & Elntib, S. (2016). Can you identify violent extremists using a screening checklist and open-source intelligence alone? *Journal of Threat Assessment and Management*, 3(1), 21-36. <http://dx.doi.org/10.1037/tam0000058>
- el-Said, H., & Barrett, R. (2017). *Enhancing the understanding of the foreign terrorist fighters phenomenon in Syria*. United Nations Office of Counter-Terrorism.
- Erikha, F., Putra, I. E., & Sarwono, S. W. (2016). ISIS discourse in radical Islamic online news media in Indonesia: Supporter or opponent. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 70-90). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch004>
- Field, A. (2005). *Discovering statistics using SPSS* (2nd ed.). Sage.
- Foucault, M. (2008). *Psychiatric power: Lectures at the college de France, 1973--1974*. Macmillan.

- Franklin, K. K., & Hart, J. K. (2007). Idea generation and exploration: Benefits and limitations of the policy Delphi research method. *Innovative Higher Education*, 31(4), 237-246. <https://doi.org/10.1007/s10755-006-9022-8>
- Freeman, L., Schroeder, R., & Everton, S. F. (2017). Social media exploitation by covert networks: A case study of ISIS. *Communications of the Association for Information Systems*, 41(1), 97-120. <https://doi.org/10.17705/1CAIS.04105>
- Fritz, J., & Young, J. K. (2020). Transnational volunteers: American foreign fighters combating the Islamic state. *Terrorism and Political Violence*, 32(3), 449-468. <https://doi.org/10.1080/09546553.2017.1377075>
- Gan, R., Neo, L. S., Chin, J., & Khader, M. (2019). Change is the Only Constant: The Evolving Role of Women in the Islamic State in Iraq and Syria (ISIS). *Women & Criminal Justice*, 29(4-5), 204-220. <https://doi.org/10.1080/08974454.2018.1547674>
- Geeraerts, S. (2012). Digital radicalisation of youth. *Social Cosmos*, 3(1), 25-32. <https://dspace.library.uu.nl/handle/1874/237584>
- General Intelligence and Security Service [AIVD]. (2012). *Jihadism on the web: A breeding ground for jihad in the modern age*. Algemene Inlichtingen en Veiligheidsdienst. https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2012/02/14/het-jihadistisch-internet-kraamkamer-van-de-hedendaagse-jihad/Jihadism+on+the+web+EN+20120214.pdf
- Ghajar-Khosravi, S., Kwantes, P., Derbentseva, N., & Huey, L. (2016). Quantifying salient concepts discussed in social media content: A case study using Twitter content written by radicalized youth. *Journal of Terrorism Research*, 7(2), 79–90. <https://doi.org/10.15664/jtr.1241>
- Giannasi, P. (2015). Policing and hate crime. In N. Hall, A. Corb, P. Giannasi, & J. Grieve (Eds.), *The Routledge international handbook on hate crime* (pp. 331-342). Routledge.
- Gill, P. (2015a). *Lone-actor terrorists: A behavioural analysis*. Routledge.

- Gill, P. (2015b). Toward a scientific approach to identifying and understanding indicators of radicalization and terrorist intent: Eight key problems. *Journal of Threat Assessment and Management*, 2(3-4), 187-191. <https://psycnet.apa.org/doi/10.1037/tam0000047>
- Gill, P., & Corner, E. (2015). Lone-actor terrorist use of the Internet and behavioural correlates. In L. Jarvis, S. Macdonald, & T. M. Chen (Eds.), *Terrorism online: Politics, law, technology* (pp. 35-53). Routledge.
- Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers. *Criminology & Public Policy*, 16(1), 99-117. <https://doi.org/10.1111/1745-9133.12249>
- Golbeck, J., Robles, C., & Turner, K. (2011). Predicting personality with social media. In *CHI'11 extended abstracts on human factors in computing systems* (pp. 253-262). <https://doi.org/10.1145/1979742.1979614>
- Goodwill, A., & Meloy, J. R. (2019). Visualizing the relationship among indicators for lone actor terrorist attacks: Multidimensional scaling and the TRAP-18. *Behavioral sciences & the law*, 37(5), 522-539. <https://doi.org/10.1002/bsl.2434>
- Gosling, S., Augustine, A.A., Vazire, S., Holtzman, N., & Gaddis, S. (2011). Manifestations of personality in online social networks: Self-reported Facebook-related behaviors and observable profile information. *Cyberpsychology, Behavior, and Social Networking*, 14(9), 483-488. <https://doi.org/10.1089/cyber.2010.0087>
- Green, R. A. (2014). The Delphi technique in educational research. *Sage Open*, 4(2). <https://doi.org/10.1177/2158244014529773>
- Gruenewald, J., Chermak, S., & Freilich, J. D. (2013). Distinguishing “loner” attacks from other domestic extremist violence: A comparison of far-right homicide incident and offender characteristics. *Criminology & Public Policy*, 12(1), 65-91. <https://doi.org/10.1111/1745-9133.12008>
- Gstrein, O. J., Bunnik, A., & Zwitter, A. (2019). Ethical, legal and social challenges of predictive policing. *Católica Law Review, Direito Penal*, 3(N3), 77-98. <https://ssrn.com/abstract=3447158>

- Gupta, D. K. (2011). Waves of international terrorism: An exploration of the process by which ideas flood the world. In J. E. Rosenfeld (Ed.), *Terrorism, identity and legitimacy: The four waves theory and political violence* (pp. 30-43). Routledge.
- Gustafson, D. H., Shukla, R. K., Delbecq, A., & Walster, G. W. (1973). A comparative study of differences in subjective likelihood estimates made by individuals, interacting groups, Delphi groups, and nominal groups. *Organizational Behavior and Human Performance*, 9(2), 280-291.
[https://doi.org/10.1016/0030-5073\(73\)90052-4](https://doi.org/10.1016/0030-5073(73)90052-4)
- Halverson, J. R., & Way, A. K. (2012). The curious case of Colleen LaRose: Social margins, new media, and online radicalization. *Media, War & Conflict*, 5(2), 139-153. <https://doi.org/10.1177/1750635212440917>
- Hassan, G., Brouillette-Alarie, S., Alava, S., Frau-Meigs, D., Lavoie, L., Fetiu, A., ... & Sieckelinck, S. (2018). Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence. *International journal of developmental science*, 12(1-2), 71-88.
<http://dx.doi.org/10.3233/DEV170233>
- Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4), 1008-1015. <https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x>
- Hegghammer, T. (2013). Should I stay or should I go? Explaining variation in western jihadists' choice between domestic and foreign fighting. *The American Political Science Review*, 107(1), 1-15.
<https://doi.org/10.1017/S0003055412000615>
- Hegghammer, T. (2014). Interpersonal trust on Jihadi internet forums. *Norwegian Defence Research Establishment*, 5, 1-43.
<https://pdfs.semanticscholar.org/82aa/d0a0dde965274e03944bf318b4852dafab24.pdf>
- Hettiarachchi, M. (2018). Rehabilitation to deradicalise detainees and inmates: a counter-terrorism strategy. *Journal of Policing, Intelligence and Counter Terrorism*, 13(2), 267-283.
<https://doi.org/10.1080/18335330.2018.1476774>

- Hirschhorn, F. (2019). Reflections on the application of the Delphi method: Lessons from a case in public transport research. *International Journal of Social Research Methodology*, 22(3), 309-322.
<https://doi.org/10.1080/13645579.2018.1543841>
- Holbrook, D., & Horgan, J. (2019). Terrorism and ideology: Cracking the nut. *Perspectives on Terrorism*, 13(6), 2-15.
<https://www.jstor.org/stable/26853737>
- Holden, M. (2007, November 6). Experts say West can't stop web radicalisation. *Reuters*. <http://uk.reuters.com/article/2007/11/06/uk-britain-security-Internet-idUKL2658640020071106>
- Holman, T. (2016). 'Gonna get myself connected' The role of facilitation in foreign fighter mobilizations. *Perspectives on Terrorism*, 10(2), 2-23.
<https://www.jstor.org/stable/26297549>
- Holmer, G., & Shtuni, A. (2017). *Returning foreign fighters and the reintegration imperative*. United States Institute of Peace.
https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/USIP_sr402-returning-foreign-fighters-and-the-reintegration-imperative.pdf
- Horgan, J. (2005). *The psychology of terrorism*. Routledge.
- Horgan, J. (2019). Psychological approaches to the study of terrorism. In E. Chenoweth, R. English, A. Gofas, & S. N. Kalyvas (Eds.), *The Oxford handbook of terrorism* (pp. 207-223). Oxford University Press.
- Horgan, J., Altier, M. B., Shortland, N., & Taylor, M. (2017). Walking away: the disengagement and de-radicalization of a violent right-wing extremist. *Behavioral Sciences of Terrorism and Political Aggression*, 9(2), 63-77. <https://doi.org/10.1080/19434472.2016.1156722>
- Horgan, J., Shortland, N., & Abbasciano, S. (2018). Towards a typology of terrorism involvement: A behavioral differentiation of violent extremist offenders. *Journal of Threat Assessment and Management*, 5(2), 84-102.
<https://doi.org/10.1037/tam0000102>

- Hu, W. (2016). Psychological effects of the threat of ISIS: A preliminary inquiry of Singapore case studies. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 168-173). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch009>
- Hussain, G., & Saltman, E. M. (2014). *Jihad trending: a comprehensive analysis of online extremism and how to counter it*. Quilliam Foundation. <https://preventviolentextremism.info/jihad-trending-comprehensive-analysis-online-extremism-and-how-counter-it>
- Hussain, S. (2018). Exploring people's perceptions of precursors to the development of radicalisation and extremism. *Journal for Deradicalization*, 14, 79-110. <https://journals.sfu.ca/jd/index.php/jd/article/view/136/110>
- Hutchinson, S., & O'malley, P. (2007). A crime–terror nexus? Thinking on some of the links between terrorism and criminality. *Studies in Conflict Terrorism*, 30(12), 1095-1107. <https://doi.org/10.1080/10576100701670870>
- Innes, M., Abbott, L., Lowe, T., & Roberts, C. (2007). *Hearts and minds and eyes and ears: reducing radicalisation risks through reassurance-oriented policing*. Cardiff University: Universities' Police Science Institute. <http://www.upsi.org.uk/storage/publications/HeartsMinds>
- Institute for Policy Analysis of Conflict [IPAC]. (2019, April 29). *The ongoing problem of pro-ISIS cells in Indonesia*. <http://www.understandingconflict.org/en/conflict/read/81/The-Ongoing-Problem-of-Pro-ISIS-Cells-in-Indonesia>
- ISD Research Command. (2018). Empowering the community against terrorism: evolution of the terrorism threat to Singapore. *Home Team Journal*, 7, 70-74. <https://www.mha.gov.sg/docs/default-source/publications/hta-journal-hr-issue-no-7.pdf>
- Jackson, B., Baker, J., Cragin, K., Parachini, J., Trujillo, H., & Chalk, P. (2005). *Aptitude for destruction, volume 1. Organizational learning in terrorist groups and its implications for combating terrorism*. RAND Corporation. <https://www.rand.org/pubs/monographs/MG331.html>

- Jayakumar, S. (2016). The curious case of Wang Yuandongyi: Why do some want to fight with anti-ISIS groups? *RSIS Commentaries (074/2016)*. S. Rajaratnam School of International Studies. <https://www.rsis.edu.sg/wp-content/uploads/2016/04/CO16074.pdf>
- Jayakumar, S. (2019). *Transnational volunteers against ISIS*. International Centre for the Study of Radicalisation. <https://icsr.info/wp-content/uploads/2019/08/ICSR-Report-Transnational-Volunteers-Against-ISIS.pdf>
- Jerard, J. (2017, June 3). Commentary: Are lone wolves or regional terrorist networks more dangerous to Singapore? *Channel News Asia*. <https://www.channelnewsasia.com/news/singapore/commentary-are-lone-wolves-or-regional-terrorist-networks-more-8907484>.
- Johansson, F., Kaati, L., & Sahlgren, M. (2016). Detecting linguistic markers of violent extremism in online environments. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 374-390). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch018>
- Johnson, H. (2015, September 17). Kurdish fighters: We'd really appreciate if you came to Syria to help fight ISIS. *Foreign Policy*. <http://foreignpolicy.com/2015/09/17/kurdish-fighters-wed-really-appreciate-if-you-came-to-syria-to-help-fight-isis/>
- Jones, S. G., Toucas, B., & Markusen, M. B. (2018). *From the IRA to the Islamic State: The evolving terrorism threat in Europe*. Center for Strategic & International Studies. <https://www.csis.org/analysis/ira-islamic-state-evolving-terrorism-threat-europe>
- Jore, S. H., & Njå, O. (2010). Risk of terrorism: A scientifically valid phenomenon or a wild guess? The impact of different approaches to risk assessment. *Critical Approaches to Discourse Analysis across Disciplines*, 4(2), 197-216. https://www.lancaster.ac.uk/fass/journals/cadaad/wp-content/uploads/2015/01/Volume-4_Jore-Njaa.pdf

- Kalpakis, G., Tsikrika, T., Gialampoukidis, I., Papadopoulos, S., Vrochidis, S., & Kompatsiaris, I. (2018). Analysis of suspended terrorism-related content on social media. In G. Leventakis, & M. R. Haberfeld (Eds.), *Community-oriented policing and technological innovations* (pp. 107-118). Springer.
- Kebbell, M. R., & Porter, L. (2012). An intelligence assessment framework for identifying individuals at risk of committing acts of violent extremism against the West. *Security Journal*, 25(3), 212-228.
<https://doi.org/10.1057/sj.2011.19>
- Keil, M., Tiwana, A., & Bush, A. (2002). Reconciling user and project manager perceptions of IT project risk: a Delphi study 1. *Information Systems Journal*, 12(2), 103-119. <https://doi.org/10.1046/j.1365-2575.2002.00121.x>
- Kern, M. L., Eichstaedt, J. C., Schwartz, H. A., Dziurzynski, L., Ungar, L. H., Stillwell, D. J., ... & Seligman, M. E. (2014). The online social self: An open vocabulary approach to personality. *Assessment*, 21(2), 158-169.
<https://doi.org/10.1177%2F1073191113514104>
- Khader, M. (2016). What we know and what else we need to do to address the problem of violent extremism online: Concluding chapter. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 486-495). IGI Global.
<https://doi.org/10.4018/978-1-5225-0156-5.ch024>
- Khader, M., Neo, L. S., Tan, J., Cheong, D. D., & Chin, J. (2019). Learning from violent extremist attacks: An introduction. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. xxxiii-lxii). World Scientific.
https://doi.org/10.1142/9789813275447_others01
- Kimmage, D., & Rudolfo, K. (2007). *Iraqi insurgent media: The war of images and ideas*. Radio Free Europe/Radio Liberty.
<https://docs.rferl.org/archive/online/OLPDFfiles/insurgent.pdf>

- King, M., & Taylor, D. M. (2011). The radicalization of homegrown jihadists: A review of theoretical models and social psychological evidence. *Terrorism and political violence*, 23(4), 602-622.
<https://doi.org/10.1080/09546553.2011.587064>
- Kinnear, P. R., & Gray, C. D. (2006). *SPSS 14 made simple*. Psychology Press.
- Kipane, A. (2019, November 25). Meaning of profiling of cybercriminals in the security context. https://www.shs-conferences.org/articles/shsconf/abs/2019/09/shsconf_shw2019_01009/shsconf_shw2019_01009.html
- Klausen, J. (2015). Tweeting the jihad: Social media networks of western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, 38(1), 1-22. <https://doi.org/10.1080/1057610X.2014.974948>
- Klausen, J., Barbieri, E. T., Reichlin-Melnick, A., & Zelin, A. Y. (2012). The YouTube jihadists: A social network analysis of Al-Muhajiroun's propaganda campaign. *Perspectives on Terrorism*, 6(1), 36-53.
<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/klausen-et-al-youtube-jihadists/html>
- Klausen, J., Champion, S., Needle, N., Nguyen, G., & Libretti, R. (2016). Toward a behavioral model of "homegrown" radicalization trajectories. *Studies in Conflict & Terrorism*, 39(1), 67-83.
<https://doi.org/10.1080/1057610X.2015.1099995>
- Knight, S., Keatley, D., & Woodward, K. (2019). Comparing the different behavioral outcomes of extremism: A comparison of violent and non-violent extremists, acting alone or as part of a group. *Studies in Conflict & Terrorism*, 1-22. <https://doi.org/10.1080/1057610X.2019.1680192>
- Koçak, M. (2012). Threat assessment of terrorist organizations: the application of Q methodology. *Journal of Risk Research*, 15(1), 85-105.
<https://doi.org/10.1080/13669877.2011.601323>
- Koch, A. (2019). The non-jihadi foreign fighters: Western right-wing and left-wing extremists in Syria. *Terrorism and Political Violence*, 1-28.
<https://doi.org/10.1080/09546553.2019.1581614>
- Koehler, D. (2014). The radical online: Individual radicalization processes and the role of the Internet. *Journal for Deradicalization*, 1, 116-134.
<https://journals.sfu.ca/jd/index.php/jd/article/view/8>

- Koo, T. K., & Li, M. Y. (2016). A guideline of selecting and reporting intraclass correlation coefficients for reliability research. *Journal of Chiropractic Medicine*, 15(2), 155-163.
<https://doi.org/10.1016/j.jcm.2016.02.012>
- Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States*, 110(15), 5802-5805. <https://doi.org/10.1073/pnas.1218772110>
- Kruglanski, A. W. (2014, October 28). Psychology not theology: Overcoming ISIS' secret appeal. *E-International Relations*. <http://www.e-ir.info/2014/10/28/psychology-not-theology-overcoming-isis-secret-appeal/>
- Kruglanski, A. W., Bélanger, J. J., & Gunaratna, R. (2019). *The three pillars of radicalization: Needs, narratives, and networks*. Oxford University Press.
- Kruglanski, A. W., Jasko, K., Chernikova, M., Dugas, M., & Webber, D. (2017). To the fringe and back: Violent extremism and the psychology of deviance. *American Psychologist*, 72(3), 217–230. <https://doi.org/10.1037/amp0000091>
- Kruglanski, A. W., Jasko, K., Webber, D., Chernikova, M., & Molinaro, E. (2018). The making of violent extremists. *Review of General Psychology*, 22(1), 107-120. <https://doi.org/10.1037/gpr0000144>
- Kruglanski, A. W., Pierro, A., Mannetti, L., & De Grada, E. (2006). Groups as epistemic providers: Need for closure and the unfolding of group-centrism. *Psychological review*, 113(1), 84-100.
<https://psycnet.apa.org/doi/10.1037/0033-295X.113.1.84>
- Kruskal, J. B. (1964). Multidimensional scaling by optimizing goodness of fit to a nonmetric hypothesis. *Psychometrika*, 29(1), 1-27.
<https://doi.org/10.1007/BF02289565>
- LaFree, G., & Dugan, L. (2009). Research on terrorism and countering terrorism. *Crime and Justice*, 38(1), 413-477.
<https://doi.org/10.1080/17539153.2019.1579777>
- Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33, 159-174.
<https://www.jstor.org/stable/2529310>

- Lara-Cabrera, R., Pardo, A. G., Benouaret, K., Faci, N., Benslimane, D., & Camacho, D. (2017). Measuring the radicalisation risk in social networks. *IEEE Access*, 5, 10892-10900.
<https://doi.org/10.1109/ACCESS.2017.2706018>
- Lee, E., & Leets, L. (2002). Persuasive storytelling by hate groups online: Examining its effects on adolescents. *American Behavioral Scientist*, 45(6), 927-957. <https://doi.org/10.1177/0002764202045006003>
- Lee, L. Y. (2018, January 27). Previous ISIS terror plots on Singapore ‘will not be the last’: President Halimah. *Channel News Asia*.
<https://www.channelnewsasia.com/news/singapore/isis-terror-plots-singapore-will-not-be-the-last-halimah-9902040>
- Lemieux, A. F., Brachman, J. M., Levitt, J., & Wood, J. (2014). Inspire magazine: A critical analysis of its significance and potential impact through the lens of the information, motivation, and behavioral skills model. *Terrorism and Political Violence*, 26(2), 354-371.
<https://doi.org/10.1080/09546553.2013.828604>
- Leuprecht, C., Hataley, T., Moskalenko, S., & McCauley, C. (2010). Narratives and counter-narratives for global jihad: Opinion versus action. In E. J. A. M. Kessels (Ed.), *Countering violent extremist narratives* (pp. 58-71). National Coordinator for Counterterrorism.
- Levine, M., Prosser, A., Evans, D., & Reicher, S. (2005). Identity and emergency intervention: How social group membership and inclusiveness of group boundaries shape helping behavior. *Personality and social psychology bulletin*, 31(4), 443-453.
<https://doi.org/10.1177/0146167204271651>
- Li, L., Li, A., Hao, B., Guan, Z., & Zhu, T. (2014). Predicting active users’ personality based on micro-blogging behaviors. *PloS one*, 9(1).
<https://doi.org/10.1371/journal.pone.0084997>
- Lim, S. (2016). The contested ethics of mainstream reporting of terrorism in the social media age. *Auckland UL Rev.*, 22, 249.
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/auck22&div=12&id=&page=>

- Linstone, H. A., & Turoff, M. (2002). Introduction. In M. Turoff, & H. A. Linstone (Eds.), *The Delphi method: Techniques and applications* (pp. 3-12). Addison-Wesley.
- Lloyd, M. (2019). *Extremism risk assessment: A directory*. The Centre for Research and Evidence on Security Threats (CREST).
<https://crestresearch.ac.uk/resources/extremism-risk-assessment-directory/>
- Lloyd, M., & Dean, C. (2015). The development of structured guidelines for assessing risk in extremist offenders. *Journal of Threat Assessment and Management*, 2(1), 40-52. <https://doi.org/10.1037/tam0000035>
- Loadenthal, M. (2019). Othering terrorism: A rhetorical strategy of strategic labeling. *Genocide Studies and Prevention: An International Journal*, 13(2), 9. <https://scholarcommons.usf.edu/gsp/vol13/iss2/9/>
- Loh, D. (2017, September 13). Individuals in Singapore being radicalised at faster pace: Shanmugam. *Channel News Asia*.
<https://www.channelnewsasia.com/news/singapore/individuals-in-singapore-being-radicalised-at-faster-pace-9213840>
- Loke, K. F. (2017). Anti-terror efforts to continue as threats remain at ‘a high level’: Shanmugam. *Channel NewsAsia*. <https://www.channelnewsasia.com/news/singapore/anti-terror-efforts-to-continue-as-threats-remain-at-a-high-9504264>.
- Long, J. S. (1997). *Regression models for categorical and limited dependent variables*. Sage.
- Lucas, K., & Aly, A. (2015). *Counter narratives to interrupt online radicalisation*. A report on the CNOIR project presented to the Department of Attorney General. Countering online Violent Extremism Research Program, Curtin University.
- Macnair, L., & Frank, R. (2017). “To My Brothers in the West...”: A thematic analysis of videos produced by the Islamic State’s al-Hayat Media Center. *Journal of Contemporary Criminal Justice*, 33(3), 234-253.
<https://doi.org/10.1177/1043986217699313>
- Mahood, S., & Rane, H. (2017). Islamist narratives in ISIS recruitment propaganda. *The Journal of International Communication*, 23(1), 15-35.
<https://doi.org/10.1080/13216597.2016.1263231>

- Mair, D. (2017). # Westgate: A case study: How al-Shabaab used Twitter during an ongoing attack. *Studies in Conflict & Terrorism*, 40(1), 24-43. <https://doi.org/10.1080/1057610X.2016.1157404>
- Malet, D. (2013). *Foreign fighters: Transnational identity in civil conflicts*. Oxford University Press.
- Mans, K., & Tuitel, R. (2016). *Foreign fighters in their own words: Using YouTube as a source*. International Centre for Counter-Terrorism – The Hague. <https://icct.nl/publication/foreign-fighters-in-their-own-words-using-youtube-as-a-source/>
- Mascini, P. (2006). Can the violent jihad do without sympathizers?. *Studies in Conflict & Terrorism*, 29(4), 343-357. <https://doi.org/10.1080/10576100600641832>
- Matsumoto, D., Frank, M. G., & Hwang, H. C. (2015). The role of intergroup emotions in political violence. *Current Directions in Psychological Science*, 24(5), 369-373. <https://doi.org/10.1177/0963721415595023>
- McCauley, C., & Moskalenko, S. (2008). Mechanisms of political radicalization: Pathways toward terrorism. *Terrorism and political violence*, 20(3), 415-433. <https://doi.org/10.1080/09546550802073367>
- McCauley, C., & Moskalenko, S. (2011). *Friction: How radicalization happens to them and us*. Oxford University Press.
- McClelland, D. C. (1987). *Human motivation*. Cambridge University Press.
- McHugh, M. L. (2012). Interrater reliability: The kappa statistic. *Biochemia medica: Biochemia medica*, 22(3), 276-282. <https://hrcak.srce.hr/89395>
- Meleagrou-Hitchens, A., & Kaderbhai, N. (2017). *Research perspectives on online radicalisation: A literature review, 2006-2016*. International Centre for the Study of Radicalisation. https://icsr.info/wp-content/uploads/2017/05/ICSR-Paper_Research-Perspectives-on-Online-Radicalisation-A-Literature-Review-2006-2016.pdf
- Meloy, J. R. & Gill, P. (2016). The lone-actor terrorist and the TRAP-18. *Journal of Threat Assessment and Management*, 3(1), 37–52. <https://doi.org/10.1037/tam0000061>
- Meloy, J. R., & O'Toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences & the Law*, 29(4), 513–527. <https://doi.org/10.1002/bsl.986>

- Meloy, J. R., Hoffmann, J., Guldemann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30(3), 256-279.
<https://doi.org/10.1002/bsl.999>
- Meloy, J. R., Roshdi, K., Glaz-Ocik, J., & Hoffmann, J. (2015). Investigating the individual terrorist in Europe. *Journal of Threat Assessment and Management*, 2(3-4), 140-152. <https://doi.org/10.1037/tam0000036>
- Meloy, J. R., Sheridan, L., & Hoffmann, J. (2008). *Stalking, threatening, and attacking public figures: A psychological and behavioral analysis*. Oxford University Press.
- Menn, J., & Volz, D. (2016, June 25). Exclusive: Google, Facebook quietly move toward automatic blocking of extremist videos. *Reuters*.
<http://mobile.reuters.com/article/idUSKCN0ZB00M>,
- Milla, M. N., & Umam, A. N. (2019). Understanding intergroup contact on terrorist prisoners in Indonesia. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 259-278). World Scientific. https://doi.org/10.1142/9789813275447_0013
- Ministry of Home Affairs [MHA]. (2019, January 22). *Singapore Terrorism Threat Assessment Report 2019*.
<https://www.mha.gov.sg/newsroom/press-release/news/singapore-terrorism-threat-assessment-report-2019>
- Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. *American Psychologist*, 60(2), 161-169.
<https://psycnet.apa.org/doi/10.1037/0003-066X.60.2.161>
- Monahan, J. (2012). The individual risk assessment of terrorism. *Psychology, Public Policy, and Law*, 18(2), 167-205.
<https://doi.org/10.1037/a0025792>
- Moore, C. (2015). Moral disengagement. *Current Opinion in Psychology*, 6, 199-204. <https://doi.org/10.1016/j.copsyc.2015.07.018>
- Morin, R. (2016, January 29). The Western volunteers fighting ISIS. *The Atlantic*.
<http://www.theatlantic.com/international/archive/2016/01/peshmerga-isis-western-volunteers/433803/>

- Mukhtar, A. (2016). Tactics of recruitment. In A. Mukhtar (Ed.), *Terrorist threat in the Euro-Mediterranean region* (pp. 23-42). European Institute of the Mediterranean. <https://www.iemed.org/publicacions-en/historic-de-publicacions/joint-policy-studies/terrorist-threat-in-the-euro-mediterranean-region>
- Muluk, H., Umam, A. N., & Milla, M. N. (2020). Insights from a deradicalization program in Indonesian prisons: The potential benefits of psychological intervention prior to ideological discussion. *Asian Journal of Social Psychology*, 23(1), 42-53. <https://doi.org/10.1111/ajsp.12392>
- Nambisan, S., Agarwal, R., & Tanniru, M. (1999). Organizational mechanisms for enhancing user innovation in information technology. *MIS Quarterly*, 23(3), 365-395. <https://www.jstor.org/stable/249468>
- National Counter Terrorism Center [NCTC]. (2011). *Behavioral indicators offer insights for spotting extremists mobilizing for violence*. <https://info.publicintelligence.net/NCTC-SpottingHVEs.pdf>
- Nave, G., Minxha, J., Greenberg, D. M., Kosinski, M., Stillwell, D., & Rentfrow, J. (2018). Musical preferences predict personality: Evidence from active listening and facebook likes. *Psychological science*, 29(7), 1145-1158. <https://doi.org/10.1177/0956797618761659>
- Neo, L. S. (2016). An internet-mediated pathway for online radicalisation: RECRO. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 197-224). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch01>
- Neo, L. S. (2019). Singapore's Total Defence: Overcoming complacency. *RSIS Commentaries (062/2019)*. S. Rajaratnam School of International Studies. <https://www.rsis.edu.sg/rsis-publication/nssp/singapores-total-defence-overcoming-complacency/>
- Neo, L. S. (2020). Leveraging on digital footprints to identify potential security threats: Insights from the behavioural sciences perspective. In M. Khosrow-Pour (Ed.), *Encyclopaedia of criminal activities and the deep web* (pp. 1003-1017). IGI Global. <https://doi.org/10.4018/978-1-5225-9715-5.ch068>

- Neo, L. S., Dillon, L., & Khader, M. (2017). Identifying individuals at risk of being radicalised via the internet. *Security Journal*, 30(4), 1112-1133. <https://doi.org/10.1057/s41284-016-0080-z>
- Neo, L. S., Khader, M., & Pang, J. S. (2018). Comparing ISIS foreign fighters versus sympathisers: Insights from their Twitter postings. *Home Team Journal*, 7, 87-106. <https://www.mha.gov.sg/docs/default-source/publications/hta-journal-hr-issue-no-7.pdf>
- Neo, L. S., Pang, J. S., & Chin, J. (2019). Bystander intervention to prevent radicalisation. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 175-197). World Scientific. https://doi.org/10.1142/9789813275447_0010
- Neo, L. S., Shi, P., Dillon, L., Tan, J., Wang, Y., & Gomes, D. (2016). Why is ISIS so psychologically attractive? In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 149-167). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch008>
- Neubronner, S. (2019). Managing social media in the event of a terror attack. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 377-396). World Scientific. https://doi.org/10.1142/9789813275447_0020
- Neumann, P. R. (2012). *Countering online radicalisation in America*. Bipartisan Policy Center. https://bipartisanpolicy.org/wp-content/uploads/2019/03/BPC-_Online-Radicalization-Report.pdf
- New York Port Authority attack: Akayed Ullah ‘inspired by IS’ (2017, December 12). *BBC News*. <http://www.bbc.com/news/world-us-canada-42320366>
- Newness, K., Steinert, J., & Viswesvaran, C. (2012). Effects of personality on social network disclosure: Do emotionally intelligent individuals post inappropriate content? *Psychological Topics*, 21(3), 473-486. <https://hrcak.srce.hr/95507>

- Noor, M., Shnabel, N., Halabi, S., & Nadler, A. (2012). When suffering begets suffering: The psychology of competitive victimhood between adversarial groups in violent conflicts. *Personality and Social Psychology Review*, 16(4), 351-374. <https://doi.org/10.1177/1088868312440048>
- Nuraniyah, N. (2018). Not just brainwashed: Understanding the radicalization of Indonesian female supporters of the Islamic State. *Terrorism and Political Violence*, 30(6), 890-910. <https://doi.org/10.1080/09546553.2018.1481269>
- O'Connor, B. P. (2000). SPSS and SAS programs for determining the number of components using parallel analysis and Velicer's MAP test. *Behavior research methods, instruments, & computers*, 32(3), 396-402. <https://doi.org/10.3758/BF03200807>
- O'Hara, K., & Stevens, D. (2015). Echo chambers and online radicalism: Assessing the Internet's complicity in violent extremism. *Policy & Internet*, 7(4), 401-422. <https://doi.org/10.1002/poi3.88>
- Orton, K. (2017). The forgotten foreign fighters: The PKK in Syria. *The Henry Jackson Society*. <http://henryjacksonsociety.org/wp-content/uploads/2017/08/3053-PYD-Foreign-Fighter-Project-1.pdf>
- Osman, S. (2010). Jemaah Islamiyah: of kin and kind. *Journal of Current Southeast Asian Affairs*, 29(2), 157-175. <https://doi.org/10.1177/186810341002900205>
- Ozdemir, V. E., & Hewett, K. (2010). The effect of collectivism on the importance of relationship quality and service quality for behavioral intentions: A cross-national and cross-contextual analysis. *Journal of International Marketing*, 18(1), 41-62. <https://www.jstor.org/stable/27755626>
- Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjällhed, A. (2018). Countering information influence activities: The state of the art. *Department of Strategic Communication, Lund University*. <https://www.msb.se/RibData/Filer/pdf/28698.pdf>

- Pang, J. S. (2016). Understanding personality and person-specific predictors of cyber-based insider threat. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 107-128). IGI Global. <https://10.4018/978-1-5225-0156-5.ch006>
- Patin, N. (2015, August 26). The other foreign fighters: An open-source investigation into American volunteers fighting the Islamic State. *Bellingcat*. <https://www.bellingcat.com/news/mena/2015/08/26/the-other-foreign-fighters>
- Pauwels, L., & Schils, N. (2016). Differential online exposure to extremist content and political violence: Testing the relative strength of social learning and competing perspectives. *Terrorism and Political Violence*, 28(1), 1-29. <https://doi.org/10.1080/09546553.2013.876414>
- Pearson, E. (2016). The case of roshonara choudhry: Implications for theory on online radicalization, ISIS women, and the gendered jihad. *Policy & Internet*, 8(1), 5-33. <https://doi.org/10.1002/poi3.101>
- Pearson, E. (2018). Online as the new frontline: Affect, gender, and ISIS-take-down on social media. *Studies in Conflict & Terrorism*, 41(11), 850-874. <https://doi.org/10.1080/1057610X.2017.1352280>
- Peng, C. Y. J., Lee, K. L., & Ingersoll, G. M. (2002). An introduction to logistic regression analysis and reporting. *The journal of educational research*, 96(1), 3-14. <https://doi.org/10.1080/00220670209598786>
- Post, J. M., Ruby, K. G., & Shaw, E. D. (2002). The radical group in context: 1. An integrated framework for the analysis of group risk for terrorism. *Studies in Conflict & Terrorism*, 25(2), 73-100. <https://doi.org/10.1080/105761002753502466>
- Powis, B., Randhawa, K., & Bishopp, D. (2019). An examination of the structural properties of the Extremism Risk Guidelines (ERG22+): A structured formulation tool for extremist offenders. *Terrorism and Political Violence*, 1-19. <https://doi.org/10.1080/09546553.2019.1598392>
- Pressman, D. E. (2009). *Risk assessment decisions for violent political extremism*. User Report 2009-02. Public Safety Canada. <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2009-02-rdv/index-en.aspx>

- Pressman, D. E., & Flockton, J. S. (2012). Calibrating risk for violent political extremists: The VERA-2 Structural Assessment. *The British Journal of Forensic Practise*, 14(4), 237-251.
<https://doi.org/10.1108/14636641211283057>
- Pressman, D. E., & Ivan, C. (2016). Internet use and violent extremism: A cyber-VERA risk assessment protocol. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 391-409). IGI Global. <https://10.4018/978-1-5225-0156-5.ch019>
- Prucha, N. (2016). IS and the Jihadist information highway—projecting influence and religious identity via telegram. *Perspectives on Terrorism*, 10(6), 48-58. <https://www.jstor.org/stable/26297705>
- Qiu, L., Lin, H., Ramsay, J., & Yang, F. (2012). You are what you tweet: Personality expression and perception on Twitter. *Journal of Research in Personality*, 46(6), 710-718. <https://doi.org/10.1016/j.jrp.2012.08.008>
- Quercia, D., Kosinski, M., Stillwell, D., & Crowcroft, J. (2011, October). Our Twitter profiles, our selves: Predicting personality with Twitter. In *2011 IEEE third international conference on privacy, security, risk and trust and 2011 IEEE third international conference on social computing* (pp. 180-185). IEEE. <https://doi.org/10.1109/PASSAT/SocialCom.2011.26>
- Radlauer, D. (2007). Virtual communities as pathways to extremism. In B. Ganor, K. V. Knop, & C. Duarte (Eds.), *Hypermedia seduction for terrorist recruiting* (pp. 67-75). IOS Press.
<http://ebooks.iospress.nl/volumearticle/24119>
- Ramakrishna, K. (2009). *Radical pathways: Understanding Muslim radicalization in Indonesia*. Praeger Security International.
- Ramakrishna, K. (2013). From virtual to violent: Preliminary conceptual explorations of religious radicalisation in youth. In Southeast Asia Regional Centre for Counter-Terrorism (Ed.), *Youth and Terrorism: A Selection of Articles* (pp. 1-14). Ministry of Foreign Affairs Malaysia.

- Ramakrishna, K. (2016). Towards a comprehensive approach to combating violent extremist ideology in the digital space: The counter-ideological response (CIR) model. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 260-282). IGI Global. <https://doi.org/10.4018/978-1-5225-0988-2.ch031>
- Ramalingam, V. (2012). *Far-right extremism: Trends and methods for response and prevention* (Policy Briefing). Institute for Strategic Dialogue. http://www.strategicdialogue.org/Policy_Briefing_-_Far_Right_Extremism_FINAL.pdf
- Reed, A., Pohl, J., & Jegerings, M. (2017). *The four dimensions of the Foreign Fighter threat: making sense of an evolving phenomenon*. ICCT Policy Brief. <https://icct.nl/publication/the-four-dimensions-of-the-foreign-fighter-threat-making-sense-of-an-evolving-phenomenon/>
- Reeve, Z. (2019). Engaging with online extremist material: Experimental evidence. *Terrorism and Political Violence*, 1-26. <https://doi.org/10.1080/09546553.2019.1634559>
- Reicher, S., Haslam, S. A., & Rath, R. (2008). Making a virtue of evil: A five-step social identity model of the development of collective hate. *Social and Personality Psychology Compass*, 2(3), 1313-1344. <https://doi.org/10.1111/j.1751-9004.2008.00113.x>
- Reynolds, S. C., & Hafez, M. M. (2019). Social network analysis of German foreign fighters in Syria and Iraq. *Terrorism and Political Violence*, 31(4), 661-686. <https://doi.org/10.1080/09546553.2016.1272456>
- Rieger, D., Frischich, L., & Bente, G. (2013). *Propaganda 2.0 Psychological effects of right-wing and Islamic extremist Internet videos*. German Federal Criminal Police Office.
- Roberson, Q. M., Collins, C. J., & Oreg, S. (2005). The effects of recruitment message specificity on applicant attraction to organizations. *Journal of Business and Psychology*, 19(3), 319-339. <https://doi.org/10.1007/s10869-004-2231-1>

- Robert, B. (2019). At-risk and radicalised Singaporean youths: Themes observed and considerations for a youth-centric rehabilitation framework. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 239-257). World Scientific. https://doi.org/10.1142/9789813275447_0013
- Rogan, H. (2007). *Al-Qaeda's online media strategies: From Abu Reuter to Irhabi 007*. Norwegian Defence Research Establishment (FFI). <https://publications.ffi.no/nb/item/asset/dspace:3401/07-02729.pdf>
- Rognstad, S., Brekke, M., Fetveit, A., Spigset, O., Wyller, T. B., & Straand, J. (2009). The Norwegian General Practice (NORGE) criteria for assessing potentially inappropriate prescriptions to elderly patients: a modified Delphi study. *Scandinavian Journal of Primary Health Care*, 27(3), 153-159. <https://doi.org/10.1080/02813430902992215>
- Romyn, D., & Kebbell, M. (2016). Using the internet to plan for terrorist attack. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Countering violent extremism and radicalisation in the digital era* (pp. 91-105). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch005>
- Rowe, M., & Saif, H. (2016, May). Mining Pro-ISIS radicalisation signals from social media users. *Proceedings of the Tenth International AAAI Conference on Web and Social Media*. Retrieved from <https://core.ac.uk/download/pdf/78075234.pdf>
- Sageman, M. (2004). *Understanding terror networks*. University of Pennsylvania Press.
- Sageman, M. (2008). *Leaderless jihad: Terror networks in the twenty-first century*. University of Pennsylvania Press.
- Saifudeen, O. A. (2014). *The cyber extremism orbital pathways model*. RSIS Working Paper 283. S. Rajaratnam School of International Studies. <https://dr.ntu.edu.sg/handle/10356/82410>
- Saifudeen, O. A. (2016). Getting out of the armchair: Potential tipping points for online radicalisation. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Countering violent extremism and radicalisation in the digital era* (pp. 129-148). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch007>

- Saifudeen, O. A. (2019). A common framework for pre-radicalisation indicators. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural sciences insights for practitioners and policymakers* (pp. 99-130). World Scientific. https://doi.org/10.1142/9789813275447_0006
- Saltman, E. M. (2016). Western female migrants to ISIS: Propaganda, radicalisation, and recruitment. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 174-196). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch010>
- Samuel, T. K. (2018). *Undergraduate radicalisation in selected countries in Southeast Asia: A Comparative quantitative analysis on the perception of terrorism and counter-terrorism among undergraduates in Indonesia, Malaysia, the Philippines, Singapore and Thailand*. Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT), Ministry of Foreign Affairs, Malaysia.
- Santtila, P., Junkkila, J., & Sandnabba, N. K. (2005). Behavioural linking of stranger rapes. *Journal of Investigative Psychology and Offender Profiling*, 2(2), 87-103. <https://doi.org/10.1002/jip.26>
- Sarma, M. K. (2017). Risk assessment and the prevention of radicalisation from nonviolence into terrorism. *American Psychologist*, 72(3), 278-288. <https://psycnet.apa.org/doi/10.1037/amp0000121>
- Scanlon, J. R., & Gerber, M. S. (2014). Automatic detection of cyber-recruitment by violent extremists. *Security Informatics*, 3(1), 5. <https://doi.org/10.1186/s13388-014-0005-5>
- Scheibe, M., Skutsch, M., & Schofer, J. (1975). Experiments in Delphi methodology. In H. A. Linstone, & M. Turoff (Eds.), *The Delphi method: Techniques and applications* (pp. 262-287). Addison-Wesley Publishing Company.
- Schmid, A. P. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. *ICCT Research Paper*. <http://www.icct.nl/download/file/ICCT-Schmid-Radicalisation-De-Radicalisation-Counter-Radicalisation-March-2013.pdf>

- Schneider, P., Evaniew, N., Rendon, J. S., McKay, P., Randall, R. L., Turcotte, R., ... & Ghert, M. (2016). Moving forward through consensus: Protocol for a modified Delphi approach to determine the top research priorities in the field of orthopaedic oncology. *BMJ open*, 6(5).
<http://dx.doi.org/10.1136/bmjopen-2016-011780>
- Schouten, R. (2010). Terrorism and the behavioral sciences. *Harvard Review of Psychiatry*, 18(6), 369-378.
<https://doi/abs/10.3109/10673229.2010.533005>
- Schulze, K. E., & Liow, J. C. (2019). Making jihadis, waging jihad: Transnational and local dimensions of the ISIS phenomenon in Indonesia and Malaysia. *Asian Security*, 15(2), 122-139.
<https://doi.org/10.1080/14799855.2018.1424710>
- Schuurman, B. (2018). Research on terrorism, 2007–2016: A review of data, methods, and authorship. *Terrorism and Political Violence*, 1-16.
<https://doi.org/10.1080/09546553.2018.1439023>
- Schuurman, B., & Eijkman, Q. (2013). *Moving terrorism research forward: The crucial role of primary sources*. International Centre for Counter-Terrorism—The Hague. <https://www.icct.nl/download/file/Schuurman-and-Eijkman-Moving-Terrorism-Research-Forward-June-2013.pdf>
- Schuurman, B., & Eijkman, Q. (2015). Indicators of terrorist intent and capability: Tools for threat assessment. *Dynamics of Asymmetric Conflict*, 8(3), 215-231. <https://doi.org/10.1080/17467586.2015.1040426>
- Scrivens, R., Davies, G., & Frank, R. (2018). Searching for signs of extremism on the web: an introduction to sentiment-based identification of radical authors. *Behavioral Sciences of Terrorism and Political Aggression*, 10(1), 39–59. <https://doi.org/10.1080/19434472.2016.1276612>
- Sehgal, U. (2011, July 23). Media reacts to news that Norwegian terror suspect isn't Muslim. *The Wire*. <http://www.thewire.com/global/2011/07/media-reacts-news-norwegian-terror-suspect-isnt-muslim/40322/>
- Seib, P., & Janbek, D. M. (2010). *Global terrorism and new media: The post-Al Qaeda generation*. Routledge.

- Selfhout, M., Burk, W., Branje, S., Denissen, J., van Aken, M., & Meeus, W. (2010). Emerging late adolescent friendship networks and Big Five personality traits: A social network approach. *Journal of Personality*, 78(2), 509-538. <https://doi.org/10.1111/j.1467-6494.2010.00625.x>
- Seow, J. (2019, January 26). More SGSecure initiatives to be held in malls, private estates and community groups. *The Straits Times*. <https://www.straitstimes.com/singapore/more-sgsecure-initiatives-to-be-held-in-malls-private-estates-and-community-groups>
- Seto, M. C., Karl Hanson, R., & Babchishin, K. M. (2011). Contact sexual offending by men with online sexual offenses. *Sexual Abuse*, 23(1), 124-145. <https://doi.org/10.1177%2F1079063210369013>
- Sezgin, E. (2007). *A comparative perspective of international cooperation against terrorism* (Doctoral dissertation). https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=kent1185301559&disposition=inline
- Shabi, R. (2016, March 18). Deradicalising Britain: The activists turning young Muslims away from extremism. *The Guardian*. <https://www.theguardian.com/uk-news/2016/mar/18/deradicalising-britain-the-activists-turning-young-muslims-away-from-extremism>
- Shaftoe, H., Turksen, U., Lever, J., & Williams, S. J. (2007). Dealing with terrorist threats through a crime prevention and community safety approach. *Crime Prevention and Community Safety*, 9(4), 291-307. <https://doi.org/10.1057/palgrave.cpcs.8150053>
- Shi, P. (2016). A supplementary intervention to deradicalisation: CBT-based online forum. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 410-424). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch020>
- Shortland, N. D. (2016). "On the internet, nobody knows you're a dog": The online risk assessment of violent extremists. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 1-15). IGI Global. <https://doi.org/10.4018/978-1-5225-0156-5.ch017>

- Shrout, P. E., & Fleiss, J. L. (1979). Intraclass correlations: uses in assessing rater reliability. *Psychological Bulletin*, 86(2), 420-428. <https://doi.org/10.1037/0033-2909.86.2.420>.
- Silber, M. D., & Bhatt, A. (2007). *Radicalization in the West: The home-grown threat*. New York City Police Department. <https://www.brennancenter.org/sites/default/files/legacy/Justice/20070816.NYPD.Radicalization.in.the.West.pdf>
- Silke, A. (1998). Cheshire-cat logic: The recurring theme of terrorist abnormality in psychological research. *Psychology, Crime and Law*, 4(1), 51-69. <https://doi.org/10.1080/10683169808401747>
- Simons, G. (2018). Brand ISIS: interactions of the tangible and intangible environments. *Journal of Political Marketing*, 17(4), 322-353. <https://doi.org/10.1080/15377857.2018.1501928>
- Skidmore, J. (2014). Foreign fighter involvement in Syria. *International Institute for Counterterrorism*, 9. <https://i-hls.com/wp-content/uploads/2014/01/Foreign-Fighter-Involvement-in-Syria.pdf>
- Skillicorn, D. (2008). *Knowledge discovery for counterterrorism and law enforcement*. CRC Press.
- Skinner, P. (2015, September 2). The power of ISIS' message. *The Cipher Brief*. <https://www.thecipherbrief.com/article/power-isis-message-0>
- Soral, W., Bilewicz, M., & Winiewski, M. (2018). Exposure to hate speech increases prejudice through desensitization. *Aggressive Behavior*, 44(2), 136-146. <https://doi.org/10.1002/ab.21737>
- Speckhard, A., & Ellenberg, M. (2020, April 15). Is internet recruitment enough to seduce a vulnerable individual into terrorism? *Homeland Security Today*. <https://www.hstoday.us/subject-matter-areas/counterterrorism/is-internet-recruitment-enough-to-seduc-a-vulnerable-individual-into-terrorism/>
- Speckhard, A., Shajkovci, A., & Yayla, A. S. (2017). Following a military defeat of ISIS in Syria and Iraq: What happens next after the military victory and the return of foreign fighters? *Contemporary Voices: St Andrews Journal of International Relations*, 8(1), 81-89. <http://doi.org/10.15664/jtr.1341>

- Stankov, L., Higgins, D., Saucier, G., & Knežević, G. (2010). Contemporary militant extremism: A linguistic approach to scale development. *Psychological Assessment*, 22(2), 246-258.
<https://psycnet.apa.org/doi/10.1037/a0017372>
- Stephenson, W. (1954). *The study of behavior: Q-technique and its methodology*. University of Chicago Press.
- Stern, J., & Berger, J. M. (2015). *ISIS: The state of terror*. Harper Collins.
- Sunstein, C. R. (2002). The law of group polarisation. *Journal of Political Philosophy*, 10(2), 175-195. <https://doi.org/10.1111/1467-9760.00148>
- Swann, W. B., Gomez, A., Dovidio, J. F., Hart, S., & Jetten, J. (2010). Dying and killing for one's group: Identity fusion moderates responses to intergroup versions of the trolley problem. *Psychological Science*, 21(8), 1176-1183. <https://doi.org/10.1177/0956797610376656>
- Tan, E. (2006). *Road to radicalisation: A psychological analysis of the Jemaah Islamiyah group and its members*. Research Report No. 01/2006. Home Team Behavioural Sciences Centre.
- Tapio, P., Paloniemi, R., Varho, V., & Vinnari, M. (2011). The unholy marriage? Integrating qualitative and quantitative information in Delphi processes. *Technological Forecasting and Social Change*, 78(9), 1616-1628. <https://doi.org/10.1016/j.techfore.2011.03.016>
- Tarrant, B. (2019). *The great replacement* [manifesto].
- Taylor, M., & Horgan, J. (2006). A conceptual framework for addressing psychological process in the development of the terrorist. *Terrorism and Political Violence*, 18(4), 585-601.
<https://doi.org/10.1080/09546550600897413>
- Thangaratinam, S., & Redman, C. W. (2005). The Delphi technique. *The obstetrician & gynaecologist*, 7(2), 120-125.
<https://doi.org/10.1576/toag.7.2.120.27071>
- The Soufan Group. (2015, December). *Foreign fighters: An updated assessment of the flow of foreign fighters into Syria and Iraq*.
http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf

- Tolis, E. (2019). Investigating the influence of ISIS radicalisation on the recruitment process: a critical analysis. *Journal of Policing, Intelligence and Counter Terrorism*, 14(2), 129-146.
<https://doi.org/10.1080/18335330.2019.1572910>
- Topal, R. (2019). A cyber-psychological and behavioral approach to online radicalization. In M. Khosrow-Pour (Ed.), *Multigenerational online behavior and media use: Concepts, methodologies, tools, and applications* (pp. 1031–1042). IGI Global. <https://doi-org/10.4018/978-1-5225-7909-0.ch056>.
- Torok, R. (2013). Developing an explanatory model for the process of online radicalisation and terrorism. *Security Informatics*, 2(1), 6.
<https://doi.org/10.1186/2190-8532-2-6>
- Torok, R. (2016). Social media and the use of discursive markers of online extremism and recruitment. In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era* (pp. 39-69). IGI Global. <https://10.4018/978-1-5225-0156-5.ch003>
- Torres-Soriano, M. R. (2019, August 13). *Jihadist Activism on the Internet Following the Collapse of the Caliphate*. VOX-Pol.
<https://www.voxpol.eu/jihadist-activism-on-the-internet-following-the-collapse-of-the-caliphate/>
- Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207-222.
<https://doi.org/10.1111/1467-8551.00375>
- Trojan, C., & Salfati, C. G. (2010). A multi-dimensional analysis of criminal specialization among single-victim and serial homicide offenders. *Homicide Studies*, 14(2), 107-131.
<https://doi.org/10.1177/1088767910364936>
- Tuck, H., Silverman, T., & Smalley, C. (2016). “Shooting in the right direction”: *Anti-ISIS foreign fighters in Syria and Iraq*. Institute for Strategic Dialogue. Retrieved from <https://www.isdglobal.org/wp-content/uploads/2016/08/ISD-Report-Shooting-in-the-right-direction-Anti-ISIS-Fighters.pdf>

- Ulschak, F. L. (1983). *Human resource development: The theory and practice of need assessment*. Reston Publishing Company.
- Vacca, J. R. (Ed.). (2019). *Online terrorist propaganda, recruitment, and radicalization*. CRC Press.
- van Buuren, J. (2012). Performative violence? The multitude of lone wolf terrorism. *Terrorism - An Electronic Journal and Knowledge Base*, 1, 1-23. Retrieved from <https://www.terrorisemelectronicjournal.org/terrorism-journal-1/volume-i-issue-1/performative-violence-the-multitude-of-lone-wolf-terrorism/>
- van Dyke, N., & Soule, S. A. (2002). Structural social change and the mobilizing effect of threat: Explaining levels of patriot and militia organizing in the United States. *Social Problems*, 49(4), 497-520. <https://doi.org/10.1525/sp.2002.49.4.497>
- van Ginkel, B., & Entenmann, E. (2016). *The foreign fighters phenomenon in the European Union. Profiles, threats & policies*. The International Centre for Counter–The Hague. <https://icct.nl/publication/report-the-foreign-fighters-phenomenon-in-the-eu-profiles-threats-policies/>
- van Wilgenburg, W. (2015). The Kurdish periphery. *Terrorism Monitor*, 13(24), 13-15. <https://jamestown.org/program/the-kurdish-periphery/>
- Vassar, M., Atakpo, P., & Kash, M. J. (2016). Manual search approaches used by systematic reviewers in dermatology. *Journal of the Medical Library Association*, 104(4), 302-304. <https://dx.doi.org/10.3163%2F1536-5050.104.4.009>
- Venhaus, J. M. (2010). *Why youth join al-Qaeda*. US Institute of Peace. <http://www.usip.org/publications/why-youth-join-al-qaeda>
- Vergani, M., & Bliuc, A. M. (2018). The language of new terrorism: Differences in psychological dimensions of communication in Dabiq and Inspire. *Journal of Language and Social Psychology*, 37(5), 523-540. <https://doi.org/10.1177/0261927X17751011>
- Vidino, L., & Hughes, S. (2015). *ISIS in America: From retweets to Raqqa*. Program on Extremism, The George Washington University. <https://extremism.gwu.edu/isis-america>

- Vito, D. C. (2017). Using media literacy to combat youth extremism. *YALS Spring 2017 Resources*, 18-20. <http://yalsa.ala.org/blog/2017/05/03/yals-spring-2017-resources-using-media-literacy-to-combat-youth-extremism/>
- von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the digital age: The use of the Internet in 15 cases of terrorism and extremism*. RAND Corporation.
https://www.rand.org/pubs/research_reports/RR453.html
- von Sikorski, C., Schmuck, D., Matthes, J., & Binder, A. (2017). “Muslims are not terrorists”: Islamic State coverage, journalistic differentiation between terrorism and Islam, fear reactions, and attitudes toward Muslims. *Mass Communication and Society*, 20(6), 825-848.
<https://doi.org/10.1080/15205436.2017.1342131>
- Watkin, W. (2019). *What we learned from Cambridge Analytica*.
<https://www.brunel.ac.uk/news-and-events/news/articles/What-we-learned-from-Cambridge-Analytica>
- Weimann, G. (2004). *www.terror.net: How modern terrorism uses the Internet*. Special Report No.116. United States Institute of Peace.
- Weimann, G. (2010). Terror on Facebook, Twitter, and YouTube. *Brown Journal of World Affairs*, 16(2), 45-54.
<https://www.jstor.org/stable/24590908>
- Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research*, 3(2), 75-90. <http://doi.org/10.15664/jtr.405>
- Weimann, G., & von Knop, K. (2008). Applying the notion of noise to countering online terrorism. *Studies in Conflict & Terrorism*, 31(10), 883-902. <https://doi.org/10.1080/10576100802342601>
- Weisburd, D., Savona, E. U., Hasisi, B., & Calderoni, F. (2020). *Understanding recruitment to organized crime and terrorism*. Springer.
<https://doi.org/10.1007/978-3-030-36639-1>
- Whitty, M. T., Doodson, J., Creese, S., & Hodges, D. (2018). A picture tells a thousand words: What Facebook and Twitter images convey about our personality. *Personality and Individual Differences*, 133, 109-114.
<http://dx.doi.org/10.1016/j.paid.2016.12.050>

- Wilner, A. S., & Dubouloz, C. J. (2011). Transformative radicalization: Applying learning theory to Islamist radicalization. *Studies in Conflict & Terrorism*, 34(5), 418-438.
<https://doi.org/10.1080/1057610X.2011.561472>
- Wimmer, A., & Nastiti, A. (2015). Darknet, social media, and extremism: Addressing Indonesian Counterterrorism on the Internet. *Deutsches Asienforschungszentrum Asian Series Commentaries*, 30.
<https://www.dafz.org/publications/commentaries/indonesian-internet-counter-terrorism/>
- Winter, C. (2015). *The virtual 'caliphate': Understanding Islamic State's propaganda strategy*. Quilliam Foundation.
<https://core.ac.uk/download/pdf/30671634.pdf>
- Wojcieszak, M. (2010). 'Don't talk to me': effects of ideologically homogeneous online groups and politically dissimilar offline ties on extremism. *New Media & Society*, 12(4), 637-655.
<https://doi.org/10.1177/1461444809342775>
- Wong, S. Y. (2015, May 27). 2 Singaporean youths radicalised by ISIS arrested, one of them detained for planning terror attacks. *The Straits Times*. <https://www.straitstimes.com/singapore/2-singaporean-youths-radicalised-by-isis-arrested-one-of-them-detained-for-planning-terror>
- Wood, G. (2015, March). What ISIS really wants. *The Atlantic*.
<http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/>
- Yasin, N. A. M. (2017). The evolution of online extremism in Malaysia. *Counter Terrorist Trends and Analyses*, 9(7).
<https://www.jstor.org/stable/26351534>
- Yousuf, M. I. (2007). Using experts opinions through Delphi technique. *Practical assessment, research, and evaluation*, 12(1), 1-8.
<https://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1171&context=pape>
- Zelin, A. (2013). *The state of global Jihad online*. New America Foundation.

Appendix A
Commonalities across the Six Terrorism Risk Assessment Tools

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
1	Need to redress injustice and express grievance (i.e., engagement with a terrorist group, cause or ideology meets needs to express or act on feelings of anger, grievance or injustice)	Need to redress injustice and express grievance	—	Personal grievance and moral outrage	Perceived injustice	Victim of injustice and grievances	Personal, terrorist narrative to promote extremist views, aggression, grievances Perceived victim of injustice, grievances for collective group or individual
2	Need to defend against threat (i.e., the individual feels that he, his family, identity, culture or values are under threat and a terrorist group or cause offers a vehicle to articulate these threats and defend and protect against them)	Need to defend against threat	—	—	Intergroup threat	Hostility to national collective identity	Identity conflict, rejection of national collective identity
3	Need for identity and meaning (i.e., the individual uses the terrorist group, cause or ideology to provide a clear sense of identity, meaning and belonging)	Need for identity, meaning, belonging	—	Identification	—	Commitment to group, group ideology	—
4	Need for status (i.e., the individual uses a terrorist group, cause or ideology to provide a sense of status and superiority)	Need for status	—	—	—	Driven by moral imperative, moral superiority	—

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
5	Need for excitement, comradeship or adventure (i.e., the individual uses a terrorist group, cause or ideology to fulfil a desire for excitement, adventure or comradeship)	Need for excitement, comradeship or adventure	Risk taking behaviour	—	—	Driven by excitement, adventure	—
6	Need for dominance (i.e., the individual uses a terrorist group, cause or ideology to dominate and control others)	Need for dominance	—	—	Violent role or status in group	—	—
7	Susceptibility to indoctrination (i.e., the individual accepts the ideology, beliefs and doctrine of a terrorist group or cause uncritically and without question)	Susceptibility to indoctrination	—	—	—	Susceptible to influence, authority, indoctrination	Susceptible to influence, authority, indoctrination
8	Political/ moral motivation (i.e., engagement with a terrorist group, cause or ideology is motivated by a desire to bring about political or moral change)	Political/ moral motivation	—	Framed by an ideology	—	—	—
9	Opportunistic involvement (i.e., engagement with a terrorist group, cause or ideology is motivated by self-interest rather than a political or moral cause)	Opportunistic involvement	—	—	—	Driven by criminal opportunism	—

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
10	Family or friends support terrorist offending (i.e., the individual's engagement with a terrorist group, cause or ideology is supported or condoned by their family or friends)	Family or friends support extremist offending	Negative peer influences	—	—	Network (family, friends) involved in violent action	—
11	Transitional periods (i.e., the individual engages with a terrorist group, cause or ideology during a transitional period in their life)	Transitional periods	—	Thwarting of occupational goals	—	—	—
12	Group influence and control (i.e., the individual is a member of a terrorist group that imposes a significant level of influence and control over their behaviour and conduct)	Group influence and control	Isolated from peer group	—	Group cohesion Group base identity Isolative group	—	—
13	Over-identification with a group or cause (i.e., the individual over-identifies with a group, cause and/or ideology to the extent of losing his own agency and sense of identity)	Over-identification with a group or cause	Extremist group membership	—	Commitment to group	—	—
14	Us and Them thinking (i.e., the individual divides the world into a demonised out-group and a favoured in-group with whom he identifies and whose cause he has adopted)	Us and Them thinking	Cultural and religious isolation	—	Negative attitudes toward out-group	Lack of empathy, understanding outside own group	Lack of understanding, tolerance outside own group

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
15	Dehumanisation of the enemy (i.e., the individual dehumanises members of the out-group and believes they should be purged or made to suffer)	Dehumanisation of the enemy	Hate rhetoric	—	—	Dehumanisation/ demonisation of identified targets of injustice	—
16	Attitudes that justify offending (i.e., the individual holds attitudes or beliefs that support and justify offending on behalf of their group, or ideology)	Attitudes that justify offending	—	—	Violent group norms	Commitment to ideology justifying violence	—
17	Harmful means to an end (i.e., the individual is prepared to commit serious or significant harm to realise terrorist goals)	Harmful means to an end	Violent rhetoric	—	—	—	Commitment to ideology justifying violence
18	Harmful end objectives (i.e., the individual holds objectives that are inherently harmful)	Harmful end objectives	—	—	—	Expressed desire to die for cause or martyrdom	Expresses willingness to die for cause, achieve martyrdom
19	Individual knowledge, skills and competencies to commit terrorist offences (i.e., the individual has specific knowledge, skills and competencies to support or commit a terrorist offence that could cause serious and significant harm)	Individual knowledge, skills and competencies	Advanced paramilitary training Basic paramilitary training	—	—	Tactical, paramilitary, explosives training Extremist ideological training	Has paramilitary, explosives training or information on explosives-bomb making

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
20	Establishes friendship bonds, networks other terrorists online	Access to networks, funding and equipment	Contact with known recruiters and extremists	Dependence on the virtual community	—	Personal contact with violent extremists Access to funds, resources, organisational skills	Is affiliated with an online group/ social media promoting terrorist violence Establishes friendship bonds, networks other violent extremists online
21	Criminal history (i.e., the individual has a criminal history that provides a level of capability to support or commit a terrorist offence that could cause serious and significant harm)	Criminal history	—	Predatory violence	Individual non-violent criminal behaviour	Prior criminal history of violence	—
22	Overseas combat experience	—	Overseas combat	—	—	—	—
23	Sudden change in religious practice	—	Sudden change in religious practice	—	—	—	—
24	Death rhetoric	—	Death rhetoric	—	—	—	—
25	Travel/ residence abroad	—	Travel/ residence abroad	—	—	—	—
26	Political activism	—	Political activism	—	—	—	—
27	Isolation from family	—	Isolation from family	—	Individual lack of pro-social integration	—	—
28	Greater creativity and innovation (i.e., there was evidence of tactical thinking, ‘Outside the box’)	—	—	Greater creativity and innovation	—	—	—
29	Nexus of psychopathology and ideology (i.e., if there was evidence of a major mental disorder by history or at present)	—	—	Nexus of psychopathology and ideology	Individual mental health problems	—	—

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
30	Failure of sexually intimate pair bonding and the sexualisation of violence (i.e., refers to the finding of a sexual attitude or behaviour in the subject which appears to substitute for the absence of a sexual pair bond, such as the sexualisation of weapons, the anticipation of unlimited sexual gratification in the afterlife, the exclusive use of prostitutes and other unbonded sources of sexual gratification, or compulsive use of pornography: all of these behaviours may be rationalised by the ideology)	—	—	Failure of sexually intimate pair bonding and the sexualisation of violence	—	—	—
31	Changes in thinking and emotion (i.e., indicated when thoughts and their expression become more strident, simplistic, and absolute)	—	—	Changes in thinking and emotion	—	—	—
32	Failure to affiliate with a terrorist group (i.e., actual failure or rejection of the individual terrorist from a radical or terrorist group that he wants to join)	—	—	Failure to affiliate with an extremist group	—	—	—

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
33	Directly communicated threat warning signs (i.e., the communication of a direct threat to the target or law enforcement be- forehand)	—	—	Directly communicated threat	Individual violent behaviour Group violence	Anger and expressed intent to act violently	Expresses intention to act violently, incites violence
34	Last resort warning signs (i.e., evidence of a “violent action imperative” and “time imperative”)	—	—	Last resort	—	—	—
35	Leakage warning signs (i.e., the communication to a third party of an intent to do harm to a target through an attack)	—	—	Leakage	—	—	—
36	Energy burst warning signs (i.e., an increase in the frequency or variety of any noted activities related to the target, even if the activities themselves are relatively innocuous, usually in the days or weeks before the attack)	—	—	Energy burst	—	—	—
37	Novel aggression warning signs (i.e., instance of violence that appears unrelated to any targeted violence pathway and is committed for the first time)	—	—	Novel aggression	—	—	—
38	Fixation warning signs (i.e., an increasingly pathological preoccupation with a person or a cause, accompanied by a deterioration in social and occupational life)	—	—	Fixation	—	—	—

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
39	Pathway warning signs (i.e., research, planning, preparation or implementation of an attack)	—	—	Pathway	—	Expressed intent to plan, prepare violent action	Evidence planning, preparing for violent action
40	Individual escalation in violent behaviour	—	—	—	Individual escalation in violent behaviour	—	—
41	Group escalation in group violence	—	—	—	Group escalation in group violence	—	—
42	Individual problems resulting from victimisation	—	—	—	Individual problems resulting from victimisation	—	—
43	Extreme social status of the group	—	—	—	Extreme social status of the group	—	Organises site/ page, rubrics to glorify violence, promote aggression, rigid worldview
44	Social instability	—	—	—	Social instability	—	—
45	Glorification of violent action	—	—	—	—	Glorification of violent action	—
46	Rejection of democratic society and values	—	—	—	—	Rejection of democratic society and values	Rejection of democratic society and values
47	Feelings of hate, frustration, persecution, alienation	—	—	—	—	Feelings of hate, frustration, persecution, alienation	Moral emotions: hate, anger, frustration, persecution, and/ or alienation
48	Seeker, consumer, developer of terrorist materials	—	—	—	—	Seeker, consumer, developer of violent extremist materials	—

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
49	Identification of target (person, place, group) in response to perceived injustice	—	—	—	—	Identification of target (person, place, group) in response to perceived injustice	—
50	Early exposure to pro-violence militant ideology	—	—	—	—	Early exposure to pro-violence militant ideology	—
51	Re-interpretation of ideology less rigid, absolute	—	—	—	—	Re-interpretation of ideology less rigid, absolute	—
52	Rejection of violence to obtain goals	—	—	—	—	Rejection of violence to obtain goals	—
53	Change of vision of enemy	—	—	—	—	Change of vision of enemy	—
54	Involvement with non-violent, de-radicalisation, offence-related programs	—	—	—	—	Involvement with non-violent, de-radicalisation, offence-related programs	—
55	Community support for non-violence	—	—	—	—	Community support for non-violence	—
56	Family support for non-violence	—	—	—	—	Family support for non-violence	—
57	Uses musical background to incite hatred, recruitment to violent action	—	—	—	—	—	Uses musical background to incite hatred, recruitment to violent action
58	Frequently changes profile and cover photos – inconsistent identity	—	—	—	—	—	Frequently changes profile and cover photos – inconsistent identity

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
59	Adherence to conspiracy theories about the affiliated ethnic/ religious group	—	—	—	—	—	Adherence to conspiracy theories about the affiliated ethnic/ religious group
60	Repetitively accesses posts blogs, terrorist forums, terrorist information, know-how	—	—	—	—	—	Repetitively accesses posts blogs, extremist forums, terrorist information, know-how
61	Uses multiple e-mail addresses, names to obscure identity	—	—	—	—	—	Uses multiple e-mail addresses, names to obscure identity
62	Subject has large following, network, significant role as leader online	—	—	—	Strong violent leadership	—	Subject has large following, network, significant role as leader online
63	Uses graphic representations, symbols/ logos of terrorist groups, steganography	—	—	—	—	—	Uses graphic representations, symbols/ logos of terrorist groups, steganography
64	Organises site/ page, rubrics to glorify violence, promote aggression, rigid worldview	—	—	—	—	—	Organises site/ page, rubrics to glorify violence, promote aggression, rigid worldview
65	Uses multiple/ alternative narratives related to identity	—	—	—	—	—	Uses multiple/ alternative narratives related to identity
66	Uses idealised content about own community, vilifies others, dehumanisation	—	—	—	—	—	Uses idealised content about own community, vilifies others, dehumanisation

Appendix A (continued)

No	Finalised factor	ERG 22+	IVP	TRAP-18	MLG	VERA-2	Cyber-VERA
67	Uses language to display terrorist views, allegiance to terrorist group, narrative	—	—	—	—	—	Uses language to display extremist views, allegiance to terrorist group, narrative

Note. Similarly defined factors from different tools were grouped as the same factor.

From “The development of structured guidelines for assessing risk in extremist offenders”, by M. Lloyd, & C. Dean, 2015, *Journal of Threat Assessment and Management*, 2(1), pp. 40-52, (<https://doi.org/10.1037/tam0000035>). Copyright 2015 by American Psychological Association; “Investigating the individual terrorist in Europe”, by J. R. Meloy, K. Roshdi, J. Glaz-Ocik, & J. Hoffmann, 2015, *Journal of Threat Assessment and Management*, 2(3-4), pp. 140-152, (<https://doi.org/10.1037/tam0000036>). Copyright 2015 by American Psychological Association; “Calibrating risk for violent political extremists: The VERA-2 Structural Assessment”, by D. E. Pressman, & J. S. Flockton, 2012, *The British Journal of Forensic Practise*, 14(4), pp. 237-251, (<https://doi.org/10.1108/14636641211283057>). Copyright 2012 by Emerald Publishing; “Can you identify violent extremists using a screening checklist and open-source intelligence alone?”, by V. Egan, J. Cole, B. Cole, L. Alison, E. Alison, S. Waring, & S. Elntib, 2016, *Journal of Threat Assessment and Management*, 3(1), pp. 21-36, (<http://dx.doi.org/10.1037/tam0000058>). Copyright 2016 by American Psychological Association; “Risk assessment and management of group-based violence”, by A. N. Cook, 2014, Doctoral dissertation. Copyright 2014 by Simon Fraser University; “Internet use and violent extremism: A cyber-VERA risk assessment protocol”, by D. E. Pressman, & C. Ivan, 2016, In M. Khader, L. S. Neo, G. Ong, E. Tan, & J. Chin (Eds.), *Combating violent extremism and radicalisation in the digital era*, pp. 391-409. Copyright 2016 by IGI Global.

Appendix B
Survey Used for Modified Delphi Technique

**USE OF THE MODIFIED DELPHI METHOD TO IDENTIFY AND RATE RISK AND
PROTECTIVE FACTORS FOR ONLINE VIOLENT EXTREMISM**

Thank you for agreeing to participate in this modified Delphi method survey.

2. This survey has been approved by the Nanyang Technological University (NTU)'s Institutional Review Board (IRB); IRB reference number is **IRB-2017-08-023**.

Instruction for first round of the modified Delphi method survey

3. The modified Delphi method survey comprises of two rounds. For the current first round, you will be required to evaluate and rate a list of factors with respect to its relevance (i.e., to identify individuals being radicalised via the internet) using a seven-point Likert-type rating scale that ranged from 'strongly disagree' (1) to 'strongly agree' (7).

4. These factors were collated from a conceptual literature review of extant violent extremism risk assessment tools such as the Extremism Risk Guidance 22+ (Lloyd & Dean, 2015), the Identifying Vulnerable People [IVP] guidance (Egan et al., 2016), the Terrorist Radicalisation Assessment Protocol [TRAP-18] (Meloy, Roshdi, Glaz-Ocik, & Hoffmann, 2015), Violent Extremist Risk Assessment [VERA-2] protocol (Pressman & Flockton, 2012), and the Cyber-VERA (Pressman & Ivan, 2016).

5. In addition, you are encouraged to suggest any additional factors that you feel are relevant to identifying individuals being radicalised via the internet.

Follow up for round 2 of the survey

6. Based on the results derived from this current first round, you will be sent a modified list to rate the relevance of the factors. Together, the entire survey (i.e., round 1 [current] and round 2) would take about 45 minutes to complete.

7. If you have any questions about the study, please contact the principal investigator and/or co-investigator.

Principal Investigator:

Neo Loo Seng
Division of Psychology
School of Social Sciences
Mobile: +65 9642-4926
Email: NEOL0015@e.ntu.edu.sg

Co-investigator:

Prof Joyce Pang
Division of Psychology
School of Social Sciences
Phone: +65 6790-6745
Email: JoycePang@ntu.edu.sg

Factor	Strongly Disagree		Neutral				Strongly agree
	1	2	3	4	5	6	7
Need to redress injustice and express grievance (i.e., engagement with an extremist group, cause or ideology meets needs to express or act on feelings of anger, grievance or injustice)							
Need to defend against threat (i.e., the individual feels that he, his family, identity, culture or values are under threat and an extremist group or cause offers a vehicle to articulate these threats and defend and protect against them)							
Need for identity, meaning, belonging (i.e., the individual uses the extremist group, cause or ideology to provide a clear sense of identity, meaning and belonging)							
Need for status (i.e., the individual uses an extremist group, cause or ideology to provide a sense of status and superiority)							
Need for excitement, comradeship or adventure (i.e., the individual uses an extremist group, cause or ideology to fulfil a desire for excitement, adventure or comradeship)							
Need for dominance (i.e., the individual uses an extremist group, cause or ideology to dominate and control others)							
Susceptibility to indoctrination (i.e., the individual accepts the ideology, beliefs and doctrine of an extremist group or cause uncritically and without question)							
Political/ moral motivation (i.e., engagement with an extremist group, cause or ideology is motivated by a desire to bring about political or moral change)							
Opportunistic involvement (i.e., engagement with an extremist group, cause or ideology is motivated by self-interest rather than a political or moral cause)							
Family or friends support extremist offending (i.e., the individual's engagement with an extremist group, cause or ideology is supported or condoned by their family or friends)							
Transitional periods (i.e., the individual engages with an extremist group, cause or ideology during a transitional period in their life)							
Group influence and control (i.e., the individual is a member of an extremist group that imposes a significant level of influence and control over their behaviour and conduct)							
Over-identification with a group or cause (i.e., the individual over-identifies with a group, cause and/or ideology to the extent of losing his own agency and sense of identity)							
Us and Them thinking (i.e., the individual divides the world into a demonised out-group and a favoured in-group with whom he identifies and whose cause he has adopted)							
Dehumanisation of the enemy (i.e., the individual dehumanises members of the out-group and believes they should be purged or made to suffer)							
Attitudes that justify offending (i.e., the individual holds attitudes or beliefs that support							

and justify offending on behalf of their group, or ideology)							
Harmful means to an end (i.e., the individual is prepared to commit serious or significant harm to realise extremist goals)							
Harmful end objectives (i.e., the individual holds objectives that are inherently harmful)							
Individual knowledge, skills and competencies to commit extremist offences (i.e., the individual has specific knowledge, skills and competencies to support or commit a terrorist offence that could cause serious and significant harm)							
Access to networks, funding and equipment to commit extremist offences (i.e., the individual has access to networks, funding and/or equipment to support or commit a terrorist offence that could cause serious and significant harm)							
Criminal history (i.e., the individual has a criminal history that provides a level of capability to support or commit a terrorist offence that could cause serious and significant harm)							
Overseas combat experience							
Sudden change in religious practice							
Death rhetoric							
Travel/ residence abroad							
Political activism							
Isolation from family							
Greater creativity and innovation (i.e., there was evidence of tactical thinking 'Outside the box')							
Nexus of psychopathology and ideology (i.e., if there was evidence of a major mental disorder by history or at present)							
Failure of sexually intimate pair bonding and the sexualisation of violence (i.e., refers to the finding of a sexual attitude or behaviour in the subject which appears to substitute for the absence of a sexual pair bond, such as the sexualisation of weapons, the anticipation of unlimited sexual gratification in the afterlife, the exclusive use of prostitutes and other unbonded sources of sexual gratification, or compulsive use of pornography: all of these behaviours may be rationalised by the ideology)							
Changes in thinking and emotion (i.e., indicated when thoughts and their expression become more strident, simplistic, and absolute)							
Failure to affiliate with an extremist group (i.e., actual failure or rejection of the individual terrorist from a radical or extremist group that he wants to join)							
Directly communicated threat warning signs (i.e., the communication of a direct threat to the target or law enforcement beforehand)							
Last resort warning signs (i.e., evidence of a "violent action imperative" and "time imperative")							
Leakage warning signs (i.e., the communication to a third party of an intent to do harm to a target through an attack)							
Energy burst warning signs (i.e., an increase in the frequency or variety of any noted activities)							

related to the target, even if the activities themselves are relatively innocuous, usually in the days or weeks before the attack)							
Novel aggression warning signs (i.e., instance of violence that appears unrelated to any targeted violence pathway and is committed for the first time)							
Fixation warning signs (i.e., an increasingly pathological preoccupation with a person or a cause, accompanied by a deterioration in social and occupational life)							
Pathway warning signs (i.e., research, planning, preparation or implementation of an attack)							
Individual escalation in violent behaviour							
Group escalation in group violence							
Individual problems resulting from victimisation							
Extreme social status of the group							
Social instability							
Glorification of violent action							
Rejection of democratic society and values							
Feelings of hate, frustration, persecution, alienation							
Seeker, consumer, developer of violent extremist materials							
Identification of target (person, place, group) in response to perceived injustice							
Early exposure to pro-violence militant ideology							
Re-interpretation of ideology less rigid, absolute							
Rejection of violence to obtain goals							
Change of vision of enemy							
Involvement with non-violent, de-radicalization, offence-related programs							
Community support for non-violence							
Family support for non-violence							
Uses musical background to incite hatred, recruitment to violent action							
Frequently changes profile and cover photos – inconsistent identity							
Adherence to conspiracy theories about the affiliated ethnic/religious group							
Repetitively accesses posts blogs, extremist forums, terrorist information, know-how							
Uses multiple e-mail addresses, names to obscure identity							
Subject has large following, network, significant role as leader online							
Uses graphic representations, symbols/logos of terrorist groups, steganography							
Organises site/page, rubrics to glorify violence, promote aggression, rigid worldview							
Uses multiple/ alternative narratives related to identity							
Uses idealised content about own community, vilifies others, dehumanisation							
Uses language to display extremist views, allegiance to terrorist group, narrative							
Lack of understanding, tolerance outside own group							
Is affiliated with an online group/social media promoting terrorist violence							

Establishes friendship bonds, networks other violent extremists online							
--	--	--	--	--	--	--	--

Any other factors?

- Thank you -

Appendix C
Codebook for Identifying Factors and their Indicators

PERSON-CENTRIC DIMENSION

Factor	Indicators	Example	Keywords
PERCEIVED GRIEVANCES	1. Publicise the injustices targeted at one's own community, faith, or belief	"No freedom of speech for you if you support your religion over their laws."	Shia, Shiite, Alawite, Kuffar, Kufr, War on Islam, Kafir, America, Britain, France, Germany, Canada, Australia, the West, Israel, Palestine, West Bank, Gaza, Jews, Bush, Blair, Cameron, Obama, Hollande, Merkel, Netanyahu, Guantanamo, Abu Ghraib, Patriot Act, Prevent, Terrorism, Bashar al-Assad, Starving, Chemical Weapons, Bomb, Tauhid
	2. Demonstrates a preoccupation with certain group(s) of concern who is responsible for the injustice	"so when will Obama be in a war crimes tribunal for his latest massacre of 70 civilians in Iraq?"	
	3. Express frustration with the injustice targeted at one's own community, faith, or belief	"Around the world we have #Muslims dying for #Islam #Syria #Burma here we have #Muslims laughing at #Islam #WakeUp"	
	4. Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice	"Never forget 14 year Abeer Qassim, gang raped and murdered along with her family by US forces in Iraq.. #USACrimes"	
	5. Openly challenge certain group(s) of concern about the injustice	"Shiites and USA who destroy. IS is the only one building any infrastructure in Iraq"	
KNOWLEDGE AND SKILLS TO COMMIT TERRORIST OFFENCES	6. Demonstrate an interest in learning combat skills	Images of themselves in military uniforms or with military paraphernalia, using language of military tactics	Guns, Knives, Mixed Martial Arts, Extreme Street Fighting, inspire, dabiq, azan, Manchester document
	7. Showcase interest in the use of weapons and explosives	Images of themselves using weapons and explosives	
	8. Has information on explosives-bomb making	Provide instruction guide to construct explosives; share training manuals via web-links	
REDEMPTION AND THE PURSUIT FOR SIGNIFICANCE	9. Desire to partake in humanitarian activities in countries associated with terrorism opportunities	They really need experts on the aging electrical grid! This is a big problem here, and if you contact the Lions through our website we will assist you to come here, and give you instruction in language and connect you with the right groups here. To properly make full effect of your time here, you should aim for 6 months here, although we say 3 months minimum	Hijrah, Hijra, Migration, Leave, Sham, Turkey, Border, Khilafah, Muslims, Kuffar, Kafir, Kufr, Drinking, Drunk, Drunken, Homosexuality, Gay, Fornication, Free Mixing, Islam, Sisters, Brothers, Plane, Airport, Fly, Convoy, Bus, Tawwakul
	10. Desire to migrate to countries associated with terrorism opportunities	"When conducting hijrah, do not worry if we get weird label from our environment, Rasulallah even experienced more than than. Only God knows the truth."	

	11. Expresses feelings of contempt for own prior practices	Condemns one's prior moderate religious practices	
	12. Intention to search for opportunity to do something meaningful	Engage others online and express interest in doing something useful for one's community	
PERSONAL UNCERTAINTY	13. Desire to explore different ideologies and beliefs – inconsistent identity	Frequently changes profile and cover photos; strong negative feelings associated with change	loss, isolation, uncertainty, fear, threat
READINESS TO USE VIOLENCE	14. Voice strong support for the use of violence as a solution towards a certain group(s) of concern?	"Running away from jihad will not save you from death. You can die as a coward or you can die as a martyr"	Attack, Bomb, Knife, Chop, Qareeban, Qariban, Ummah, Brothers, Fathers, Mothers, Sisters, Jihad, Soldier, Army Parliament, Hijra, Hijrah, Humiliation, Jail, Prison, Defend, Avenge, Free, Migrate, Leave, Ummah, Brothers, Fathers, Mothers, Sisters, Jihad, Martyr, Shaheed, Shahada, Tauhid, Tauheed, Tawheed, Quran, Shariah, Sword, Flag, Raya, Rayat, Ribat, Ribaat, Checkpoint, Klash, AK, AK47, AK-47, Humvee, Glock, Call of Duty, Alawites, Alawite, Alawi, Nusairi, Nusayri, Tourism, Qareeban, Qariban, Conquer, Dabiq, mobilise
	15. Incites friends, colleagues or family to join the violent extremist cause to defend their faith, religion or belief?	"In the name of Allah, winter operation is challenging. Baramils fall as we pray underground. But this is a battle, patience... Because martyrdom is a gift for those who are genuine in their fight. Here's hoping that the picture I post inspire others to fight..."	
	16. Expresses willingness to die for cause, and achieve martyrdom	"To have Islam triumph is my goal. Syahid is my dream. "	
	17. Demonstrates a preoccupation with an individual from group(s) of concern as a potential target	"To the murtad, munafiqueen, the kuffar, to those sell out who are causing hardship to the Muslims, wallahi I pray that you meet Allah soon and that he gives the worst of his torments"	
	18. Display themselves as a protector/hero of their fellow believers of the same faith, religion or belief?	"The time is here, around the corner it will appear. When t does the world will watch in awe how the breeze of the Khilafah sweeps across"	
	19. Perceives an urgency to act and that non-violent alternative are ineffective solutions	"We've tried everything, it's hopeless, and now we have no other choice but to..."	
	20. Indicate their intention to travel and participate in overseas conflict?	"Hi baran my name is john and I'm from Ireland. I want to volunteer. Can you provide info? Please contact me at"	

PSYCHOSOCIAL DIMENSION

Factor	Indicators	Example	Keywords
COMMITMENT TO TERRORIST GROUPS	21. Quotations from / associations with personalities known for their radical views	Anwar Al-Awlaki; Anjem Choudhry; Jihadi John; Abu Bakr Al-Bashir; Yusha Evans	Ummah, Brothers, Fathers, Mothers, Sisters, Prison, Aleppo, Halab, Damascus, Sham,

	22. Identifies with symbols of known terrorist groups on one's online profile	Islamic State of Iraq and the Levant; AlKhalifah; The Nusra Front	Idlib, Raqqa, Raqqah, Deir ez-Zour, Mosul, Dawla, Dawlah, Khilafah, Abu Bakr al-Baghdadi, Baghdadi, Baghdad, Maliki, Bashar al-Assad, Bashar, Assad, Alawites, Alawite, Alawi, Nusairi, Nusayri, Dogs, Syrian Army, Murtad, Kafir, Kufr, Kuffar, Starving, Siege, Barrel Bomb, Helicopter, Jet, Drone, Bomb, Civilians, Regime, Chemical Weapons, Gas, International Community, United Nations, UN, Mujahideen, Mujahid, Soldier
	23. Display their public allegiance to terrorist groups	Islamic State of Iraq and the Levant; AlKhalifah; The Nusra Front	
	24. Praise and defend terrorist groups	All the conditions for the state were met in Iraq now we're just expanding and it's going really well alhamdulillah	
INTOLERANCE TOWARDS MULTI-RACIAL AND MULTI-RELIGIOUS LIVING	25. Force friends, colleagues or family to distance themselves from certain group(s) or community	"This is a war against Islam and it is know (sic) that either "you're with them or with us". So pick a side."	Kuffar, Kafir, Kufr, Drinking, Drunk, Drunken, Homosexuality, Gay, Fornication, Free Mixing, democracy, bad Muslims, infidels
	26. Dehumanises group(s) of concern who hold different viewpoints/ beliefs system	"They [Shias] are not Muslims at all, they all apostated ages ago"	
	27. Dissatisfaction with local cultures, practices, values, and governance	"Christians are living under dawlat & you are still in darul kufr, what a shame"	
	28. Anti-integration messaging – exclusivity of one's own community, faith, or belief	"It is better to kiss the hands of a goat than the hands of a person who does not pray"	
ONLINE RELATIONSHIP BUILDING WITH LIKE-MINDED INDIVIDUALS	29. Attempts to reach out to terrorists	posting comments in response to others; liking/ sharing/ retweeting/ posting comments	
	30. Develops and disseminates terrorist content	Recirculate terrorist materials;	
	31. Seeking to set up physical meeting with terrorists	Offer one's contact details and make arrangements to meet others	
INVOLVEMENT IN TERRORIST ONLINE COMMUNITY	32. Possess terrorist documents, music, videos etc. on computer or mobile devices	Contain terrorist related materials available for viewing, or sharing	Islamic State of Iraq and the Levant; AlKhalifah; The Nusra Front, Facebook, Twitter, Instagram, Tawheed Network; Ummah News; Green Birds; Bilad al Sham 19; Group Symbols
	33. Host web-links to other online platforms that contain terrorist context	Other social media accounts; materials that are available for viewing, sharing or downloading	

	34. Subscribes to sources that propagate terrorist ideologies, news or in-group favouritism	Tawheed Network; Ummah News; Green Birds; Bilad al Sham 19; Group Symbols (One Finger Salute; ISIS Flag)	
	35. A sudden increase in the user's activity	A sudden flurry of activity or a sharp drop in activity.	
NEGATIVE SOCIAL SUPPORT	36. Presence of supportive family members and friends that encourage involvement in the terrorist online communities and/or terrorist offending	Families and friends support the subject financially or grant them permission	

PROTECTIVE DIMENSION

Factor	Indicators	Example	Keywords
INDIVIDUAL-CENTRIC PROTECTIVE ELEMENTS	37. Presence of supportive family members and friends that discourage terrorist offending	Family and friends challenge the subject and offer help and assistance for the rejection of violent actions and views	Support, Counter productive
	38. Demonstrates willingness to engage in discussions of ideology and the use of violence	Presence of cognitive opening in relation to a shift in ideology	
	39. Disillusioned with using violence to solve problems	Presence of cognitive opening in relation to a shift in the use of violence	
	40. Demonstrates an appreciation for diversity	Able to co-exist in a multi-racial and multi-religious society	
ONLINE ENVIRONMENT-CENTRIC PROTECTIVE ELEMENTS	41. Inability to obtain access to the terrorist online community	Express frustration at one's inability to connect with the 'right' people online	
	42. Recognizes and fear the detection by law enforcement and social media companies	Voice concerns about being detected	

Appendix D
Survey on ‘understanding community’s perceptions towards radicalisation via
the internet, and terrorism’

**UNDERSTANDING COMMUNITY’S PERCEPTIONS TOWARDS RADICALISATION
VIA THE INTERNET, AND TERRORISM**

Thank you for agreeing to participate in this survey.

2. This survey has been approved by the Nanyang Technological University (NTU)’s Institutional Review Board (IRB); IRB reference number is **IRB-2019-02-035**.

Instruction for survey

3. This survey aims to understand the perceptions and ideas that the community may have towards radicalisation via the internet, and terrorism in general.
4. There are three sections in the survey (demographics; opinions about factors for radicalisation via the internet; awareness about the threat of terrorism), which will take approximately 15 minutes to complete.
5. Please be assured that your identity will be kept confidential, and no personal data will be revealed.
6. If you have any questions about the study, please contact the principal investigator and/or co-investigator.

Principal Investigator:

Neo Loo Seng
Division of Psychology
School of Social Sciences
Mobile: +65 9642-4926
Email: NEOL0015@e.ntu.edu.sg

Co-investigator:

Prof Joyce Pang
Division of Psychology
School of Social Sciences
Phone: +65 6790-6745
Email: JoycePang@ntu.edu.sg

SECTION A: Demographics (5 questions)

This section seeks to obtain basic demographic information about the participant.

1. Gender: _____

- Male
- Female

2. Age bracket: _____

- 18-22
- 23-27
- 28-32
- 33-37
- 38-42
- 43-47
- >48

3. Race: _____

- Malay
- Chinese

- Indian
- Eurasian
- Others

4. Religious group affiliation: _____

- Islam
- Christian
- Buddhism
- Hindu
- Others

5. Nationality: _____

- Singaporean
- Others: _____

SECTION B: Opinions about factors for radicalisation via the internet (42 questions)

This section seeks to obtain participants' opinions about the relevance of 42 indicators in identifying an individual who is becoming radicalised via the internet. The participants will be told to rate them on a five-point Likert scale— from one (strongly irrelevant) to five (strongly relevant).

Qn	Factor	Strongly disagree 1	2	Neutral 3	4	Strongly agree 5
6	Publicise the injustices targeted at one's own community, faith, or belief					
7	Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice					
8	Express frustration with the injustice targeted at one's own community, faith, or belief					
9	Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice					
10	Openly challenge certain group(s) of concern about the injustice					
11	Force friends, colleagues or family to distance themselves from certain group(s) or community					
12	Dehumanise group(s) of concern who hold different viewpoints/ beliefs system					
13	Dissatisfaction with local cultures, practices, values, and governance					
14	Anti-integration messaging— exclusivity of one's own community, faith, or belief					
15	Demonstrate an interest in learning combat skills					

16	Showcase interest in the use of weapons and explosives					
17	Have information on explosives-bomb making					
18	Desire to partake in humanitarian activities in countries associated with terrorism opportunities					
19	Desire to repent by migrating to countries associated with terrorism opportunities					
20	Express feelings of contempt for own prior practices					
21	Intention to search for opportunity to do something meaningful					
22	Desire to explore different ideologies and beliefs—inconsistent identity					
23	Voice strong support for the use of violence towards a certain group(s) of concern as a viable solution					
24	Incite friends, colleagues or family to join the terrorist cause to defend his/her faith, religion or belief					
25	Express willingness to die for cause, and achieve martyrdom					
26	Demonstrate a preoccupation with an individual from group(s) of concern as a potential target					
27	Display himself/herself as a protector/hero of his/her fellow believers of the same faith, religion or belief					
28	Perceive an urgency to act, and that non-violent alternative are ineffective solutions					
29	Indicate his/her intention to travel and participate in overseas conflict					
30	Quotations from / associations with personalities known for their extremist views					
31	Identify with symbols of known terrorist groups on one's online profile					
32	Display his/her public allegiance to terrorist groups					
33	Praise and defend terrorist groups					
34	Attempt to reach out to terrorist					
35	Develop and disseminates terrorist content					

36	Attempt to set up physical meeting with terrorists					
37	Possess terrorist documents, music, videos etc. on computer or mobile devices					
38	Host web-links to other online platforms that contain terrorist context					
39	Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism					
40	A sudden increase in the user's activity					
41	Presence of supportive family members and friends that encourage extremist offending					
42	Presence of supportive family members and friends that discourage extremist offending					
43	Demonstrate willingness to engage in discussions of ideology and the use of violence					
44	Disillusioned with using violence to solve problems					
45	Demonstrate an appreciation for diversity					
46	Inability to obtain access to online community					
47	Recognise and fear the detection by law enforcement and social media companies					

SECTION C: Awareness about the threat of terrorism (27 questions)

This section seeks to obtain participants' awareness about radicalisation via the internet, and the threat of terrorism.

Sources of information

Qn	Question	Answer scale	Remarks
48	Where do you obtain information on terrorism?	<ul style="list-style-type: none"> • Television • Internet • Newspapers • Books • Radio • Magazines • Seminars/ courses/ conferences • Others: _____ 	Select all that apply
49	The media conveniently links terrorism with Islam	1 (strongly disagree) 2 (disagree)	-

50	There is sufficient fair coverage on terrorism in the media	3 (neutral) 4 (agree) 5 (strongly agree)	
51	I have sufficient knowledge on the threat of terrorism in my country		
52	My fellow citizens are aware of the threat of terrorism		

Definition of terrorism

Qn	Question	Answer scale	Remarks
53	What is terrorism?	<ul style="list-style-type: none"> • Riots/ strikes • Murder • Killing of civilians • Hijacking • Armed robbery • Rape • Street demonstrations • Others: _____ 	Select all that apply
54	How likely do you think it is for a terror attack to happen in my country?	1 (strongly disagree) 2 (disagree) 3 (neutral)	-
55	Terrorism is illegal and unethical at all times	4 (agree) 5 (strongly agree)	

Terrorism and the internet

Qn	Question	Answer scale	Remarks
56	Terrorism needs the internet to grow	1 (strongly disagree) 2 (disagree)	-
57	It is easy for an individual becoming radicalised via the internet	3 (neutral) 4 (agree) 5 (strongly agree)	

Countering terrorism

Qn	Question	Answer scale	Remarks
58	The community plays an important role in countering terrorism	1 (strongly disagree) 2 (disagree) 3 (neutral) 4 (agree) 5 (strongly agree)	-
59	Military action is the most effective way in dealing with terrorism		
60	The government is capable of handling the threat of terrorism		
61	I have a role to play in preventing a terrorist attack in my country.		
62	I am responsible for reporting individuals whom I suspect to be radicalised to the authorities.		
63	I know who to report to if I suspect that an individual is radicalised.		
64	Who should I report to?	_____	<open ended>

65	What would prevent someone from reporting people to the authorities if they observed them showing signs of radicalisation?		
----	--	--	--

Radicalisation process

Qn	Question	Answer scale	Remarks
66	A terrorist usually starts out by having violent radical ideas	1 (strongly disagree) 2 (disagree) 3 (neutral) 4 (agree) 5 (strongly agree)	
67	It is possible to have violent radical ideas without resorting to terrorism		
68	It is not wrong to have violent radical ideas just as long as you do not engage in terrorism		
69	It is possible to move from having violent radical ideas to actually conducting violent acts such as terrorism		
To what extent do you agree or disagree that terrorists are:			
70	Mentally ill		
71	Religious		
72	From low-income families		
73	Heroic		
74	Male		

- Thank you -

Appendix E Mean and Standard Deviation for Ratings on the 42 Indicators

Indicator	Combined		NTU		MTurk	
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
PG1: Publicise the injustices targeted at one's own community, faith, or belief	3.55	1.01	3.48	1.08	3.61	0.93
PG2: Demonstrate a preoccupation with certain group(s) of concern who is responsible for the injustice	3.87	0.91	3.83	0.87	3.91	0.93
PG3: Express frustration with the injustice targeted at one's own community, faith, or belief	3.61	1.01	3.57	1.03	3.65	1.00
PG4: Express a strong sense of hatred towards a certain group(s) of concern who is responsible for the injustice	4.37	0.84	4.31	0.82	4.43	0.86
PG5: Openly challenge certain group(s) of concern about the injustice	3.73	1.00	3.77	0.99	3.70	1.01
K1: Demonstrate an interest in learning combat skills	3.03	1.27	2.60	1.16	3.46 **	1.24
K2: Showcase interest in the use of weapons and explosives	3.70	1.23	3.50	1.23	3.91 *	1.19
K3: Have information on explosives-bomb making	3.80	1.22	3.71	1.18	3.88	1.26
S1: Desire to partake in humanitarian activities in countries associated with terrorism opportunities	3.21	1.29	3.18	1.31	3.25	1.26
S2: Desire to repent by migrating to countries associated with terrorism opportunities	3.67	1.21	3.62	1.20	3.71	1.22
S3: Express feelings of contempt for own prior practices	3.15	1.06	3.07	0.98	3.23	1.13
S4: Intention to search for opportunity to do something meaningful	2.56	1.25	2.40	1.12	2.71 *	1.35
P1: Desire to explore different ideologies and beliefs—inconsistent identity	2.72	1.18	2.53	1.06	2.91 *	1.25
R1: Voice strong support for the use of violence towards a certain group(s) of concern as a viable solution	4.29	0.98	4.33	0.94	4.25	1.02
R2: Incite friends, colleagues or family to join the terrorist cause to defend their faith, religion or belief	4.33	1.06	4.38	1.11	4.27	1.01
R3: Express willingness to die for cause, and achieve martyrdom	4.24	1.10	4.23	1.16	4.25	1.03
R4: Demonstrate a preoccupation with an individual from group(s) of concern as a potential target	4.00	0.95	4.05	0.98	3.95	0.92
R5: Display themselves as a protector/hero of their fellow believers of the same faith, religion or belief	3.71	1.01	3.70	1.00	3.71	1.04
R6: Perceive an urgency to act and that non-violent alternative are ineffective solutions	4.03	1.01	4.10	0.98	3.95	1.03
R7: Indicate their intention to travel and participate in overseas conflict	3.98	1.08	4.08	1.02	3.88	1.14
C1: Quotations from/ associations with personalities known for their radical views	3.83	1.05	3.96 *	1.02	3.71	1.08
C2: Identify with symbols of known terrorist groups on one's online profile	4.19	1.00	4.28	0.94	4.10	1.04
C3: Display their public allegiance to terrorist groups	4.38	1.02	4.50 *	0.93	4.25	1.10
C4: Praise and defend terrorist groups	4.26	1.13	4.44 **	1.00	4.08	1.23

Appendix E (continued)

Indicator	Combined		NTU		MTurk	
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
I1: Force friends, colleagues or family to distance themselves from certain group(s) or community	3.97	1.06	3.95	1.06	4.00	1.06
I2: Dehumanise group(s) of concern who hold different viewpoints/ beliefs system	4.12	1.00	4.21	1.00	4.02	0.99
I3: Dissatisfaction with local cultures, practices, values, and governance	3.20	1.10	3.10	1.02	3.30	1.17
I4: Anti-integration messaging—exclusivity of one's own community, faith, or belief	3.71	1.00	3.71	0.98	3.71	1.03
OR1: Attempt to reach out to terrorists	4.37	1.13	4.53 *	0.98	4.21	1.25
OR2: Develop and disseminates terrorist content	4.37	1.03	4.54 **	0.91	4.20	1.11
OR3: Attempt to set up physical meeting with terrorists	4.43	1.04	4.57 *	0.97	4.30	1.09
OC1: Possess terrorist documents, music, videos etc. on computer or mobile devices	4.16	1.09	4.32 *	1.01	4.01	1.15
OC2: Host web-links to other online platforms that contain terrorist context	4.17	1.07	4.38 **	0.97	3.97	1.13
OC3: Subscribe to sources that propagate terrorist ideologies, news or in-group favouritism	4.19	1.04	4.31 *	0.99	4.06	1.08
OC4: A sudden increase in the user's activity	2.85	1.13	2.68	1.03	3.03 **	1.20
N1: Presence of supportive family members and friends that encourage involvement in the terrorist online communities and/or terrorist offending	3.79	1.03	3.80	1.04	3.78	1.02
IP1: Presence of supportive family members and friends that discourage terrorist offending	2.73	1.18	2.77	1.09	2.70	1.27
IP2: Demonstrate willingness to engage in discussions of ideology and the use of violence	3.58	1.10	3.51	1.09	3.65	1.10
IP3: Disillusioned with using violence to solve problems	3.44	1.31	3.86 **	1.08	3.01	1.38
IP4: Demonstrate an appreciation for diversity	2.24	1.29	2.00	1.08	2.48 **	1.43
OP1: Inability to obtain access to the terrorist online community	2.48	1.07	2.42	0.91	2.53	1.22
OP2: Recognise and fear the detection by law enforcement and social media companies	3.31	1.11	3.18	1.08	3.45 *	1.12

Note. Analysis based on t-test: * $p < .05$. ** $p < .00$.

<End of Thesis>