Countering Violent Extremism Online

Understanding Adversity And Adaptation In An Increasingly Complex Digital Environment
In this report, we have sought to understand how violent extremists behave across an increasingly complex online ecosystem and consider the implications for how online violent extremism (VE) activity can be countered. We interrogated the variety of measures, behaviours and technology platforms that are being used by violent extremists internationally. In so doing, we identified gaps in understanding of the complex and expansive contours of the VE online landscape, and the extent to which VE online does, or does not, constitute a distinctive phenomenon that might require a different policy setting. The outcomes of the research will contribute to the undertakings of the Office of the Ambassador for Counter-Terrorism in establishing a first-rate network between Australia and its international partners that enables a ready and trusted exchange of knowledge and communication on VE and terrorism activities to maximise the effectiveness of counters.

**Funding**

This work was sponsored by the Australian Department of Foreign Affairs and Trade.

**About RAND Australia**

RAND Australia is RAND’s Canberra-based subsidiary that analyses defence, national security, economic, and social issues for Australian clients. With a commitment to core values of quality and objectivity, RAND Australia combines local research talent with world-class experts from across RAND’s global presence to solve complex Australian public policy problems.

For more information on RAND Australia or to contact our director, please visit www.rand.org/australia.

**Acknowledgments**

We thank the (former) Ambassador of Counter Terrorism, MAJGEN Roger Noble (ret’d) for engaging us to examine this fascinating problem. More recently, we thank Ciara Spencer, First Assistant Secretary Intelligence and Security, for her ongoing support. In addition, we thank the following members of the Office of the Ambassador for Counter-Terrorism (OCT) team for their interaction, for their guidance and for introducing us to more stakeholders: Nicholas Kittel, Renee McGregor and Aaron Watson. Finally, we thank Suzanne Raine and Jacopo Bellasio for their thoughtful and helpful reviews of this work and Jade Yeung for participating in our long discussions as we progressed the research.
Summary

Issue

In this report, we seek to understand how violent extremists behave in an increasingly complex online ecosystem. This ecosystem, which is characterised by technological innovation and diversification of platforms, offers significant utility and advantages to violent extremists. By interrogating the variety of measures and behaviours that are being used by violent extremists internationally, we have identified gaps in understanding of the complex and expansive contours of the violent extremism (VE) online landscape and the extent to which VE online constitutes a distinctive phenomenon that might require a different policy setting.

This report is situated after the 2017 launch of the Global Internet Forum to Counter Terrorism and the United Nations–backed Tech Against Terrorism initiative. Both bodies emerged following significant public and political pressure to challenge the rise of the Islamic State’s (IS’s) virtual caliphate across a variety of mainstream social media platforms. However, the resulting emphasis on coordinated deplatforming appears to have encouraged violent extremists, particularly at the network level, to explore other alternative-technology platforms on which they are less challenged and more secure.\(^1\) In addition, violent extremists have learned to adjust their behavioural posture through a variety of tactical measures to evade these counters. Although law enforcement agencies are conscious of how enforcement and denial actions change behaviours, there will always be a trade-off between keeping extremists where they can be monitored online and deplatforming them to reduce potential harm. Some of the ongoing adaptations of violent extremists are illustrated in this report using case studies and examples from a variety of different platforms. Moreover, at the strategic level, we dissect the ways in which violent extremist networks engage across alternative-technology and mainstream platforms according to the opportunities afforded by each type of platform. Developing a greater, more detailed understanding of the online VE landscape is imperative because of the extraordinary proliferation of VE activity online since the early 2000s. We primarily focus our research on ideologically motivated violent extremism (IMVE) but note the continued rise and impact of racially and ethnically motivated violent extremism (REMVE). The IMVE focus was adopted because of a growing tendency in English-language research to overemphasise REMVE trends following the U.S. domestic experience at the expense of the persistent and much larger global issues of terrorism and ideological violence.

Although this report notes that exploitation of the internet by violent extremists is as old as the technology itself, like broader social trends, it has become increasingly rare to see incidences of terrorism and VE that do not have a digital footprint. Furthermore, although violent extremists have continued to prioritise their exploitation of the internet in myriad ways to progress their

---

\(^1\) *Deplatforming* in the online context is the practice of denying a user access to a method of communication, or their platform, typically by banning the user from a website or social network or deleting or deleting their account on that platform.
causes, we observe that IMVE actors generally, and especially in the online space, have been adapting to and adopting the evolving technological landscape in sophisticated ways. This research demonstrates that extremist use of online platforms is entering a new phase: the development of a thriving and resilient ecosystem as technological innovation meets behavioural adaptation.

Although there is agreement among the academic, policy and practitioner communities that online activity and online platforms significantly influence the changing nature of the modern VE landscape, there is not a clear picture of how that evolving ecosystem is being used and specifically how its contours are being exploited by violent extremists to maintain influence and connectivity in ways that could be difficult to reverse.

This risk is heightened because of the nature of policy settings, which are fragmented internationally, from one legal jurisdiction to another, between platforms and even, at times, across the different servers of individual platforms. This challenge is even more stark when situated against the accelerating pace of technological innovation, including the emergence of decentralised and encrypted networks and enhanced use of the dark web, that combines with the increasingly entrepreneurial posture employed by violent extremists across an astonishingly broad tapestry of platforms. Continued elision of detailed analysis and understanding of these dynamics will likely have significant implications for problem-recognition, risk-mitigation, devising counteractions and appropriate policy development.

Approach

In this report, we seek to understand and interrogate the dynamics of online VE ecosystems; particularly those areas that have evaded scrutiny and afforded violent extremists the space to pursue a variety of extremist ends. Through a comprehensive literature review, we highlight key research questions, gaps in the existing knowledge base and emerging trends. Layered onto this macro picture, we identify and analyse violent extremist accounts and networks and conduct a virtual ethnographic analysis to better understand real-world patterns and typologies of behaviour.

Drawing this mixed-methods approach together, we address the fundamental question: How do violent extremists behave online, and how is that behaviour changing? To better understand this spectrum of behaviour, we develop a ‘Five-Stage Engagement Model’ that illustrates such behaviours as generic online consumption that has the potential inclusion of extremist content; prioritisation of extremist content, risk mitigation and clarity of extremist identity; and focused VE content generation and dissemination. The purpose of this model, shown in Figure S.1, is to illustrate the interplay between government policy instruments that can be applied to negate, counter, or contest VE activities and violent extremists’ behavioural adaptations in response to those instruments. In addition to providing a useful analytical framework, this model will support more nuanced and targeted counterterrorism (CT) and countering violent extremism (CVE) interventions and appropriate and responsive policy development. It is anticipated that the practical application of this model and framework will be explored further in a future research project.
**Figure S.1. Five-Stage Engagement Model: From User to Violent Extremism Campaigner**

<table>
<thead>
<tr>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
<th>Stage 4</th>
<th>Stage 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic online consumption which includes extremist content</td>
<td>Filtration of content to construct an ideologically informed ecosystem</td>
<td>Prioritisation of extremist content and most to brand-specific consumption</td>
<td>Growth of user role, activity and reputation</td>
<td>Pivot to content generation, translation and focused dissemination</td>
</tr>
<tr>
<td>Unfocused transmission of extremist content to peers</td>
<td>Online footprint increasingly influence by extremism</td>
<td>Risk awareness and mitigation – use of VPNs, TOR, encrypted platforms, accounts etc.</td>
<td>Continued consumption and active promotion of extremist content</td>
<td>Facilitation and recruitment activity</td>
</tr>
<tr>
<td>Limited actor ability to distinguish gradation of content and different extremist brands</td>
<td>Signs of ideological identity solidifying</td>
<td>Clarity of extremist identity</td>
<td>Defensive posture towards extremist brand and refutation of ‘others’</td>
<td>Potential connectivity to brand seniors, real world actors including in conflict zones</td>
</tr>
<tr>
<td>Growing awareness of risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: VPNs = virtual private networks; TOR = The Onion Router.

**Key Findings**

- Technological advancement, the ubiquity of the internet and the growth of online VE activity change much about the dynamics of the extremist landscape and the ways in which extremism is both encountered and countered. Against this backdrop, VE must be recognised as existing as multiple complex ecosystems, and consequently countered as such.
- These VE ecosystems transcend platforms and have existed for decades. They are widely accessible and host content that continues to be curated in a sophisticated manner despite deplatforming measures and users at varying levels of extremism can engage with them.
- The five-stage engagement model illustrates the means that VE campaigners use to spread VE content and pull users and actors into spaces where campaigners can reach, influence, cultivate, recruit and deploy users more easily. VE campaigners must inhabit each of these different stages simultaneously and maintain access to all other parts of their network, organisational and broader movement content, and diverse and broad audiences that depend on their specific role. Simultaneously, the model identifies the area in which a user might transition from passive consumer to active participant. This area might not be accessible or vulnerable to the current variety of counters being deployed to combat VE.
- Through the detailed thematic analysis of an expansive dataset of primary VE content, at least four distinct yet diverse patterns of behaviour can be distilled, and these behaviours are practised in different ways and at different levels across the engagement model. They form aggregate responses to or emerge from external and internal pressures.

**Recommendations**

The following six recommendations emerge from our exploration and analysis:
1. **Undertake further examination of the behaviours by VE actors in the online world.** The five-stage engagement model and behavioural typology developed present a useful starting point from which we can begin to better explore violent extremist behaviour online. As discussed in the report, if engagement in VE is associated with an immersive psychological state, then it could be investigated as a progression of antecedents, attributes and outcomes to understand the influence this has on their involvement in VE. The idea of progression sits well with the progressive stages shown in the engagement model developed here, thus investigation into the prevalence of specific antecedents and attributes exhibited through stages of engagement would be useful.

2. **Extend and test the typology of online behaviours to better understand how they change relative to observed ecosystem behaviour.** If we are to understand the problem as an ecosystem, we need to examine the behaviour exhibited by the entire system. This system behaviour might be characterised by ebbs and flows, which would be consistent with other observations made of terrorist activity. The typology of online behaviours developed here represents only a small window of VE activity. Whether this window sits within an ebb or flow has not been determined and what impact that has on the behaviour of the VE within that system at that time is unknown. This issue is separate from the sophisticated tools, tactics, techniques and procedures that violent extremists have developed.

3. **Identify minimum viable capabilities to maintain vigilance around evolving online VE, including consideration of policy and technology infrastructure.** Once we better understand the problem, the next step is to recognise that how we respond to, counter and inhibit it as an ecosystem (in its entirety online and offline) requires a fundamentally different approach to that currently being practiced, which is largely focused on the manifestations of the system (e.g. content on platforms, the targeting of individuals). This approach must be complemented or perhaps superseded by one that recognises the behaviour of the system as a whole and at all times. Fundamentally, this approach would entail understanding what is occurring during the peaks and the troughs of VE activity and ensuring that decisionmaking is informed by constant engagement with the VE ecosystem. We recognise that doing so would be a challenge from a resource perspective and in the face of other emerging priorities, but new ways of managing this challenge are needed to remain alert to the actions of violent extremists.

4. **Review existing analytical approaches to better understand VE operational cycles.** If the focus is on the entire problem, then counters must similarly extend beyond how a person enters or exits the system. Governments tend to focus more on the physical manifestations of the system by pivoting policy in response to a violent act; this approach is no longer sufficient. As we will explore in this report, deplatforming has had a profound impact in terms of creating space for disruptive alternative-technology platforms, including highly encrypted ones, to emerge and compete for audiences, including violent extremists, who have been removed from mainstream platforms. Violent extremists are clearly adapting their behaviours to circumvent deplatforming policies, evade law enforcement and become first movers who are highly incentivised to tailor, obfuscate and exploit the online environment according to societal and political shifts and technological advancements. Ebbs in VE activity might represent even more risk than the flows that naturally attract much more of these preventive or punitive counters. Governments could focus on addressing factors that might prompt people to join an ecosystem rather than addressing the outcomes of participation in that ecosystem. But these issues are long-standing and socioeconomic and could take many years and heavy investment to be addressed. Thus, a gap appears between these measures where the threat exists and might be most dangerous before it becomes more evident. This gap
suggests that it might be necessary to think *counter cyclically*, or counter to what apparent trends indicate and governmental policy dictates, to better understand the operational planning cycles of violent extremists. As a first step towards unpacking these ideas, we make this recommendation noting that there is advantage to be rendered from each analytical approach that emerges from a variety of sources. Collectively they might offer more detailed insight into the gaps than they do individually.

5. **Map REMVE ecosystems against a variety of IMVE systems to determine their relative maturity and identify the likely trajectories along which REMVE systems might progress.** Reviewing existing analytical approaches leads us to consider how to directly leverage the research findings of our focus on IMVE to apply them to REMVE, which is an area of increasing concern in English-language-speaking environments. As shown in this report, IMVE virtual ecosystems have evolved through sophisticated adoption and adaption of technology and online behaviours. This evolution might partially be a response to the relentless pursuit of IMVE actors and campaigners after the 11 September 2001 terrorist attacks. Nevertheless, examination of this evolution renders a much more advanced understanding of how other VE ecosystems might also evolve. As policymakers and practitioners, we must therefore learn to understand how both situations are simultaneously true and how each feeds off and learns from the other. Analytical approaches to IMVE might have implications for REMVE, the ecosystem which is relatively immature in terms of how actors within it exploit digital technology and the online world. By leveraging knowledge of IMVE actors, it might be possible to build better responses to the REMVE ecosystem as it is likely to evolve because of the attention that REMVE currently attracts from governments.

6. **Encourage collaboration between disparate groups across the national security landscape to improve situational awareness.** As a priority, the interplay and overlaps between terrorism, extremism, foreign interference and misinformation and disinformation should be investigated. Beyond linking different VE ecosystems, governments should recognise that VE does not occur separately from other events and issues. Just as governments are increasingly looking at how to better manage the concurrence of events in other areas (for example, between disaster management, national resilience and democracy), they might need to better understand, for example, any interplay between terrorism and extremism (non-state-based action) with foreign interference (state-based action), particularly because the online world presents opportunities for these lines to blur.

**Conclusion**

VE online is increasingly characterised by the exploitation and manipulation of online and offline systems, the ability to maintain influence and connectivity in sophisticated ways and a complex and inextricable interface with broader national security issues. The gamut of stakeholders involved in CVE will need to recognise the requisite capacity for addressing this multifaceted and dynamic landscape and the need to prioritise efforts and resourcing. Situational awareness is required across a spectrum of interrelated areas rather than pivoting focus only to the current priority. Although the ebb of VE might represent a lesser physical threat than the

---

flow, it provides an opportunity to build resilience, better understand how an event might arise, develop warning times, and plan and prepare for terrorist shocks. There should be incentive to pursue these ends because the VE ecosystem represents a danger that has the potential to threaten society.
Contents

Chapter 1. Introduction ...................................................................................................................... 1
Definitional Ambiguity ...................................................................................................................... 2
Ideologically Motivated Violent Extremism .................................................................................... 2
Racially or Ethnically Motivated Violent Extremism ...................................................................... 3
Ideologically Motivated Violent Extremism Continues to Be the Largest and Most Pervasive Problem ............................................................................................................................................... 5
Organisation of This Report ............................................................................................................. 5

Chapter 2. Identifying the Problem ................................................................................................. 8

Chapter 3. Violent Extremism Online: The Evolution of a Growing Challenge .............................. 14
Different Forms of Violent Extremism ............................................................................................ 16
Salafi-Jihadism Online: Evolution, Adaptation, Websites and Forums ........................................... 17
Social Media ........................................................................................................................................ 21
From Twitter to Telegram ................................................................................................................ 24
The Decentralised Web and Dark Web: Game Changers for Violent Extremism? ........................ 26

Chapter 4. Catalysing the Transition ............................................................................................... 30
Grasping Complexity: Ethnographic Insights, Ethics and Method .................................................. 30
Disaggregating Violent Extremist Behaviours and Building a Typology ........................................ 33
Obfuscation ......................................................................................................................................... 34
Security and Platform Selection ...................................................................................................... 37
Network Linking .............................................................................................................................. 39
Content Engagement ....................................................................................................................... 43

Chapter 5. The Engagement Model ................................................................................................. 46
Antecedents ........................................................................................................................................ 47
Attributes .......................................................................................................................................... 48
Outcomes .......................................................................................................................................... 48
Counters ........................................................................................................................................... 50

Chapter 6. Implications for Policy and Practice ............................................................................ 52
The Violent Extremism Ecosystem Is a Significant Threat ............................................................. 52
There Is a Heightened Need for Capacity, Expertise and Situational Awareness......................... 54
Counters Must Be Consistent with the Threat ................................................................................ 55
The Relative Immaturity of Racially or Ethnically Motivated Violent Extremists Could Be Exploited ............................................................................................................................................... 56
A Grand Strategy for National Security Might Be Required ......................................................... 56
Conclusion ......................................................................................................................................... 57

Appendix. Case Studies: Buffalo and Bratislava ............................................................................ 58
Abbreviations .................................................................................................................................... 60
References .......................................................................................................................................... 61
Figures

Figure S.1. Five-Stage Engagement Model: From User to Violent Extremism Campaigner ........ vi
Figure 2.1. Example of an Influence Diagram Highlighting Factors Driving the Transition of Nonactors to Actors ................................................................................................................................. 12
Figure 3.1. Example of an al-Uyayri Text Being Distributed via Telegram in November 2022 .... 19
Figure 3.2. Issue 1 in November 2006 and Issue 2 in February 2007 of the Technical Mujahid Magazine .................................................................................................................................................. 21
Figure 3.3. al Qaeda Supporter Tweets in Response to the April 2013 Boston Marathon Bombing .................................................................................................................................................. 23
Figure 3.4. IS Campaigner Encourages Supporters to Expand Media Operations to Twitter .... 24
Figure 3.5. Prominent al Qaeda and IS Bots on Telegram in December 2022 .......................... 25
Figure 3.6. I’lam Media on the Dark Web ................................................................................... 29
Figure 4.1. Conceptualising the Overlaps in Violent Extremist Behavioural Patterns ............... 34
Figure 4.2. Examples of Textual Obfuscation .............................................................................. 35
Figure 4.3. Examples of Visual Obfuscation ............................................................................... 36
Figure 4.4. Creation of Misleading Profiles ............................................................................... 36
Figure 4.5. Examples of Language-Based Obfuscation ............................................................... 37
Figure 4.6. ChirpWire Accounts for al Qaeda and Taliban Affiliated Networks ....................... 38
Figure 4.7. Australian National Socialist Network on Telegram and Gab .................................. 38
Figure 4.8. An Example of Linking Across Different Platforms .................................................. 39
Figure 4.9. Examples of Platform Selection Driven by Security Requirements .......................... 39
Figure 4.10. Examples of Network Linking Within the Same Platform .................................... 41
Figure 4.11. Network Linking Between Platforms That Have Different Governance Standards ................................................................................................................................. 42
Figure 4.12. Linking English-Language Islamic State Content Across Platforms ...................... 42
Figure 4.13. A Twitter Account Linking to a Telegram-Based Self-Described News Channel .... 42
Figure 4.14. Examples of Content Posted Across Multiple Platforms ....................................... 43
Figure 4.15. High-Frequency Reposting ..................................................................................... 44
Figure 4.16. Repurposing Mainstream Content to Support VE .................................................. 44
Figure 4.17. An Example of Security Measures to Mitigate Exploitation by Violent Extremists .................................................................................................................................................. 45
Figure 5.1. Five-Stage Engagement Model: From User to Violent Extremism Campaigner ....... 47
Figure 5.2. Bell-Shaped Distribution of ‘Unchecked’ Campaigner Activity ................................. 51
Chapter 1. Introduction

The al Qaeda attacks of 11 September 2001 prompted reexamination of terrorism in the 21st century. The October 2002 Bali attacks brought those issues into much sharper focus for Australia. Terrorism remains a persistent and ever-changing threat and among the highest national security risks for Australia. Even in the context of policy issues that might appear unrelated, such as the coronavirus 2019 global pandemic response, the threat of terrorism is pervasive. Although counterterrorism efforts were scaled back to enable the government to focus on responding to the pandemic, recent research has shown that some groups sought to ‘weaponize and exploit the pandemic, to use it as a means of spreading their extremist ideologies and to radicalize others to their causes.’\(^3\) Similar to many other areas, the pandemic brought the perceived risks associated with the prevalence of online violent extremism (VE) activity into the spotlight, but concerns regarding the role that the digital world plays in VE have existed for much longer.

The 2017 launch of the Global Internet Forum to Counter Terrorism by Facebook, Microsoft, Twitter and YouTube, and the United Nations–backed Tech Against Terrorism initiative, emerged following significant public and political pressure to challenge the rise of virtual caliphate of the Islamic State (IS) across a variety of mainstream social media platforms.\(^4\) More recently, in October 2022, the Delhi Declaration, which resulted from the United Nations Counter Terrorism Committee Emerging Technology special meeting, professed palpable concern regarding ‘the increased use, in a globalized society, by terrorists and their supporters of Internet and other information and communications technologies, including social media platforms, for terrorist purposes, such as for recruitment and incitement to commit terrorist acts, as well as for the financing, planning, and preparation of their activities.’\(^5\) There was a recognised need to act cooperatively to prevent and counter the use of new information and communications technologies, and other emerging technologies, for terrorist purposes, including recruitment and incitement to commit terrorist acts, as well as the financing, planning and preparation of their activities and stresses the importance of cooperation with civil society and the private sector in this endeavour.\(^6\)

Exploitation of the internet by violent extremists is almost as old as the technology itself. Like other broader social trends, it has become rare to see incidences of terrorism and VE that do

---

5 Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes, United Nations Counterterrorism Community, 29 October 2022, p. 1.
6 Delhi Declaration, 2022, p. 2.
not have a digital footprint. Violent extremists increasingly prioritise exploitation of the internet in different ways to progress their causes and have become proficient in the adoption and adaptation of every emerging online platform they can access. But how much is really known about the mechanics and dynamics of VE online? Are the behaviours associated with VE online the same as those associated with VE offline? What is the relationship between online and offline activities? Does radicalisation occur in the same way? Moreover, do we need to understand VE online on its own terms? This understanding is critical to the pursuit of effective countermeasures.

**Definitional Ambiguity**

Definitions or descriptors abound in relation to terrorism, VE and VE online. Although we primarily examine the way in which VE online is developing and investigated, we are cognisant that such online activity can also manifest in the physical world. To this end, we considered various perspectives before selecting the definitions used in this report. We present our rationale for this in the following sections to inform the reader of the definitions used, context for our research and our justification for our predominant focus on what we define as ideologically motivated violent extremism (IMVE) as opposed to religiously motivated violent extremism (RMVE).

**Ideologically Motivated Violent Extremism**

We chose IMVE to encompass the most prevalent form of terrorism, which, according to the Institute for Economics and Peace’s 2022 Global Terrorism Index (GTI), results from Islamist extremism or Islamic militancy. It is noted that in the West, and specifically in Australia, this is denoted as RMVE. However, this phrasing appears to be driven by a Western experience of such terrorism, which has constituted only a very small fraction of the global terrorism that has occurred since around 2007. In countries that have large Muslim populations, such as Indonesia and the Philippines, Islamist extremism and terrorism is described in ideological terms.

---


8 Although we have distinguished between IMVE and REMVE in this report, VE might also be separated into centrally organised VE and self-initiated VE. For example, a centrally organised group such as IS will use social media differently than would locally based groups with less experience and more need for experimentation. This dynamic might extend to identification of differences between organisations that have media wings and those that have only individual supporters. Although we have not been able to pursue this analysis, the posited deconstruction might offer additional useful insights.


10 According to the 2022 GTI, ‘[b]etween 2007 and 2021 there were 126,740 deaths from terrorism globally. Of these, 865 occurred in the West, or just 0.68 per cent of the total.’ Of these 865 fatalities, only 61 per cent were a result of what are characterised in the West as religious attacks. Institute for Economics and Peace, 2022, p. 32.
rather than in religious terms.\textsuperscript{11} Although Shawcross, in the 2023 United Kingdom (UK) Prevent Review, advises that ‘officials [should] not interpret religion and ideology as interchangeable or mutually exclusive’, he does state that misconceptions or inaccurate assessments can be made if it is assumed that ideological motivation is equated with deep religious understanding.\textsuperscript{12}

A final point of note is that the work presented in this report was sponsored by the Office of the Ambassador for Counter-Terrorism (OCT) within the Department of Foreign Affairs and Trade (DFAT), with the intent that the outcomes of the research would contribute to the undertakings of the OCT in establishing a first-rate network between Australia and its international partners. We aim to be sensitive to the issues of how Islamist terrorism and VE are described outside Australia, with the knowledge that the primary target audience for the work are our international partners, not necessarily an Australian audience. We believe that the definition of IMVE we have adopted in this report is the most appropriate, even if it is inconsistent with current terminology used in Australia.

**Racially or Ethnically Motivated Violent Extremism**

In the West, the definition that is used most often to describe local VE that is motivated by a variety of political ideologies is IMVE. However, because this type of VE is increasingly perpetrated by networks with no clear organisational affiliation, we believe that REMVE,\textsuperscript{13} which refers to racially or ethnically motivated violent extremism, is a more suitable term in the context of this report.\textsuperscript{14} REMVE can draw from racist, anti-Semitic, xenophobic, Islamophobic, misogynistic and homophobic influences and ideologies in addition to far-right extremism, right-wing terrorism, radical right ideologies and extreme right or extreme left ideologies. This type of VE is increasingly prevalent in the West and is of growing concern in Australia.

The 15 March 2019 Christchurch terrorist attack ‘mainstreamed [such] concerns.’\textsuperscript{15} These concerns intensified following the 6 January 2021 riot at the U.S. Capitol. A 2022 RAND report states that REMVEs present some of the most pressing threats to the United States. REMVE also has been identified as the White Identity Terrorist Movement (WITM). REMVEs are among the most lethal domestic violent extremists, and they are the most likely to commit mass-casualty attacks. These movements are characterized by a broad


\textsuperscript{13} In the UK and Europe, violent right-wing extremism (VRWE) or right-wing terrorism (RWT) are the preferred terms and abbreviations.


\textsuperscript{15} Maura Conway, Ryan Scrivens and Logan Macnair, Right-Wing Extremists’ Persistent Online Presence: History and Contemporary Trends, International Centre for Counter-Terrorism, October 2019, p. 2.
ideological orientation toward xenophobic, anti-Semitic, racist, and misogynistic sentiment.\textsuperscript{16}

Williams et al. reviewed the relevant literature on REMVE networks and collected and analysed social media data from six social networks (Twitter, Reddit, Gab, Ruqqus, Telegram, and Stormfront) to produce a global network map of the digital REMVE space.\textsuperscript{17} Research results in this report clearly show the dominance of REMVE activity in the United States; more than 60 per cent of Twitter users sampled were located in the United States. The second-highest number of users came from the UK, although UK users made up less than 10 per cent of the total population.\textsuperscript{18} This same research shows that there are many Twitter communities distributed globally, but as the report itself highlights, this distribution is overshadowed by three large communities located in the United States.\textsuperscript{19}

\textit{Western Exceptionalism Versus Trends in Global Terrorism}

We observe that, although online VE does not recognise national borders or language distinctions, there is a constituent risk that we apply a domestic and local framing of the problem to a global landscape.\textsuperscript{20} That is to say, the REMVE trends observed in the West and especially in the United States are generally emphasised at the expense of the persistent and much larger global issues of terrorism or ideological violence. Coming full circle, this argument could also be applied to the preferences of IMVE and RMVE definitions in the West versus REMVE and IMVE, respectively, on a global stage.

Outside the United States, this exceptionalism is being acknowledged and discussed more after some initial swings in effort towards understanding and engaging emergent REMVE activity. For example, in his 2022 Annual Threat update, the MI5 Director General stated that, for the UK, ‘Islamist Terrorism remains the larger problem—about three quarters of our terrorist caseload . . . the other quarter of our counter-terrorist caseload: Extreme Right-Wing Terrorism.’\textsuperscript{21} Shawcross, in his 2023 Prevent Review, stated that ‘Islamist terrorism is currently the largest terrorist threat facing the United Kingdom. In the years since the 2017 Westminster Bridge attack, the vast majority of realised and foiled plots have been Islamist in nature. At present, 80% of the Counter Terrorism Police network’s live investigations are Islamist while 10% are Extreme Right-Wing.’\textsuperscript{22}

\begin{enumerate}
\item Williams et al., 2022.
\item Williams et al., 2022.
\item Williams et al., 2022, p. 45.
\item Williams et al., 2022, p. 46.
\item See, for example, Williams et al., 2022, p. 46. A variety of countries are involved in VE discourse on Twitter.
\item MI5, ‘Director General Ken McCallum Gives Annual Threat Update’, webpage, 16 November 2022.
\item Shawcross, 2023, p. 14.
\end{enumerate}
Ideologically Motivated Violent Extremism Continues to Be the Largest and Most Pervasive Problem

The GTI 2022 reports that ‘[t]errorism in the West represents only a fraction of total terrorism globally’ and is ‘notable because it occurs almost entirely outside the context of an ongoing conflict or war.’\(^{23}\) Outside the West, the GTI links ongoing intensity of ideologically motivated terrorism with the presence of significant conflict. It has been reported that ‘all of the ten countries most impacted by terrorism in 2021 were involved in an armed conflict in the preceding year. Four of those, Afghanistan, Nigeria, Somalia, and Syria, had conflicts that resulted in over 1,000 deaths in a calendar year.’\(^{24}\)

Against this backdrop, it should come as no surprise that ideologically motivated terrorist groups, and their supportive violent extremist networks, have wide and organised reach across the digital landscape. Despite online counters and deplatforming measures, these networks continue to flourish. The flourishing of these networks is even more noteworthy considering the expansive military campaigns that have also been waged against them over a significant period of time. This dual-pincer movement of online and offline pressure over a sustained period and at the local and global levels has meant that the IMVE online landscape has developed differently than the landscape of REMVE in the West.

Largely because of the constitutional protections around freedom of speech in the United States and diffuse ideological trend lines that can blur with mainstream culture, many REMVE online platforms and ecosystems remain more or less unchallenged. Thus, because ‘[t]he global REMVE network on social media is largely U.S.-created and -fuelled,’\(^{25}\) platforms and networks are not only easy to access, but, in aggregate, because of the lack of action by the platforms to manage this content, and despite persistent calls to do so, there has been less need for innovation and adaptation by actors promoting REMVE views.\(^{26}\)

We assert that, because of the interplay between the long-term pursuit of IMVE actors and campaigners and their corresponding efforts to avoid capture or scrutiny, examination of IMVE virtual ecosystems renders a much more advanced understanding of how VE ecosystems have evolved. In this report, therefore, we purposefully focus out analysis on the IMVE threat that continues to be the largest and most pervasive problem in the online VE landscape.

Organisation of This Report

This report unfolds in five additional chapters.

In Chapter 2, we identify the nature of the problem of VE and propose that we have reached an inflection point in the evolution of VE. Technological advancement, the ubiquity of the internet and the growth of online VE activity have significantly changed the dynamics of the

\(^{23}\) Institute for Economics and Peace, 2022, p. 32.
\(^{24}\) Institute for Economics and Peace, 2022, p. 60.
\(^{25}\) Williams et al., 2022, p. ix.
\(^{26}\) For a history of REMVE interplay with the internet, see Conway, Scrivens and Macnair, 2019.
extremist landscape and the ways in which extremism is both encountered and countered. Here, we suggest that to better describe and understand the complexities inherent to this online VE problem, and to illustrate the dynamic and evolutionary nature of the landscape, it is necessary to conceptualise the VE landscape as an ecosystem.

In Chapter 3, we examine the evolution of VE online. Specifically, we examine the ways that violent extremists have exploited technologies that enable effective and comprehensive dissemination of the material and ideas that resonate with supporters and attract new adherents. In this chapter, we demonstrate how violent extremists are incentivised to adapt their online behaviours as new technologies and platforms emerge. The nature and degree of technology and platform use and engagement is observed to vary as they attempt to navigate and circumvent counteraction efforts. We also demonstrate how violent extremists capitalise on the dynamics that new technologies and platforms can facilitate.

For Chapters 2 and 3, a broad and diverse literature was accessed and analysed. One of the early findings from this analysis was a recognition of the ways in which subject-matter experts from different backgrounds engage with issues according to their organisational requirements and culture. For example, the issue is approached rather differently by a researcher who works in academia or for a think tank, a government department or the tech sector. Even this categorisation oversimplifies the variety of actors engaging and researching within this space. This dynamic creates a challenge in understanding the interplay of subject-matter experts and the issues that they are focused on; this challenge is compounded by the pace of technology change in the digital world. As a result, different partners who are engaged in understanding VE view different parts of the ecosystem or examine the same part but arrive at different conclusions. These are all valid conclusions that are situated in the context the unique requirements of the different partners.

Compounding this issue further is that most of the subsequent analysis and development of policy response or countermeasures undertaken or applied by subject-matter experts often occurs postevent and, in some cases, using open-source, unclassified incident reporting that might not disclose all the nuances of an event. It is at this stage of analysis that the pace of technology change and the speed at which the online VE ecosystem adopts and adapts affects the effectiveness of all this work. These insights aside, the literature that we examined offers the reader a useful list of research regarding online VE and CVE strategies to interrogate in the context of their own requirements.

In Chapter 4, we look at how VE campaigners use increasingly sophisticated means to disseminate VE content and pull users and actors into spaces where campaigners can more easily engage in cultivation and recruitment. To better understand this complex ecosystem, we undertook a granular virtual ethnography of VE landscapes that illustrated the presence of multiple VE ecosystems that transcend platforms and engage with users at varying levels of extremism.

In Chapter 5, we distil the knowledge gained from this ethnographic approach into a five-stage engagement model. While the model is simple in its two-dimensional representation, it offers nuanced insights by disaggregating key aspects of violent extremist behaviour online.
model is therefore useful in terms of improving analysis, identifying gaps in the interplay of current counters across the VE landscape and in suggesting the need for further detailed research.

In Chapter 6, we consider some of the implications of our findings for policy and practice. We suggest that to understand, respond to, counter, and inhibit an ecosystem (in its entirety online and offline) stakeholders must move beyond responding to manifestations of the system (content on platforms or the targeting of individuals) to an approach that recognises the behaviour of the entire system. We list a variety of recommendations with the intention to provoke discussion, collaboration and further research within the broad community examining the VE space.

Additionally, in an appendix, we explore two case studies of incidents of VE in Buffalo, New York, and Bratislava, Slovakia.
Chapter 2. Identifying the Problem

Winter et al. argue that one of the ‘greatest challenges’ in understanding and countering online VE is ‘the rapidly changing technological landscape.’ The authors continue, ‘[r]esearch conducted today will likely have been overtaken by technical developments by the time it is published in two or three years. As a result, researchers must ask themselves which questions they can most meaningfully study in this context, and how they can better cooperate with practitioners, particularly in the field of technology.’

The international security community has reached a point of inflection in how we might seek to counter VE given its evolution. Although VE actors have long capitalised on emerging technologies and the internet, specifically, there is increased cross-platform exploitation of online opportunity and innovative violent extremist behavioural adaptation to the extent that it has resulted in resilient VE ecosystems. Technological advancement, the ubiquity of the internet, and the growth of online VE activity change much about the dynamics of the extremist landscape and the ways in which extremism is both encountered and countered. As reported in Evans and Williams, the ‘internet has been a haven for extremists since long before most people even knew it existed’, but in recent years, online VE has proliferated to such a degree that researchers are having to rethink, the contours of VE with the dominating vector of being online.

An understanding of VE must be situated not only against changing sociopolitical contexts, but also against the accelerating pace of technological innovation, including the emergence of decentralised and encrypted networks and enhanced use of the dark web that combine with the increasingly entrepreneurial posture employed by violent extremists across an astonishingly broad tapestry of platforms. These definitional and conceptual challenges are compounded by the various actors who engage in and around the online space, and the resulting disaggregated datasets.

To understand this landscape, we need to better grasp the interplay of such factors as

- **people:** those using the online space to act or campaign and their behaviour, ideology and motivation
- **processes:** how users engage with these spaces, why some users seek out such content or are pulled into the system and how they are managed by policies; processes will necessarily be linked to technology, given the online aspects of the problem
- **information:** the quality, quantity, sources and longevity of content
- **technology:** the increasing variety of platforms and applications, centralised and decentralised, encrypted or otherwise, on the clear and dark web.

---


Against the backdrop of technological change, this report generates fresh insight into the evolution of extremist online behaviours and focuses specifically on the problem of the transition of a nonactor to VE actor. VE campaigners seek to pull nonactors or users into their VE world and increasingly operate online to catalyse this transition. Campaigners and actors alike exploit technological developments within this online world as they manoeuvre against a variety of government policy instruments and private sector initiatives. Campaigners and actors exploit online and offline systems and maintain influence and connectivity in ways that might be very difficult to undo, and they do so well in advance of a violent act.

According to Micheron, ‘[t]o focus only on the attacks and their mournful toll, to make them the yardstick by which to calibrate militancy, is comparable to watching the last few minutes of a film to gauge its quality.’ He argues that what goes ‘under-analysed and under-represented in the public discourse is a jihadism that prevails between terrorist attacks.’ The violent act that can erupt or emerge without planning or notice must be understood as an element in a broader ecosystem. This ecosystem exists for many more reasons than as a mechanism through which acts of extreme violence are planned and coordinated.

For the most part, the activities of online violent extremists are not necessarily illegal and exploit gaps in governmental regulations or shortcomings in how companies manage VE content, which makes the development, evolution, or sustainment of problematic VE and terrorist operations possible. The violent dimension of extremism is the most visible and evident manifestation, and it represents only ‘the tip of an iceberg’ of terrorist activity. For example, an individual might be a member of a virtual violent extremist group or community (in other words, a group that espouses violent ideology and even violent ends) without becoming a violent actor or initiating a violent act themself.

29 Terms placed in italics in this paragraph are done so for the purpose of highlighting their use in the influence diagram in Figure 2.1, which is discussed later in this chapter.
32 Clifford, 2021, p. 86.

Horgan notes that, for terrorism (and VE), there is ‘a complex process of accommodation and assimilation across incrementally experienced stages.’ He argues that there are many features that tend to be largely underappreciated, such as ‘the gradual nature of the relevant socialization processes’, the myriad ‘supportive qualities associated with that recruitment (e.g. the ‘pull’ factors, or lures, that attract people to either involvement in terrorism in a broad sense or that are used to groom potential recruits)’, and the subtleties associated with ‘migration between roles (e.g. moving from fringe activity such as public protest to illegal, focused behavior).’ John Horgan, ‘From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalization into Terrorism’, *Annals of the American Academy of Political and Social Science*, Vol. 618, No. 1, July 2008, p. 84.
understanding and modelling ‘the trajectories of individuals in relation to both their attitudes and behaviors’, Khalil, Horgan and Zeuthen point out that ‘those who sympathize with ideologically justified violence very often remain uninvolved in its production, instead electing to ‘free-ride’ on the actions of others.’ But a reduction in high-profile attacks does not equate to diminished resolve or activity, nor does it mean that such nonviolent action does not contribute to eventual violence. As Micheron argues, ‘[t]he ideas that sparked the movement can continue to proliferate as long as the conditions for their dissemination are still in place and their supporters still have the capacity to act.’

Shawcross makes a similar point in his report by highlighting the lack of scrutiny of wider Islamist movements as opposed to the detailed ongoing analysis of the violent groups such as IS and al Qaeda, which he argues ‘risks creating a blind spot to the influence of the wider ideological movement, including groups . . . who do not cross the terrorism threshold but nevertheless create a permissive environment from which terrorists can radicalise and recruit.’

The ecosystem that underpins and facilitates the gamut of extremist behaviours represents a significant threat and must be a primary consideration in the development of appropriate CVE policy.

Evans and Williams examine the degree to which the online world is significant in the catalysation of transition from nonactor to VE actor. They argue that ‘[t]he architecture of the internet is conducive for radicalizing users to adopt extremist ideas or behaviours, including incitement to violence’ and ‘provides potentially violent actors with new ways to acquire the training, knowledge, and motivation to conduct attacks without direct recruitment by formal extremist groups.’ The level of exposure to radical ideas has risen with the growth of the number of internet users and the popularization of message forums, social media networks, and other virtual communities. In turn, the percentage of the population that subscribes to radical ideologies is expected to increase—and some subset of that population will go so far as to use violence to promote their ideas.

---


It is also necessary to understand what makes extremist online activities violent. How violence is classified, and what it entails, as was detailed in a 2021 RAND report, does not occur in isolation but ‘comprises many different facets of a crime, including motivation of the perpetrator, the significance of their online presence, any known or emerging mental health issues, and the classifier’s own knowledge, experience, and possibly any resulting biases. Misclassification of an act of violence is a potential risk’ (Sarah Grand-Clément, Diana Dascalu, Ruth Harris and Ben Baruch, Classifying Acts of Violence: Understanding How Acts of Violence Are Classified by Subject Matter Experts, RAND Corporation, RR-A1220-1, 2021 p. 3).

Schmid analyses the idea that we should distinguish between not violent militancy and principled non-violent political manifestations. However, he ultimately argues that instead of ‘distinguishing between non-violent and violent extremists, we should distinguish between extremists and non-extremists and support the latter . . . ’ (Alex P. Schmid, Violent and Non-Violent Extremism: Two Sides of the Same Coin? International Centre for Counter-Terrorism, May 2014, p. 25).

35 Micheron, 2022, p. 5.

36 Shawcross, 2023, p. 19.

37 Evans and Williams, 2022, p. 13.
To better describe some of the complexities inherent to this online VE problem, and to illustrate the dynamic and evolutionary nature of the landscape, in this report we have adopted the term ecosystem. Our use of this term aligns with 2022 research, which concluded that although digital environments are not true ecological systems in the biological sense, delineating and defining conceptual components of an ecosystem may provide a shared conception when used to describe how extremist violence emerges from online environments, or when used to interpret these descriptions in a policy and practice setting.38

Consistent with the consideration of VE online as an ecosystem is that, within that ecosystem, there are complex sociotechnical systems that in turn ‘comprise interdependent resources of people, processes, information, and technology that must interact with each other and their environment in support of a common mission.’39 This concept is useful when examining the central process of transition with which we are concerned.

Our research delivers a greater understanding of how transition is catalysed and facilitated in the online space and how the ecosystem exists, behaves and is adapted, with a view to informing policy conversations and considerations of how to develop better and more-appropriate countermeasures against VE. Therefore, we have sought to depict the VE landscape, visualise its moving parts and contextualise the problem space: the transition from nonactor to VE actor. We have done this using system dynamics with the development of an influence diagram as shown in Figure 2.1.40 This model depicts four main groups: government bodies, users, actors and campaigners. We have used these descriptors in an attempt to delineate between individuals who consume VE content without becoming violent extremists (users at risk), violent extremists who operate independently to further their ideology (VE actors) and those who work in a highly motivated position within the rubric of violent extremist networks and groups to advance their cause (VE campaigners).

38 Jade Hutchinson, Julian Droogan, Lise Waldek and Brian Ballsun-Stanton, Violent Extremist and REMVE Online Ecosystems: Ecological Characteristics for Future Research and Conceptualization, Resolve Network, August 2022, p. 4.
39 This description has been adapted from the definition of an enterprise offered by Giachetti: ‘A complex, (adaptive) socio-technical system that comprises interdependent resources of people, processes, information, and technology that must interact with each other and their environment in support of a common mission’ (Ronald Giachetti, Design of Enterprise Systems, Theory, Architecture, and Methods, 1st ed., CRC Press, 2010).
40 This system dynamics model illustrates the push and pull factors at play over time. For a detailed description of these factors, see Ashley L. Rhoades and Todd C. Helmus, Countering Violent Extremism in the Philippines: A Snapshot of Current Challenges and Responses, RAND Corporation, RR-A233-2, 2020. Within the model, at one end long-term social policy initiatives seek to correct the endemic issues that push people to act. At the other end stronger preventative and punitive measures are applied to deter those users that are being pulled or enticed into violent extremist worlds. Those measures ensure that actors or potential actors are not only punished for their crimes but also that they know well the risks of acting on violent extremist views. These policy initiatives or countermeasures are applied to stymie actions and tactics of VE campaigners.
Figure 2.1. Example of an Influence Diagram Highlighting Factors Driving the Transition of Nonactors to Actors

Shown in the influence diagram are the known and well-practiced government counters of (1) social policy that targets those conditions that could push users into transition to actors and (2) punitive and preventative measures that are focused on those who have transitioned or might be considering transition to a more active VE role. The temporal differences between these counters, however, must be considered; the former is long-term and requires sustainment over many years while latter are much more urgent in their application. The differences or gap between these government policies might present an opportunity to introduce more counters that better aligned with the evolution of conditions in the online VE space. As Horgan describes

[i]n considering the nature of involvement in terrorism, we might begin to develop phase-specific counterterrorism initiatives, depending on what we can ascertain is the most effective intervention point: whether it be initial prevention of involvement, subsequent disruption of engagement, or eventual promotion of disengagement. Acknowledging these distinctions will allow for the development of unique kinds of interventions . . . 41

This idea is revisited later in the report, as we show how the online VE footprint consists of behaviours that comprehensively represent movement ideology. The growth of cross-platform subcultures, networks and ecosystems that seek to extrapolate advantage from the organisational offering of multiple platforms has made this easier. In short, the evolution of technology combined with entrepreneurial violent extremist networks have changed the landscape online VE. We are now seeing a meeting of technological innovation with violent extremist behavioural adaptation that is producing more-resilient ecosystems for VE. Against this, additional counters

41 Horgan, 2008, p. 93.
must be more aligned to the activities and tactics of VE campaigners. Although we do not pursue a review of the counters down to the platform level within this report, it is an area ripe for future analysis and, when considered alongside this research, is likely to provide new insights for the policy and practitioner communities.
Chapter 3. Violent Extremism Online: The Evolution of a Growing Challenge

The emergence of the internet and its deepening impact has transformed society to the extent that Hine describes the internet as ‘infrastructure that underpins the things that people do, rather than a foregrounded activity that they do in its own right.’ As technology has evolved and its use has expanded, the digital aspect of behaviour has become largely indistinguishable from other everyday activities, and this trend continues apace. For Hine, these ‘techno-social developments, in their various ways, promise to decrease the significance of any boundary that might be thought to exist between the digital and the everyday. Everyday life promises to be lived more and more through digital environments and represented in digital format.’

Against this backdrop, it is unsurprising that violent extremists are also adapting to technology in multiple ways. In 1982, Schmid and De Graaf stated that communication is central to the efforts of extremists. This idea has long been the sine non qua of extremist and terrorist operations. Forty years later, in 2022, Weimann, Berton and Samouris observed that ‘just like any other enterprise seeking to remain relevant in their respective field, terrorist groups of all ideological shades undergo different degrees of digital transformation. The online behaviour of users, expecting immediate access to digital content via multiple channels, has shaped the ways in which the media wings of terrorist groups create and share their propaganda.’

However, it can be argued that because of their unique circumstances and needs, violent extremists might have even more to gain from emergent technology. Over and above communication and propaganda, Conway notes that, ‘today’s Internet does not simply allow for the dissemination and consumption of ‘extremist material’ in a one-way broadcast from producer to consumer, but also high levels of online social interaction around this material.’

---

43 Hine, 2015, p. 192.
numerous examples in this report illustrate, it also enables VE actors to become impactful producers of content in new and innovative ways, which represents a significant departure from the traditional producer-consumer models of media.

This process of engagement—with content and with others—is at the centre of VE digital ecosystems. Violent extremists tend to be attracted to technologies that enable effective and comprehensive dissemination of material and ideas that resonate with existing supporters and attract new adherents. As a result, violent extremists have become expert at exploiting what Henry Jenkins has termed, ‘convergence culture,’ that is, ‘where old and new media intersect, where grassroots and corporate media collide, where the power of the media producer and the power of the consumer interact in unpredictable ways.’

Although the nature and degree of use and engagement varies, violent extremists are incentivised to adapt their online behaviours as new technologies and platforms emerge and as they attempt to navigate and circumvent counteraction efforts, and to capitalise on the dynamics that they can facilitate. These dynamics include the exploitation of the social implications of what we have come to know as *echo chambers*, which form when ‘people position themselves to hear similar voices to their own,’ The internet has arguably enabled this effect through its facilitation of ‘anonymous, fragmented communication.’ Lanier has argued, ‘[n]ew patterns of social connection that are unique to online culture have played a role in the spread of modern networked terrorism [and VE] . . . jihadi chat looks just like poodle chat.’

In many ways, violent extremists use online platforms in the same way as any other user does: to communicate, create networks, buy and sell goods, share and access information, foster communities and view entertainment. There is no discrete, separate or specialist means or mechanics for operating as a violent extremist online, and not all online activity conducted by violent extremists online is extreme. It is exploitation of an existing ecosystem; an evolving infrastructure. Much of this activity also occurs on mainstream platforms that host nonextremist content and might even maintain community terms of use that prohibit or restrict the sharing of extremist material.

This reality of ecosystem-wide opportunity and individual willingness to take risk has been widely understood by violent extremists since the emergence of digital technology. Williams et al. note that ‘[s]ince the early days of the internet, extremists have proven themselves to be effective adopters of social media technology as tools to create and disseminate material, attract

---

47 Scriven and Conway, 2019
and radicalize adherents, organize virtual and real-world activities and raise revenue, among other functions.⁵² Weimann observes that ‘[t]he growing presence of modern terrorism on the Internet is at the nexus of two key trends: the democratization of communications driven by user-generated content on the Internet, and the growing awareness of modern terrorists of the potential of using the Internet as a tool for their purposes. Thus, the Internet has long been a favourite tool of terrorists.’⁵³

**Different Forms of Violent Extremism**

Beyond these general observations, there are clearly discernible patterns of how governments—particularly their security, intelligence and law enforcement departments—think about and counter different forms of VE. We first consider current observed trends within REMVE and IMVE.

REMVE content has long maintained a relatively stable and unchallenged presence online compared with IMVE content that is associated with the Salafi-Jihadism of al Qaeda or IS. It is arguably the case that the intensity of the counters directed at the latter tapestry of ecosystems has encouraged innovation and adaptation and, as a result, created more sophisticated learning environments.

By contrast, REMVE ecosystems, in aggregate, have not needed to evolve in response to counters and official policy, despite the increasing recognition in the literature that, ‘Jihadists and right-wing extremists use remarkably similar social media strategies . . . [b]ut platforms have been more tentative in dealing with the kind of right-wing extremism that focuses on white supremacy.’⁵⁴ As a result of the 11 September 2001 attacks and their political aftershocks, much focus was placed on understanding the minutiae of al Qaeda, Salafi-Jihadism, and, subsequently, IS.

However, as discussed in Chapter 1, there appears to have been a pivot towards the detailed exploration of REMVE ecosystems.⁵⁵ This pivot comes as a result of a reported uptick in REMVE behaviour, particularly in the United States, although such trends have also been observed elsewhere. The Director-General of Security in Australia, in his 2021 Threat Assessment Update, reported that investigations into such extremism had grown from constituting one-third of the Australian Security Intelligence Organisation’s counterterrorism caseload to 40 per cent.⁵⁶

However, as we indicated in Chapter 1, we will explore online VE through the perspective of IMVE for the remainder of this chapter and our subsequent analysis. This perspective offers a

---

⁵² Williams et al., 2021, p. 2.
⁵⁵ To better understand this transition from a U.S. perspective, see Brian Michael Jenkins, ‘Elements of a Pragmatic Strategy to Counter Domestic Political Violence’, *CTC Sentinel*, Vol. 15, No. 10, October 2022. For a detailed assessment of the development of REMVE online, see Williams et al., 2021.
complementary view and avoids duplication of the research focused on REMVE. We also believe that there is much to be rendered for analysts and policymakers in understanding how radicalisation occurs online, which is an increasing trend, including among young Australians.\footnote{In his 2022 Annual Threat Assessment, the Director-General of Security described a continuing trend of radicalisation occurring online among young Australians embracing extremism (Australian Security Intelligence Organisation, 2021).}

Salafi-Jihadism Online: Evolution, Adaptation, Websites and Forums

Weimann notes that ‘[a]mong the earliest jihadist attempts to use the Internet was the establishment of Azzam.com in 1997 by a student at Imperial College, London.’\footnote{Weimann, 2015, pp. 90–91.} This website became a prominent feature of the English-language VE ecosystem and focused on conflicts across the Muslim world, such as those in Bosnia, Chechnya, Kashmir and Afghanistan. In the Arabic-language ecosystem, in which most online Salafi-Jihadist activity continues to manifest, significant developments can also be traced back to this period. At the level of official, organisationally driven VE activity, Weimann adds that al Qaeda’s online debut dates back to February 2000, with the creation of maalemaljihad.com. This website was followed in March 2001 by alneda.com, which was active through mid-July 2002. It was registered in Singapore and appeared on Web servers in Malaysia and Texas before it was taken down at the request of U.S. officials. It then changed its name and URL every few days, forced to move from server to server by citizens who complained to the Internet service providers (ISPs) that were hosting the sites . . . . In April 2003, al-Qaeda’s website re-emerged, this time named “Faroq,” and it waved the banner of alneda.com\footnote{Weimann, 2015, p. 97. See also Bruce Hoffman, ‘The Use of the Internet by Islamic Extremists’, testimony before the House Permanent Select Committee on Intelligence, RAND Corporation CT-262-1, 4 May 2006.}

These VE efforts, against the backdrop of early counters, are unsurprising given that the senior ideologically motivated violent extremists recognised the importance of this new infrastructure. This perspective was reflected in a June 2002 letter from Osama bin Laden to then–Taliban leader Mullah Umar in which he discussed the situation in Afghanistan, continuation of jihad in the Central Asian Islamic Republics and the situation in the Arabian Peninsula. In this correspondence, bin Laden stressed that the ‘media war in this century is one of the strongest methods; in fact, its ratio may reach 90 percent of the total preparation for the battles.’\footnote{Osama bin Laden, letter to Mullah Mohammed ‘Omar, trans., 5 June 2002.} This point of emphasis was picked up by Jenkins, who argued that ‘[w]hile almost all terrorist organisations have websites, al Qaeda is the first to fully exploit the Internet. This reflects al Qaeda’s unique characteristics. It regards itself as a global movement . . . . Its leaders view communication as 90 percent of the struggle.’\footnote{Brian Michael Jenkins, ‘Is Al Qaeda's Internet Strategy Working?’ testimony before the House Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, RAND Corporation, CT-371, 6 December 2011.} With regards to al Qaeda, Hoffman suggests that ‘its leadership seems to have intuitively grasped the enormous communicative potential of the

\[\text{\textsuperscript{57}}\text{In his 2022 Annual Threat Assessment, the Director-General of Security described a continuing trend of radicalisation occurring online among young Australians embracing extremism (Australian Security Intelligence Organisation, 2021).}\]
\[\text{\textsuperscript{58}}\text{Weimann, 2015, pp. 90–91.}\]
\[\text{\textsuperscript{59}}\text{Weimann, 2015, p. 97. See also Bruce Hoffman, ‘The Use of the Internet by Islamic Extremists’, testimony before the House Permanent Select Committee on Intelligence, RAND Corporation CT-262-1, 4 May 2006.}\]
\[\text{\textsuperscript{60}}\text{Osama bin Laden, letter to Mullah Mohammed ‘Omar, trans., 5 June 2002.}\]
\[\text{\textsuperscript{61}}\text{Brian Michael Jenkins, ‘Is Al Qaeda's Internet Strategy Working?’ testimony before the House Homeland Security Committee, Subcommittee on Counterterrorism and Intelligence, RAND Corporation, CT-371, 6 December 2011.}\]
Internet and sought to harness this power both to further the movement’s strategic aims and facilitate its tactical operations. Indeed, for bin Laden and his followers the weapons of terrorism are no longer simply the guns and bombs that they always have been, but now include the mini-cam and videotape, editing suite and attendant production facilities; professionally produced and mass-marketed CD-ROMs and DVDs; and, most critically, the laptop and desk-top computers, CD burners and e-mail accounts, and Internet and worldwide web access that have defined the information revolution today.

In short, as technology has developed, the opportunity that it offers to such groups as al Qaeda has expanded.

Outside al Qaeda’s leadership core, the focus on new technology has also permeated the operational model of the Saudi Arabia–based al Qaeda in the Arabian Peninsula (AQAP). The group’s first leader, Yusuf al-Uyayri, was hyper aware of the opportunity presented by the internet beginning in the late 1990s. Meijer highlights that some of his writings ‘were published by his newly founded research institute, The Center for Islamic Studies and Research, which acted as a forum for jihadi ideas. In this period, he probably also became Webmaster for al Qaeda’s site al-Neda.’ He was also a prolific commentator on his al-Dirasat website and participated in some of the Paltalk rooms under the name ‘Azzam.’ Despite his death early in AQAP’s terrorist campaign in June 2003, al-Uyayri set the tone for how the group would seek to engage public opinion. In so doing, the internet became a central plank for a key al Qaeda affiliate with a young leadership demographic. Al-Uyayri remains such a figure of influence that his writings are still distributed today across the Salafi-Jihadist ecosystem, as shown in Figure 3.1.

65 Following the 12 May 2003 terrorist attacks in Riyadh, al-Uyayri was pursued by the security forces and eventually killed in a clash on 31 May 2003 about 10 km northeast of the village of Turbah, seemingly while en route to the Iraqi border. Al-Uyayri’s writings include ‘Constants on the Path of Jihad’, ‘The Islamic View of Self-Sacrificing Operations: Suicide or Martyrdom?’ ‘The Path to the Land of War’, and ‘The Role of Women in Jihad’.
In this early period, ideologically motivated violent extremists were largely consumers of content located on static websites that were organised in a centralised manner. One example of such a website that had a remarkable impact was Abu Mohammad al-Maqdisi’s ‘Minbar al-Tawhid wal-Jihad’. This website aggregated Sunni Islamist extremist content at scale. However, technological developments soon permitted the incorporation of bulletin-board style sections that allowed users to post questions and answers, news stories, commentaries, discussions and ideological rebuttals, etc. Notably, this direct engagement created the need for site administrators to manage such interactions in these sections and, at times, provide organisational and ideological guidance.

Following al-Dirasat, al-Neda and al-Foruq around late 2003, a new wave of websites emerged, many of which were connected to the insurgency in Iraq, including the prominent al-Ansar forum. Other leading sites that emerged in this period included al-Qala’a, al-Masada, al-Ekhlas (succeeded by al-Fida al-Islam in 2011), al-Boraq, al-Firdaws, al-Hesbah, al-Fallujah and Shumook al-Islam.

---


68 Anne Stenersen, ‘The History of the Jihadi Forums’, *Jihadica*, blog, 4 March 2009

69 For a detailed study drawing on material collected primarily from the al-Ikhlas and al-Fallujah forums in September 2007, see Daniel Kimmage, *The Al-Qaeda Media Nexus, the Virtual Network Behind the Global Message*, Radio Free Europe/Radio Liberty, March 2008. Interestingly, the three key al Qaeda media production outlets referenced Kimmage (al-Fajr Information Center, the Global Islamic Media Front and al-Sahab) are all active today.
Other websites were connected to dissident Islamist political activity. For example, prominent UK-based Saudi dissidents Mohammad al-Masari and Sad al-Faqih both developed websites with discussion forums to support their political projects. The former’s al-Islah website became influential because of users’ interest in and commentary on AQAP’s terrorist campaign in Saudi Arabia. These forums would have differing degrees of success in staying active and online, and over time many forums would become password protected in an early attempt to control audiences, prevent disruption by perceived malicious actors and evade excessive penetration by security agencies. However, increased security necessarily created other challenges. Klausen notes that ‘[t]he requirement that participants be ‘vetted’ by administrators limited the ability of al-Qaeda to spread its message beyond the circle of those who were already motivated to seek out contact with jihadist extremists. Participants needed to know where to go as well as have connections to someone who can recommend them to gain access with a password.’

This focus on coordination and doctrinal reinforcement among existing VE campaigners and actors reduced the extent to which the exploitation of technology could be used to cultivate and recruit others, inhibiting the transition of nonactors to actors.

Another early VE adaptation was to improve cybersecurity. In November 2006, al Qaeda’s al-Fajr Information Center issued the first Technical Mujahid Magazine, examples of which are shown in Figure 3.2. In 2007, al Qaeda’s Global Islamic Media Front released an encryption program for Microsoft Windows, Mujahedeen Secrets (Asrar al-Mujahideen). This tool was widely promoted across a variety of forums. However, the emphasis on user interaction via forums, chat rooms and bulletin boards would eventually be eclipsed by the emergence of social media platforms.

---


Social Media

Like other users, violent extremists moved quickly to exploit the outreach potential offered by social media platforms such as Facebook (launched in 2004), Twitter (launched in 2006) and Instagram (launched in 2010). These platforms offered violent extremists new ways to create influence, build networks and connect with previously unreachable audiences on a larger scale. For violent extremists, this was a significant departure from engaging with like-minded users in controlled spaces. After the launch of larger-scale social media platforms, violent extremists could seek to maintain ecosystems that were embedded in the mainstream, despite the subsequent challenges and risks. Amid this transition, Bunzel identified how social media ‘had the effect of decentralizing the online jihadi environment, leading to relatively less participation on the forums in the form of discussion and analysis.’73 As a result, the transition to social media was not without its critics among violent extremists, some of whom considered it a form of ideological dilution.74 In terms of better understanding trends within the IMVE environment, researchers recognised that the move to social media created ‘the opportunity to leverage genuine interdisciplinary approaches, which combine in-depth knowledge of big data techniques and network analysis, with rich multilingual understanding of the ideological, religious, and cultural foundations of jihadist propaganda.’75

74 Bunzel, 2013.
If earlier IMVE online innovation had emerged from the direct experience of conflicts in Saudi Arabia and Iraq, then the transition to social media was empowered by the rapid territorial expansion of IS and al Qaeda–linked groups in Syria from 2011, and the pace of adoption accelerated from 2013 to 2015.\textsuperscript{76} The IS declaration of its Caliphate on 29 June 2014 further catalysed the group’s international projection and recruitment efforts. In this regard, Weimann, Berton and Samouris suggest that IS ‘took an unprecedented step to revolutionise jihadist communications. It invested in building a sophisticated media arm that would ensure high-quality outputs, effective outreach, and persuasive branding aimed to reach global audiences.’\textsuperscript{77} As a result, the group was able to recruit large numbers of fighters and maintain unprecedented connectivity with its global constituency. One key aspect of IS media success was the group’s willingness to empower foreign fighters to create culturally and linguistically sticky content which would then be disseminated across social media.\textsuperscript{78}

Klausen notes that ‘[t]he jihadist insurgents in Syria and Iraq use all manner of social media apps and file-sharing platforms, most prominently Ask.fm, Facebook, Instagram, WhatsApp, PalTalk, kik, viper, JustPaste.it, and Tumblr. Encryption software like TOR is used in communications with journalists to obscure locational information.’\textsuperscript{79} Despite use of a variety of social media platforms, the town-hall broadcast and network features of Twitter made it increasingly popular as the vehicle of choice for communication with the outside world, as shown in Figure 3.4.\textsuperscript{80} One prominent study that examined the group’s Twitter footprint from September to December 2014 estimated that ‘at least 46,000 Twitter accounts were used by IS supporters, although not all of them were active at the same time.’\textsuperscript{81} The study, perhaps more problematically, also noted that ‘[a] completely reliable ceiling proved elusive due to the size of the dataset, its rapid evolution, and the complexity of the relationships within it.’\textsuperscript{82}

---

\textsuperscript{76} Nico Prucha, ‘IS and the Jihadist Information Highway—Projecting Influence and Religious Identity via Telegram’, \textit{Perspectives on Terrorism}, Vol. 10, No. 6, December 2016

\textsuperscript{77} Weimann, Berton and Samouris, 2022, p. 132.

\textsuperscript{78} The use of the word \textit{sticky} here refers to content is easy to learn but hard to forget.

\textsuperscript{79} Klausen, 2015, p. 1.


\textsuperscript{81} J. M. Berger and Jonathon Morgan, \textit{The ISIS Twitter Census, Defining and Describing the Population of ISIS Supporters on Twitter}, Center for Middle East Policy, Brookings Institution, March 2015

\textsuperscript{82} Berger and Morgan, 2015.
Uninterrupted access to social media offered violent extremists the opportunity to influence mainstream perceptions of their group in addition to directly challenging and antagonising their adversaries, whether those adversaries are they mainstream communities or other violent extremists. Yet, given the mainstream context, as Williams et al. have highlighted, other ‘... users may not recognise that they are engaging with propaganda or other manipulative content intended to radicalize and recruit adherents.’83 Against this backdrop, it is therefore unsurprising that Twitter continues to be seen as a key access point for violent extremists to engage globally with mass audiences, as demonstrated in Figure 3.4.

---

83 Williams et al., 2021, p. 15.
Figure 3.4. IS Campaigner Encourages Supporters to Expand Media Operations to Twitter

SOURCE: Adapted from IS campaigner, Element, 5 September 2022.
NOTE: Element is a decentralised, encrypted collaboration tool.

From Twitter to Telegram

Any violent extremist group that relies on a single platform invariably faces the risks of disruption and deplatforming. At the same time, as noted previously, VE ecosystems are by their very nature adaptive entities that adjust their postures according to the stability of account access and security of platform, audience reach, network access, the ability to transmit content, etc. In 2016, Prucha described, how against the backdrop of Twitter crackdowns, IS members and supporters migrated to Telegram across hundreds of channels, [with] often more than 30,000 Telegram messages . . . being pushed out by them each week. Telegram [was] being used to share content produced by ‘official’ IS channels . . . such content [was] enriched and enhanced by media supporters from within IS held territory, as well as by sympathisers worldwide.84

Although Telegram was launched in 2013 as an encrypted messaging application, it has continued to evolve similar to other social media platforms. In September 2015, Telegram introduced the ability to broadcast content on channels, which brought its functionality somewhat closer to the functionality of Twitter. In addition, ‘[a]dministrators can create public groups and channels that are searchable within Telegram and openly accessible, and private groups and channels which are not searchable and require a URL invite key called a ‘joinlink’ to access.’85 Moreover, violent extremists can use anonymous bots to distribute content, including via invite or join links, prominent examples of which are shown in Figure 3.5.86 These changes

85 Bennett Clifford and Helen Powell, Encrypted Extremism, Inside the English-Speaking Islamic State Ecosystem on Telegram, Program on Extremism, George Washington University, June 2019, p. 7
have made the platform increasingly attractive to violent extremists of all backgrounds and persuasions.

Figure 3.5. Prominent al Qaeda and IS Bots on Telegram in December 2022

SOURCE: Adapted from Telegram, December 2022.

Shortly after the mass migration of IS supporters to the platform in the aftermath of the November 2015 Paris attacks, Telegram announced its first crackdown on IS supporters and removed 78 channels operating in 12 languages.\(^87\) However, compared with Twitter, the scale of deplatforming was extremely limited, and Telegram imposed a short time period during which it performed this deplatforming. As a result, throughout 2016 and 2017, Telegram became an anchor platform for IS and related violent extremists. Early crackdowns ‘culminated in a large-scale deplatforming action carried out by Europol and [European Union] EU law enforcement in cooperation with Telegram in late 2019.’\(^88\) Despite these ongoing efforts, Clifford and Powell noted in 2019 that ‘Telegram is currently considered the preferred digital communication tool for IS sympathisers. It serves as a stable online platform for pro-IS content, an ecosystem for building extremist networks, an effective and secure internal communications tool, and a forum for recruiting new IS members.’\(^89\) Criezis suggests that ‘[o]ne major factor in Telegram’s continuing relevance is [that] private groups are still able to function over substantial periods of time without detection or deletion. In private chats on Telegram, users need either an invite from an existing member or a unique URL with a link to the group in order to join the group and access the content within.’\(^90\) Indeed, following VE actor and campaigner tactical adaptations, which will be examined in Chapter 4, IS and other VE content remains a remarkably stable feature of the Telegram landscape.

One final point is that, despite the shift to Telegram, Twitter has not been abandoned by violent extremist groups. Twitter remains a popular target platform for violent extremists,


\(^{89}\) Clifford and Powell, 2019, p. 5.

\(^{90}\) Meili Criezis, *Create, Connect, and Deceive: Islamic State Supporters’ Maintenance of the Virtual Caliphate Through Adaptation and Innovation*, Program on Extremism, George Washington University, September 2022, p. 4.
particularly following the Elon Musk’s takeover of the company in 2022 and subsequent layoff of staff, particularly in areas outside the United States, who were moderating a variety of misinformation and hate-based speech that targeted minority groups.91 Twitter’s reach as a popular platform for those users who have not already transitioned to the ostensibly robust Telegram VE environment remains attractive to VE campaigners as it continues to offer rapid access to much larger audiences than Telegram does.

The Decentralised Web and Dark Web: Game Changers for Violent Extremism?

Against the backdrop of the various deplatforming attempts discussed previously, violent extremists began to diversify their ecosystems into new spaces, including decentralised technology. This process has not been linear, but it has resulted in increased complexity as many more platforms are being used by violent extremist groups used simultaneously. The decentralised web (DWeb) is an evolving landscape that consists of technologies aimed at improving transparency and weakening centralised control of the internet using open-source code and distributed networks. In theory, this form of governance and infrastructure offers violent extremists a tremendous advantage. The use of these decentralised new spaces might not necessarily result in greater radicalisation but it does offer an effective means through which violent extremist groups can build resilience and manage issues of longevity. As a result, radicalisation and influence become an uninterrupted feature of the environment, increasing risks associated with exposure to malicious content. For example, ‘[o]ne major reason for its attraction is that any content hosted ‘on the Dweb’ cannot be removed as it is not controlled by a central authority and thus not easily removable.’92 However, the decentralisation of these technologies, to date, often comes at the expense of easy access to large audiences. This trade-off might be less of a concern for violent extremists considering the ways in which they are building cross-platform ecosystems that have constituent parts playing different but complementary roles. Bodo notes that ‘in the context of today’s digital efforts to counter violent extremism . . . . [t]he danger is real, and the decentralised web seems to be the next logical step for IS online.’93

King highlights how IS began experimenting with the DWeb as early as summer 2014, when ‘the group set up a series of official accounts on three low-profile decentralised platforms—Friendica, Diaspora and Quitter.’94 In September 2017, IS set up accounts on another decentralised social media network, Element (known at the time as Riot), followed by

---

91 For a current synopsis, see Gerry Shih, Michael E. Miller and Joseph Menn, ‘Twitter Hate Speech Up in Large Foreign Markets After Musk Takeover’, Washington Post, 14 January 2023.
92 Loránd Bodó and Inga Kristina Trauthig, Emergent Technologies and Extremists: The DWeb as a New Internet Reality? Global Network on Extremism and Technology, 1 August 2022, p. 1.
93 Loránd Bodó, ‘Decentralised Terrorism: The Next Big Step for the So-Called Islamic State (IS)?’ Vox Pol, 12 December 2018
Rocket.Chat and ZeroNet in late 2018. Rocket.Chat and ZeroNet have proved attractive for IS media operatives, as the developers of those platforms have no way of acting against content that is stored on user-operated servers or dispersed across the user community. There is little sign of this experimentation abating. In its 2021 Review of Online Jihadist Propaganda, the European Union Internet Referral Unit of Europol noted that

IS online supporters displayed increased attempts to experiment with new open-source and decentralised technologies for propaganda dissemination. Videos by IS self-proclaimed provinces, IS-supporting media and issues of al-Naba’ were uploaded to Skynet. Al-Naba’ was also stored by IS supporters on the Inter-Planetary File System (IPFS) a distributed system for storing and accessing information.

In 2022, Weimann et al. observed that ‘Element (formerly known as Riot), an open-source, instant messaging service that relies on the federated Matrix protocol constitutes one of the most durable ‘alternative hubs’ for pro-IS propaganda accounts. But violent extremist groups have plenty of choices:

Another contender to become IS’s next ‘platform of choice’ is TechHaven, a self-hosted instance of Rocket.Chat. TechHaven had been set up by IS online supporters in 2018 ostensibly to host backup groups in case chats on Telegram were suspended. Registration and private invite links to join Rocket.Chat had been advertised by the Nashir News channel on Telegram since mid-December 2018.

In an indication of how quickly DWeb technology is evolving, in May 2022, Rocket.Chat announced that it was ‘building its new federation capabilities on the Matrix protocol to allow its users to communicate with users on other platforms.’ In short, this would make ‘it simple for organisations to easily connect with external parties, whether they’re using Rocket.Chat or any other Matrix compatible platform.’ This leap forward in encrypted cross-platform interoperability will have downstream impact on VE communication patterns and online behaviour.

---

95 King, 2019. Element, then known as Riot, is a decentralised, encrypted collaboration tool. It supports groups, channels and sharing of files between users. Registration does not require a phone number. Rocket.Chat is an ‘open-source team collaboration platform that enables banks, NGOs, start-ups, and governmental organizations to have their own chat tool, customize its look and feel, choose their users, and securely manage data.’ See Getapp, ‘Rocket.Chat Overview’, webpage, undated. ZeroNet is ‘no more anonymous than BitTorrent, but privacy . . . will increase as the network and the sites gains more peers. ZeroNet is made to work with anonymity networks: you can easily hide your IP using the Tor network.’ ZeroNet ‘Frequently Asked Questions’, webpage, undated.

96 King, 2019.


99 Weimann, Berton and Samouris, 2022.


Complementing the DWeb, the Dark Web offers violent extremists a higher level of personal security and the ability to host content in an unregulated space. As a result, violent extremists continue to grow digital repositories on the Dark Web. Even in this security focused space, innovation has made access to content much easier. For example, it is now possible to download a desktop version of the TOR browser to simplify access to the Dark Web.\textsuperscript{102} Content can then be consumed and made available by violent extremists on the Clear, or Surface, Web with relative ease. Against this background, in 2021, Europol’s European Union Internet Referral Unit noted that

IS-supporting media outlets and their networks of supporters continued to rely on websites on the Surface Web and the Dark Web to archive and distribute official IS statements, photo reports, al-Naba’ issues and video releases. Some of these web pages, for instance the one managed by the IS-supporting I’lam Media, offered translations of IS content in multiple EU and non-EU languages.\textsuperscript{103}

All these innovations and initiatives challenge the assumption that nonactors or novices will not enter and use the Dark Web in search of content and connectivity because of the barrier to access that is inherent to the Dark Web.

I’lam, the media arm of IS, is situated within a matrix of related IS channels on the Dark Web, each of which serves a different purpose. This matrix includes \textit{Akhbar al-Muslimeen} [News of the Muslims], al-Ra’ud (an archive site that contains two decades of IS content) and al-Bayan radio (a station that provides content from IS radio), as shown in Figure 3.6. Illustrating the cross-platform characteristic of VE ecosystems, this network of media channels also provides regularly updated links to key IS points of contact on Telegram. IS seeks to use different aspects of each of these platforms to achieve an overall network advantage. In this regard, Criezis notes that, ‘[t]hroughout the process of migration from one platform to the next, IS supporters have gained experience in online decision-making, affording them opportunities to adjust, innovate, and test various methods to maintain their online presence.’\textsuperscript{104}

\textsuperscript{102} According to the Tor project, \textit{[t]he need for tools safeguarding against mass surveillance became a mainstream concern thanks to the Snowden revelations in 2013. Not only was Tor instrumental to Snowden's whistleblowing, but content of the documents also upheld assurances that, at that time, Tor could not be cracked. People's awareness of tracking, surveillance, and censorship may have increased, but so has the prevalence of these hindrances to internet freedom. Today, the network has thousands of relays run by volunteers and millions of users worldwide. And it is this diversity that keeps Tor users safe.} (Tor Project, ‘History’ webpage, undated.)

\textsuperscript{103} European Union Internet Referral Unit, 2022, p. 22.

\textsuperscript{104} Criezis, 2022, p. 4.
The pace and scale of adaptation illustrated in this chapter show that IMVE actors and campaigners are adept at exploiting the opportunities that are offered by advances in digital technology and have been for about as long as the internet has existed. In 2006, Hoffman noted that

As terrorist communications continue to change and evolve, so will the nature of terrorism itself. Although one cannot predict what new forms and dimensions terrorism will assume during the rest of the 21st Century, this evolutionary process will continue and doubtless be abetted—and accelerated—by new communications technologies: as has been the case over the past decade.105

Violent extremists continue to respond to changes and challenges in digital landscapes to maintain and grow their ecosystems. In Chapter 4, we will explore the tapestry of ways that they respond and adapt.

---

Chapter 4. Catalysing the Transition

VE online consists of a dynamic tapestry of systems that can be characterised as varying types, from ecosystems to sociotechnical systems. From a sociotechnical system perspective, VE actors use technical advantages to engage on and across a broad variety of platforms, from more-mainstream websites and popular social media platforms to emergent alternative technology and the Dark Web. In addition, VE campaigners work across this landscape and use increasingly sophisticated means to spread VE content and pull users and actors into spaces in which they can more easily recruit and cultivate those users and actors. Detailed observation of this landscape has illustrated the presence of multiple VE ecosystems that transcend platforms and engage with users at varying levels of extremism. According to Ayad, Khan and al Tamimi, although these ecosystems might ‘seem like disparate networks, they are in fact cogs within the machinery of an extensive propaganda network spread and working in tandem across numerous platforms and messaging applications.”

Moreover, violent extremist networks are more capable than ever before of using a wide variety of digital opportunities to engage within the network, with other networks, and with other audiences. In doing so, violent extremists seek to reinforce ideological commitment by building community, sharing experiences and circulating content. They also seek to legitimise their world view and campaign for it with ever-larger online audiences and with a growing number of potentially violent participants who are willing to act out the violence espoused virtually in the real world. This cross-platform, networkwide characteristic gives the system its resilience while simultaneously maximising opportunities for physical violence to emerge from it, which is consistent with the characterisation of online VE as an ecosystem.

It should be emphasised that these violent extremist networks and ecosystems are in intense competition with one another according to their ideological positions and group affiliations. This dynamic reflects the offline posture of violent extremist networks in multiple conflict zones. As a result, it should come as no surprise that ideologically motivated violent extremists expend much online effort delegitimising other networks and attempting to cultivate and recruit users and actors from them. For example, note the continued global interplay between al Qaeda and IS or the local-level competition between the Taliban and IS Khorasan Province. The intensity of this competition often drives technological innovation by violent extremist groups.

Grasping Complexity: Ethnographic Insights, Ethics and Method

To better understand this complex ecosystem, over a six-month period from July to December 2022, we undertook a granular virtual ethnography of VE landscapes. This virtual


107 For more information on the process of undertaking ethnographic research online, see Christine Hine, Virtual Ethnography, SAGE Publications, 2000. Also see Maura Conway, ‘Determining the Role of the Internet in Violent
ethnography required a detailed understanding of VE organisations, culture and network history, ideology, technology and (for ideologically motivated violent extremists) the Arabic language. It was therefore highly contingent on a blend of skills, experience and expertise. According to Kozinets, ‘Netnography, the ethnography of online groups, studies complex cultural practices in action, drawing our attention to a multitude of grounded and abstract ideas, meanings, social practices, relationships, languages, and symbol systems.’\textsuperscript{108} For Guest, Namey and Mitchell, ‘The density of data produced and the intensity of the data collection experiences it entails can produce meaning on both professional and personal levels that few other approaches can rival.’\textsuperscript{109} The very dynamism and complexity of the VE landscape online makes a flexible ethnographic approach so useful.

On participant observation as a tool, Hine notes that ethnography ‘means to undertake an immersive, prolonged engagement with the members of a culture or community, followed by an attempt to understand and convey their reality . . . ’\textsuperscript{110} although ‘unobtrusive exploration of online landscapes can be an immersive ethnographic experience in its own right’\textsuperscript{111} Moreover, ‘much of the discussion of ethnography in online settings that has taken place across the social sciences in recent years has suggested that ethnographers in these new circumstances are required to be particularly agile in their methods and adaptive in their strategies.’\textsuperscript{112} This report’s focus on violent extremists necessitated such flexibility because the use of an active form of participant observation would have had clear security implications and a detrimental impact on data collection. From the perspective of research ethics, awareness of these debates was key. Kozinets notes that, ‘ethnographic inquiry already possesses some of the thorniest terrain for navigating research ethics. When we add to this the technological complexities and unique new contingencies of online interactions, these already-difficult issues become even more formidable.’\textsuperscript{113}

As a result of these considerations, we followed two guidelines from the outset. First, we did not ‘participate’ during observation nor to directly seek consent, which aligns with Conway’s broad assessment that ‘[s]afety is the chief reason that deception is generally employed by online extremism and terrorism researchers . . . This is more ethically defensible than it may first appear as the use of “real names” is uncommon in these spaces, so a pseudonym is expected.’\textsuperscript{114} In addition, the British Psychological Society notes that ‘[w]here it is reasonable to argue that there is likely no perception and/or expectation of privacy (or where scientific/social value

\textsuperscript{110} Hine, 2015, p. 60.
\textsuperscript{111} Hine, 2015, p. 157.
\textsuperscript{112} Hine, 2015, p. 22.
\textsuperscript{113} Kozinets, 2010, p. 136–137.
and/or research validity considerations are deemed to justify undisclosed observation nevertheless), use of research data without gaining valid consent may be justifiable.¹¹⁵

Second, in terms of research conduct, we took careful account of security and risk considerations. A private network was used in an anonymous way throughout; data were carefully managed and stored; and no data were shared with third parties. Again, this approach aligns with the latest guidelines issued by the British Psychological Society Working Party on Internet-Mediated Research, which encourage researchers ‘to have well-developed data management plans to fully address these confidentiality-related issues.’¹¹⁶ Finally, with regards to this report, care has been taken to anonymise all primary data and exclude all offensive and problematic material encountered during the conduct of research, through such methods as obscuring account names or other identifying information in figures. In addition, we do not offer citations for the individual social media posts depicted in the figures. The social media posts were gathered from August 2022 to January 2023.

On data and sample acquisition, a snowball-based method was used for data and sample acquisition. Researchers note that this approach can be used to enable ‘access to previously hidden populations’ and those ‘which are not hidden but are hard to reach for research purposes.’¹¹⁷ This approach was not designed to create a statistically representative sample but to gain increased access and exposure to cross-platform VE ecosystems over the duration of the research.¹¹⁸ To kick-start this process, we selected two high-profile violent extremist accounts, or nodes, on Telegram. Both accounts were based in the West and focused on English-language audiences, which ensured that our starting point was carefully calibrated. One account belonged to a prominent violent extremist with a long-established role in Salafi-Jihadism, and a previous conviction linked to IS.¹¹⁹ The other account belonged to a VE with a significant role in neo-Nazi extremism.¹²⁰ From these starting points, we identified other violent extremist accounts and acquired a significant sample across a variety of platforms. The sample varied from minor VE actors to official (and semiofficial) accounts of global VE organisations and spanned a tapestry of platforms, including, in no particular order, Telegram, Twitter, Chirpwire, Odysee, Rocket.Chat, Element (Matrix), Discord, 4Chan, 8Kun, Stormfront, Archive, Justpaste.it, noteshare.id and the Dark Web. Data collected throughout this research included detailed notes, observations, audiovisual downloads and screenshots.

¹¹⁸ Klausen describes a similar approach: ‘Using a snowball method we treated the original accounts as starter nodes in a network of followers and those being followed by others, and created a larger data set that covers the entire network’ (Klausen, 2015, p. 6).
¹¹⁹ This Telegram account (and multiple related versions) was deplatformed and no longer exists as of 2022.
¹²⁰ This Telegram account has not been deplatformed and thrives unimpeded as of 2023.
Disaggregating Violent Extremist Behaviours and Building a Typology

Throughout the process of sample identification, characteristics of behaviour exhibited by violent extremists began to emerge. From persistent categorisation and thematic analysis, we derived several conclusions. An initial observation was that behaviour was highly conditioned by the characteristics of each platform, specifically the extent to which violent extremists could be transparent about their worldview and share relevant content while mitigating the risk of deplatforming. Close attention was also paid to the cross-platform linkages and relationships within VE ecosystems and the ways in which these connections were maintained over time through the provision of links and the use of bots, within and between platforms. As a result of the ongoing sample expansion and related analysis, we established that the key feature of this landscape was associated with promoting engagement between ordinary users, VE actors and violent-extremist-network campaigners. This engagement was achieved through a variety of processes, concepts and ideologies and the use of myriad forms of technology.

Additionally, we found that VE ecosystems are remarkably resilient to external challenges and adaptive to changes in platform potential (e.g. shifts in terms of service and deplatforming policies) and technology (e.g. encryption, bots, emergent alternative technology). These ecosystems are maintained through the interplay of active (at times hyperactive) users that engage with each other and with extremist content from ‘official’ sources and content created by VE actors. The latter might include historic content or even the repurposing of content taken from mainstream sources—news articles, think tanks, policy reports, etc. As a result, the strength of the ecosystem rests on the number of users, cross-platform reach and continued supply of relevant content.

We gave careful consideration to how these characteristic behaviours could be disaggregated into useful, identifiable patterns, particularly because of the wide variety of users within the system who operate at different levels of transparency, sophistication (in organisational, ideological and technological terms) and commitment, including their willingness to take risks to share ideology and content. Against this complex backdrop and clear overlaps and similarities in violent extremist behaviours and through detailed thematic analysis of expansive datasets of primary content, we identified four key themes or patterns of behaviour: (1) engagement with VE content, (2) obfuscation or managed deception, (3) security and platform selection (4) and cross-platform network linking. The concentric circles depicted in Figure 4.1 represent the way that each of the tactics are adopted to maximise opportunities to reach and engage an audience in the relevant violent extremist cause. Delivering content that is engaging or can engage as broad an audience as possible was a key network concern. Obfuscation is the simplest tactic to apply to maintain access to a platform or sustain the presence of the content online. The degree to which obfuscation or the necessary branding of the content is needed shapes the security requirements applied to it, for example, from an accessibility point of view (i.e. some content might not be for a broad audience) or consideration of the platform where the content is to be hosted. To maximise outreach or recruitment opportunities for the violent extremist cause, the ability to

---

121 For example, see Berger and Morgan, 2015.
draw or pull users in from the largest variety of platforms and expose them to key messaging and content, some of which might be hosted in more-secure or specific online areas, requires network linking. Employment of each of these behaviours affords violent extremists freedom of manoeuvre against countermeasures and ultimately strengthens the resilience of the VE ecosystem and its ability to survive and thrive. In the following section, we describe, through examples, each of these different tactics as they apply to online content and behaviour.

Figure 4.1. Conceptualising the Overlaps in Violent Extremist Behavioural Patterns

Obfuscation

The use of obfuscation is important for violent extremist accounts to maintain account longevity and audience access by mitigating the risk of deplatforming. This risk varies tremendously from one platform to another and carries different consequences. For example, some platforms require a new phone number for new account setup with associated document registration issues in some countries, while others require only an email address. In general, the more mainstream and popular the platform, the higher the risk and, therefore, a need for greater obfuscation. In essence, this means that violent extremists need to avoid artificial-intelligence algorithms that seek to identify and triangulate particular words, phrases and ‘hashed’ images, videos and PDF files. They might also need to build profiles that minimise the interest of nonspecialist regulatory teams if the account is reported as potentially problematic by other

122 GIFCT’s ‘Hash-Sharing Database’ contains perceptual hashes of known images and videos that are produced by terrorist entities of the United Nations–designated terrorist groups. For more on hashes and hash-sharing, see Global Internet Forum to Counter Terrorism, ‘GIFCT’s Hash-Sharing Database’, webpage, undated-a.
users. Criezis describes these tactical obfuscations as ‘textual deception, visual deception, and account deception.’

Textual obfuscation involves the modification of words and phrases to convey meaning while avoiding artificial intelligence–based monitoring systems. This practice can include the use of disjoined words, oblique references, emojis, punctuation and spacing adjustments, numbers in place of letters, acronyms and mistransliterated Arabic words. As platform counters adjust, violent extremists alter their approach. Examples of this behaviour can therefore vary from being extremely simple to complex. The first example shown in Figure 4.2 illustrates a simple approach; the ‘i’ and ‘a’ in jihad are replaced with an ‘!’ and ‘@’, respectively. The second example describes ongoing conflict between IS and the al Qaeda–affiliated JNIM movement in Mali, thus greater contextual understanding is needed to fully understand the content and implications shown. In Figure 4.2, for example, ‘JNIM’ is replaced by ‘J&%M’; a reader who does not have the context for that obfuscation will not have a full understanding of the message.

Visual obfuscation involves altering images to avoid algorithmic detection. Examples are shown in Figure 4.3. The example on the left reads ‘Urgent: Those in black distribute photos showing their oath of allegiance to the new caliph from Lebanon.’ The text also includes a purposeful misspelling of the word ‘caliph’ in Arabic. Criezis notes that ‘[s]upporters will blur IS flags or well-recognized IS leader’s faces in videos and still images, alter the colour settings when reposting screenshots of official IS media, and distort the cover pages of IS media to interfere with image hashing detection.’

In short, the VE ecosystem continues to illustrate its adaptive ability to maintain audience access even when confronted with substantial automated counters.

Figure 4.2. Examples of Textual Obfuscation

SOURCES: Adapted from Twitter (left); Reproduced from Telegram (right).
NOTE: We obfuscated the account name on the left, it not was not obfuscated by the original account owner.

Visual obfuscation involves altering images to avoid algorithmic detection. Examples are shown in Figure 4.3. The example on the left reads ‘Urgent: Those in black distribute photos showing their oath of allegiance to the new caliph from Lebanon.’ The text also includes a purposeful misspelling of the word ‘caliph’ in Arabic. Criezis notes that ‘[s]upporters will blur IS flags or well-recognized IS leader’s faces in videos and still images, alter the colour settings when reposting screenshots of official IS media, and distort the cover pages of IS media to interfere with image hashing detection.’ McDonald adds that ‘[o]verlaying is also increasingly common; by overlaying terrorist content with emojis, watermarks, and banal images such as flowers or minarets, these accounts often circumvent detection algorithms.’ In short, the VE ecosystem continues to illustrate its adaptive ability to maintain audience access even when confronted with substantial automated counters.

124 Criezis, 2022, p. 16.
125 McDonald, 2022.
Violent extremists have also increasingly sought to use misleading profiles to suggest that their accounts are ordinary, mundane and mainstream. In some cases, this approach might mean that violent extremists craft profiles that suggest they are an independent researcher or journalist or name channels so as to suggest that they represent mainstream news platforms. For example, in Figure 4.4, the following ‘independent reporter,’ whose account on Twitter has been active since 2011, selectively amplifies pro-IS content and is careful not to share it directly, presumably for legal reasons.

Another form of language-based obfuscation is the use of seemingly critical or third-party impartial references to describe groups or their actions, when in fact the purpose is to promote that group and its actions. For example, in Figure 4.5, a prolific and influential Telegram-based IS account refers to ‘the terrorist group known as the IS’ and the ‘designated terror group,’

SOURCE: Adapted from Twitter.
which might mislead a nonexpert content moderation team to concluding that the post is critical of IS rather than spreading its messaging.

Figure 4.5. Examples of Language-Based Obfuscation

SOURCES: Reproduced from Telegram (left); adapted from Telegram (right).

Security and Platform Selection

Given the implicit risk of participation in violent extremist behaviour and group affiliation, it is unsurprising that violent extremists attempt to protect their online interactions in a variety of ways. Aside from account loss through deplatforming, offline costs of participation can include detention, prosecution and further punitive measures. As a result, many violent extremists use anonymisation tactics such as virtual private networks, encrypted email and TOR. Moreover, violent extremists might also operate more actively on less restrictive platforms that offer increased levels of encryption, such as Telegram, and decentralisation, such as Rocket.Chat and Element, in addition to password-protected accounts that require some form of registration or vetted access. Bots might also be used much more widely to create a technical buffer between the VE campaigner and their audience. These enhanced security measures are perceived as mitigating risk and can facilitate participation in more-problematic ecosystems that connect ordinary, and at times unsuspecting, users and VE actors with VE campaigners and associated terrorist organisations.

Some of the ecosystem presence on niche or less restrictive platforms will be the result of violent extremists experiencing deplatforming and moderation policies on more-mainstream platforms. There is an astonishing array of sites, platforms and technologies that are exploited by VE ecosystems. For example, in Figure 4.6, note the al Qaeda–linked al-Andalus account and Taliban-linked Haqqani Network Manba’-ul-Jihad account on ChirpWire. Other groups, such as al-Shabab, AQAP, JNIM and the Pakistani Taliban, also maintain uninterrupted and active presences on the platform. As Figure 4.7 shows, this practice of using multiple platforms to maximise outreach is also practiced by REMVE actors.
A further example, shown in Figure 4.8, illustrates how female IS detainees at Camp Roj in Syria (who should not have the ability to connect to online platforms) layer connectivity from Telegram to Rocket.Chat via the TechHaven bot. In addition to ideological reinforcement within the ecosystem, this also appears to facilitate the collection of donations and coordination for escape and post-release relationships.
The examples in Figure 4.9 illustrate VE movement across different platforms to avoid counters. On the left, a pro-IS Telegram account promotes the secure Element (Matrix-based) platform to improve security and facilitate engagement. On the right, anticipated deplatforming is mitigated by the use of layers of backup channels for other backup channels on Telegram.

Network Linking

A key characteristic of VE ecosystems which has already been emphasised is their cross-platform nature. This reality has had a profound impact on violent extremist behaviour and culture online. It results in violent extremists behaving in calibrated ways according to the opportunities, limitations and risks afforded by each platform while striving to maintain
continued access to community and content. In practice, this reality means that, in addition to regenerating accounts within platforms, violent extremists are adept at navigating across platforms to maintain complex ecosystems. These ecosystems are described in Weimann, Berton and Samouris, which notes that, ‘[i]n the current system of IS propaganda dissemination, social media sites, messaging applications, file sharing platforms, gaming and gaming-related platforms, open-source and decentralised platforms, online service providers (OSPs) supporting website infrastructure, and Dark Web sites all play their own, distinct but complementary role.’

The mechanics of these relationships are therefore of great interest as they build ecosystem resilience and enable violent extremists to exploit the nuanced opportunities offered by disparate platforms (e.g. by broadcasting live discussions simultaneously on Telegram and Discord, publishing video content on Odysee and Archive, distributing written content on Archive, justpaste.it, and mediagram). McDonald describes this behaviour as outlinking and notes that, within the context of IS,

> while accounts may not be able to host official ISIS [Islamic State of Iraq and Syria] publications such as the al-Naba newspaper on mainstream platforms— they frequently share outlinks to external websites or alt-tech platforms where this content is uploaded directly. Many of the pro-ISIS accounts on mainstream platforms also frequently outlink to encrypted platforms such as Telegram or Rocket.Chat, where users chat, share large media files, and plan attacks.

However, during this research, we observed violent extremists also undertaking significant linking within the same platform, which illustrates the degrees of depth of the ecosystem. For example, violent extremists on Telegram linked between more mainstream-facing, somewhat-obfuscated channels and channels with more-explicit VE connections, and between bot-driven channels and ‘official’ accounts of al Qaeda and IS. As shown in Figure 4.10, a Telegram-based account provides links to temporary IS news channels that are also on Telegram. The ‘official newspaper’ listed in one of the links is an obfuscated reference to IS’s weekly al-Naba publication. On the right of Figure 4.10, a Telegram-based bot connects users with active IS channels.

---

126 Weimann, Berton and Samouris, 2022.
127 McDonald, 2022.
We also observed violent extremists actively linking from mainstream platforms with content moderation policies to less restrictive platforms, i.e. from Twitter to Telegram, Rocket.Chat and ChirpWire, and vice versa. This VE opportunity is exacerbated by what Guhl, Marsh and Tuck describe as ‘considerable diversity in the community guidelines, standards or rules of many of the smaller platforms that make up the broader online ecosystem. Different platforms can take radically different positions on various forms of so-called “legal but harmful” activity.’

For example, in Figure 4.11, on the left, an account for al Qaeda’s al-Sahab Media links from a bot on Telegram to ‘official’ accounts on the decentralised Rocket.Chat and Riot (Matrix-based) platforms. On the right of Figure 4.11, a bot on Telegram provides links to the December 2022 release of al Qaeda’s English-language One Ummah magazine. Figure 4.12 shows further specific examples of accounts linking to English-language content across platforms. Figure 4.13 shows a pro-IS Twitter account listing links to a Telegram-based ‘news channel’ that carries real-time updates of IS-sourced content from other secure platforms.

---

Figure 4.11. Network Linking Between Platforms That Have Different Governance Standards

SOURCE: Adapted from Telegram, social media platform, 25 December 2022.

Figure 4.12. Linking English-Language Islamic State Content Across Platforms

SOURCE: Adapted from Telegram.

Figure 4.13. A Twitter Account Linking to a Telegram-Based Self-Described News Channel

SOURCES: Adapted from Twitter (left); adapted from Telegram (right).
Content Engagement

To maintain a vibrant and dynamic VE ecosystem, groups, networks and ideologues need to supply the ecosystem with fresh insight and content. Content might be new, historic (often repurposed), extreme or even, when it justifies a violent extremist position, from mainstream sources. The content will likely be segmented according to audience requirements—religious, ideological, lifestyle-focused, humanitarian, violent, etc. Some of this content is aimed at maintaining network motivation and ideology, while other content is developed to influence users and draw them into direct engagement with VE actors and campaigners. Users might belong to competing ideological groups, so some content is focused on brand reinforcement, and in those cases campaigners deploy tactics similar to any political party or other type of campaigner trying to persuade a target to swap parties, brands or groups. Violent extremists will deploy content in different ways, such as cross-seeding across platforms, surging official and branded content across multiple platforms simultaneously, and using different file types and sizes. The use of multiple methods of deploying content makes that content easier to access and facilitates onward dissemination. Clifford and Powell note that violent extremists ‘are highly dexterous, moving between platforms and constantly recreating accounts while uploading content at a higher pace than it can be theoretically taken down.’

On the left of Figure 4.14, an account for al Qaeda’s Al-Sahab Media distributes a press release across multiple upload sites. On the right, a pro-al Qaeda account that has been active on ChirpWire since December 2020 links to Part 19 of AQAP’s ‘Why I Choose Al-Qaeda,’ which focuses on ‘Their Methods in Jihadist Education.’ This content has also been made available on Rocket.Chat.

Figure 4.14. Examples of Content Posted Across Multiple Platforms

SOURCES: Adapted from Telegram (left); Adapted from Chirpwire (right).

129 Clifford and Powell, 2019, p. 42.
Figure 4.15 shows a screenshot of posts by an IS Telegram-based bot that generates temporary links, often multiple times daily, to niche hosting channels on Telegram. These links are only live for a matter of hours at most. This approach reduces the need for stable channels as fresh links are uploaded at high frequency. It also means that users can mitigate the risk of being deplatformed by avoiding the need to join easily identifiable ‘official’ channels with small numbers of members. Again, this strategy ensures that content is made accessible for onward dissemination.

**Figure 4.15. High-Frequency Reposting**

![Screenshot of Telegram posts]

SOURCE: Adapted from Telegram.

As shown in Figure 4.16, VE actors are increasingly adept at using mainstream content, which is sourced from journalists, think tanks, policymakers, etc., to reinforce their worldview.

**Figure 4.16. Repurposing Mainstream Content to Support Violent Extremism**

![Mainstream content repurposed for VE]

SOURCE: Adapted from Twitter.

This practice of repurposing content is so common that, to mitigate the risk of VE exploitation, some researcher-focused websites that aggregate primary VE data have transitioned
to require registration. For example, Figure 4.17 shows the changes to jihadology.net and the Knowledge Sharing Platform on Tech Against Terror.130

**Figure 4.17. An Example of Security Measures to Mitigate Exploitation by Violent Extremists**

The updated version of Jihadology restricts easy access to sensitive content for unauthorized users. Below is a summary of the changes implemented by Tech Against Terrorism in order to make Jihadology more secure:

- Jihadology will be able to password-protect entries containing particularly sensitive content, including material containing violence or inciting to violence
- To access these entries, users will need to register an account on the site to be able to login and view content behind password-protection
- The user registration system will consider whether an applicant has a legitimate research purpose to access Jihadology via a combination of allowing approved email domains register accounts and allowing Jihadology to manually approve applications (more details below)
- Only registered and logged in users will be able to view entries that Jihadology has placed behind a login wall
- When scrolling down the main page, non-registered or logged out users will only be able to see the title and date of password-protected entries, and will be taken to the login / registration page if attempting to access the entry
- To enable password protection of videos hosted on the platform, Tech Against Terrorism has developed a fit for purpose video streaming solution that will now play the videos behind the login
- Warning interstitials will be displayed when accessing sensitive content
- Visibility of original source URLs and imagery for non-registered users has been restricted

**SOURCE:** Reproduced from Jihadology, ‘Frequently Asked Questions’, webpage, undated.

---

130 Tech Against Terrorism, ‘Welcome to the Knowledge Sharing Platform’, webpage, undated.
Chapter 5. The Engagement Model

With the influence diagram depicted in Figure 2.1, in Chapter 2, we attempted to visualise, albeit at a high level, the push-and-pull-forces, pathways and processes that interact ecosystemwide to either drive or stop the transition of nonactors or users to VE actors. In Chapter 4, we described evolving behaviours or tactics that are used in the ecosystem at a granular level. Against this backdrop, we now construct an exploratory engagement model that seeks to describe the complex interaction of users, VE actors and campaigners across the online landscape. It also illustrates discernible patterns of behaviours that manifest as participants within the ecosystem connect with VE content and actors and, in some cases, transition into becoming violent extremists. The ‘DNA’ of this model, shown in Figure 5.1, is active engagement and is focused primarily on understanding transition, which can be seen as the central focus within the initial influence diagram shown in Figure 2.1.

The use of the word engagement to describe the model is deliberate and intended to invoke a meaning synonymous with an immersive psychological state. Other studies have examined the role that social media has in engaging people and motivating them to be involved and participate in activism (and its associated physical activities such as protests). From in-depth interviews with people who engage deeply in activism, it was necessary to understand their engagement as a progression of antecedents, attributes, and outcomes to understand the influence it had on their participation in activism. Similarly, within the constructed engagement model, we include a series of antecedents, attributes and outcomes to understand the influence online engagement might have on people’s participation in violent extremism. In describing this series, push-and-pull factors become evident throughout the model as we necessarily consider the interplay between user and campaigner.

Antecedents

A significant antecedent for increased participation in activism, observed in Smith, Krishna and Al-Sinan is the possession of skills that are necessary not only for navigating platforms, but also for building and distributing content effectively.\(^\text{132}\) As described in that study,

This sense of effectiveness is consistent with the concept [of] communicative competence. . . . Therefore, competence may be a connector between antecedents and the engagement experience . . . participants who were more confident in their ability to contribute to the protest effort online seemed more likely to demonstrate high levels of engagement than those who doubted their communicative competence.\(^\text{133}\)

This idea and its applicability to the IMVE problem discussed in this report requires further research, but our observation of the shifts in behaviour that arise from the earlier identified typology—increased obfuscation, security, network connectivity and engagement with VE content—might be predicated on a similar communicative competence. VE campaigners, along their experience, commitment to cause, motivation to pursue group objectives etc., are adept at working across multiple platforms and indicate strong communicative competence. Apart from the opportunities that are afforded and shaped by platforms, VE campaigners have had the greatest impact on both the creation and continued curation of content.

\(^{132}\) Smith, Krishna and Al-Sinan, 2019.

\(^{133}\) Smith, Krishna and Al-Sinan, 2019, p. 191.
Attributes

Beyond competence in content creation and distribution, VE campaigners have an intuitive understanding of how to behave according to their platform, context and audience. As technology evolves, their patterns of engagement will continue to adapt. Such adaptive behaviour must be considered an important attribute for VE campaigners to remain active and successful in the outcomes that they seek. This requirement might have always existed for violent extremists, but Khalil observes that the shift from static websites and closed forums to public social networking sites back to alt-tech platforms and skulking in the “dark web” or “deep web” by extremist actors has significantly changed the role of the Internet and other technologies related to extremism, depending on the affordances of each platform or technology. Current technology that did not exist in previous years, such as end-to-end encryption messaging services and drone technology, has impacted the tactics, communications and operations of extremist actors. Further advances in technology will prompt similar shifts.\(^{134}\)

Other attributes highlighted by the model are those associated with the evolution of violent extremist identity. Users initially consume the most accessible content without too much manoeuvre across platforms and gradually increase their awareness of the variety of content and the commensurate risks attached to accessing it. At Stage 1 and Stage 2, there is little to discern, characterise or identify users who might be on a path to greater engagement as different from users who might be driven by curiosity. At best, attributes at these stages could be described as passive or reflexive. However, much stronger attributes emerge at Stage 3, when users

- target and adopt a specific ideology
- move from cognition of risks to active mitigation strategies
- proselytise and coordinate across many platforms for their violent extremist cause (Stages 4 and Stage 5).

Outcomes

Stage 3 of the model is culminating point at which users have been cultivated and have themselves cultivated attributes that are much more indicative of absorption, commitment and engagement with VE. Ultimately, this outcome or transition is how VE campaigners measure their success. Across the model, they

- seek to maximise their influence operations with the largest audiences (Stage 1 and Stage 2)
- attempt to draw interested users into more-secure, interactive spaces for the purposes of cultivation and recruitment (Stages 2 through Stage 4)
- are more likely be involved in the management of digital libraries on the Dark Web, for reasons of longevity, (Stage 5) while relying on the broader ecosystem to cross-populate and seed that content throughout the model.

---

It is essential to note that the model does not imply that transition towards VE is inevitable or even probable for most users. It does not suggest that, for users who do ‘radicalise’, the pathway to radicalisation is at all linear. Radicalisation pathways are invariably highly individual, often gradual and unremarkable experiences.135 Horgan notes that, ‘[a]n inescapable social quality of increased involvement in a terrorist movement is a sense of gradual progression. From examining accounts closely, increased commitment to the movement appears to be characterized by a slow marginalization away from conventional society and toward a much narrower society where extremism becomes all-encompassing.’136 This nuanced observation also fits our view of violent extremist behaviour online.

In terms of volume, large numbers of users might flirt with VE content before rejecting it; others might stumble through VE ecosystems without fully appreciating their worldview, culture and ideology. As a result, a necessary key assumption of this model is that a diminishing number of users will progress through each of these stages.137 However, those that do will exhibit increased levels of affinity with VE with clear security and policy implications. Publicly available case studies highlight how eclectic these pathways and engagement with technology and violence can be.138 However, when these processes of change are taken in aggregate, the key dynamic is not speed of user change but overall progress of the entire ecosystem. VE campaigners and actors do not need to convince the entire system to have a disruptive impact downstream through inspired or networked violence. Whether a given user ultimately radicalises or undertakes an act of violence does not necessarily matter to the overall resilience and function of the ecosystem. That user’s presence alone benefits the system because it allows the ecosystem to continue to exist. Through that ecosystem someone, even if it is not that single user, will act. This dynamic might be driven by aggregate statistics if nothing else.


136 Horgan, 2008, p. 89.

137 Horgan, 2008, p. 89.

Counters

The model has practical applicability through its illustration of the potential gaps or disconnects between observable patterns of violent extremist behaviour and policy focus. For example, many Prevent/Counter VE (P/CVE) programs that emphasise social cohesion and community resilience operate at Stage 1 (these programs were generically referred to as social policies in Figure 2.1). Stage 1 is also likely to be the area, because of the presence of mainstream social media platforms and mass audiences, in which deplatforming is most evident.

However, law enforcement and other agencies presumably prioritise their operational efforts at Stages 4 and 5, when the risk of violence, and offline connectivity with terrorists is much higher. Here, as indicated in Figure 2.1, these operational efforts were the more punitive and preventative policy measures used by governments. Therefore, the model suggests that there are policy and intervention gaps across Stages 2 through 4 and that a more granular appreciation of online behaviours in this area could inform how CVE online interventions might be developed to mitigate these risks.

Given the mapping of existing policy coverage, we suggest there might be a bell curve of radicalisation risk that rises through Stages 1 and 2, peaks at the centre of the model, then declines in the sense that, if an intervention has not been successful by the point of user transition into VE, it could well be too late to successfully intervene at all. This is illustrated in Figure 5.2, in which we identify a ‘tipping point’ that could be considered a position where a pivot from P/CVE towards more-explicit CT-based interventions is required. By understanding the nuance of these push-and-pull factors, VE actors and campaigners, transitions and ecosystem culture and identity, we can better consider developing what Horgan describes as ‘phase-specific counterterrorism initiatives . . .’\textsuperscript{139} The policy implications of this analysis are explored further in Chapter 6.

\textsuperscript{139} Horgan, 2008, p. 93.
Figure 5.2. Bell-Shaped Distribution of ‘Unchecked’ Campaigner Activity
We discuss a variety of implications in this chapter. Against each issue, we propose recommendations for further research. These recommendations have been provided to promote thinking and discussion around the issues. In that sense, the recommendations are neither exhaustive nor suggestive that such issues are not currently being considered. However, we suggest that understanding VE as an ecosystem that evolves, persists and displays different types of behaviour through time might prompt policymakers and operational practitioners to think of different, new and perhaps more-effective solutions to engage with and challenge online VE.

The Violent Extremism Ecosystem Is a Significant Threat

The importance of understanding the VE landscape as an ecosystem is vital for accurately assessing the nature of the threat of VE and the spectrum of behaviours within the ecosystem. Although the Engagement Model presented in the Chapter 5 depicts the various levels of engagement in a simple two-dimensional framework, it should be interpreted as a VE ecosystem that encompasses a variety of ‘sociotechnical networks within a hierarchy of systems.’

Approaching examination of the VE landscape as an ecosystem involves, as Hutchinson et al. observe, ‘the examination of users, their sociotechnical networks within a hierarchy of systems, their user experiences within these networks, and how these systems develop from internal and external pressures.’ In the Engagement Model, for example, Stage 5 should not be understood as an independent stage but as one that encompasses all the preceding stages. The progress a user might make from being a consumer of VE content, to an actor, and perhaps ultimately a campaigner, describes behaviour, or ‘user experiences within these networks’, within each stage. This concept remains consistent with the idea that there are antecedents and attributes developed and outcomes sought through each stage. The model represents how the users who enter the ecosystem adapt their behaviour as their engagement increases. This might be in direct response to how the established actors and campaigners deliver and tailor their content with respect to the technology and the platform and its associated governance (or lack thereof), but the presumption is that each individual user has to decide to progress. The campaigner is a facilitator of access. An examination of the Engagement Model from the perspective of the VE campaigner illustrates how, to achieve their core online objectives, they must inhabit each of these different stages simultaneously and maintain user access to

- all other parts of the network
- organisational and movement content

140 Hutchinson, 2022, p. 5.
141 Hutchinson, 2022, p. 5.
142 Hutchinson, 2022, p. 5.
143 Smith, 2019.
• diverse and broad audiences, depending on their specific role.

This maintenance is fundamental to ensuring that VE campaigners can reach, influence and cultivate, recruit and deploy others both online and offline. As we have seen through the detailed thematic analysis of an expansive dataset of primary VE content, at least four distinct and diverse patterns of behaviour—account obfuscation, cross platform networking, security and content engagement—can be distilled. These behaviours are practised in different ways and at different levels across the engagement model, forming aggregate responses to or ‘develop[ing] from, external and internal pressures.’

As expansive as this dataset was, and insightful the analysis is, it should be noted that this research constitutes only a preliminary determination of the behaviours exhibited by VE actors online. Therefore, our initial recommendation is to undertake further examination of the behaviours of VE actors in the online world to gain insight into the prevalence of specific antecedents and attributes exhibited through stages of engagement. If we are to understand the problem as an ecosystem, we need to examine the behaviour exhibited by the entire system. On this point, Micheron has identified sinusoidal patterns that are associated with the dynamics of terrorist activity, and which constitute periods of ebb and flow of the ecosystem. In the flow phase, ‘the movement emerges from the shadows’, and ‘followers prioritize warlike jihad—physical struggle.’ In this phase, there is a heightened public profile and intensified activity. This draws ‘nonstop media coverage of these operations, especially on social networks’ which might serve to ‘galvanize supporters, seduce recruits, and intimidate opponents.’ Certainly, ‘[p]ublicity for the jihadists represents an essential component of terrorism particularly during these assertive periods.’

The ebb phase, which can also be understood as the ‘retreat’ phase, is where ‘the jihad appears to have been defeated.’ In this phase, the logic is that of ‘ideological and intellectual reconfiguration.’ Micheron observes that the prioritisation becomes ‘immediate adaptation to the new legal or security situation.’ Although there might still be attacks, ‘the security threat level has dropped considerably,’ at least in the most immediate sense. As Micheron describes,

Physical struggle gives way to ideological subversion from outside or within ‘unbeliever’ countries. The supporters strive to stay off the radar, to minimize their punishment when they are tried, even if it means formally dissociating themselves from their former terrorist affiliations or minimizing the extent of their involvement.

Under these conditions, the ideological framework might be more problematic than the actual acts of violence.

---

144 Hutchinson, 2022, p. 5.
145 Micheron, 2022, p. 11.
146 Micheron, 2022, p. 11.
147 Micheron, 2022, p. 13.
149 Micheron, 2022, p. 13.
150 Micheron, 2022, p. 13.
The typology of online behaviours developed, as shown in Figure 4.2, represents only a small window of VE activity. Whether this window sits within the ebb or flow phase has not been determined, and, until it is situated relative to this overall pattern, it might not be possible to ascertain how the actor behaviour observed is consistent with either phase or whether the situation itself is what is currently characterising the behaviour. In other words, the observation of the tools, tactics, techniques and procedures, which evolve in and of themselves, might be applied in different measure given the overall strategy being pursued. This leads to our second recommendation: **Extend and test the typology of online behaviours to better understand how they change relative to observed ecosystem behaviour.**

**There Is a Heightened Need for Capacity, Expertise and Situational Awareness**

To fully understand, respond to, counter and inhibit an ecosystem (both online and offline) requires a fundamentally different approach to that currently being practiced, which is largely focused on the manifestations of the system (be that content on platforms or the targeting of individuals). It must be complemented, perhaps even superseded, by an approach that recognises the behaviour of the entire system.

Fundamentally, this means understanding what is occurring during not only the peaks but also the troughs of activity and ensuring that decisionmaking uses ‘constant, not episodic, engagement.’ The approach requires the expertise and awareness to decide, as Raine argues, ‘whether a reduction in the amount of visible terrorist activity means extremists have genuinely reduced that activity, or whether they are planning something big’.152

On this point, Raine suggests that the decisive piece, and the challenge, is the development of the ability to ‘listen to and interpret the quiet times’ and to discern whether ‘it is actually quiet or whether an adversary is taking advantage of a lull to resupply and plan? And how do we make resource decisions if we can’t answer these questions?’153 The only way to develop this expertise is through constant, meticulous risk management; finding new ways to maintain a state of vigilance while accepting limitations on resource and reduction in vision. The real task for today’s policymakers is not about pivots and tilts but how to keep situation awareness and retain expertise so you’re agile enough to produce the right strategic response, ideally before the situation escalates.154

This necessarily requires greater situational alertness and responsiveness, and the purposeful consideration of VE alongside other national security issues and trajectories. VE, including its online manifestation, should not be conceptualised by policymakers, as a discrete area of subject-matter expertise. Such an approach will result in the failure to fully grasp the complexity

---

151 Micheron, 2022, p. 13.
of the issue and the thriving nature of an ecosystem that evolves in the online and offline worlds synchronously. This prompts our third recommendation: **Identify minimum viable capabilities to maintain vigilance of evolving online VE, including consideration of policy and technology infrastructure.**

**Counters Must Be Consistent with the Threat**

If the focus is to extend to the entire problem, then we must similarly extend counters beyond those who are entering or exiting the system. Governments tend to focus more on the physical manifestations of the ecosystem by pivoting policy in response to actual acts of violence, but this approach is no longer sufficient. Deplatforming has had a profound impact in terms of creating space for disruptive alternative-technology platforms, including highly encrypted ones, to emerge and compete for audiences, including violent extremists. Violent extremists are clearly adapting their behaviours to circumvent deplatforming policies and evade law enforcement, becoming first movers who are highly incentivised to tailor, obfuscate and exploit the online environment according to societal and political shifts and technological advancements. It has also been suggested that ebbs in VE activity might represent even more risk than do the flows that naturally attract much more of these preventive or punitive counter. Conversely, governments could focus on addressing factors that might prompt people to join an ecosystem, but these factors are long-standing socioeconomic issues that could require years and investment to address.

To develop the most effective counters, policy development must have the correct focus, and policymakers must recognise the extent to which the terrorist threat is able to thrive in the context of policy trends and best practice. Raine argues, ‘Western governments must wake up to the uncomfortable reality that when terrorists go quiet, they might be planning something big.’\(^{155}\) The ebb phase could be more dangerous than the flow phase.

If this is the case, policy must be made consistent with the threat. Governments must recognise that there might need to be an urgent shift in the way they conceive of the problem. On this point, Raine observes that the operational cycle of terrorists and that of Western governments are fundamentally different and even at odds with one another. She notes that they crank up activity at precisely the moment the West starts to relax. In practice, the threat is most dangerous before, not after, it materialises, so the risk might well be greatest before it is apparent. This requires us to think counter-cyclically, to resist the gravitational pull of the political and resource cycle, and to organise ourselves around the rhythm of the adversary rather than our own.\(^{156}\)

Thus, there appears to be a gap between current measures where the threat exists and might be most dangerous before it is even evident. To better understand this gap, thinking might need to run counter to what apparent trends indicate and government policy dictates. As a first step to better understanding what is happening, we must **review the variety of existing approaches to identify and define VE operational cycles.**

---

\(^{155}\) Raine, 2021.

\(^{156}\) Raine, 2021.
There is an advantage to be had in the fact that these analyses emerge divergently from a variety of sources and they may identify more detailed gaps in understanding when synthesised than individually. For example, analysis has been conducted within data-rich environments, in which there is limited technological infrastructure. Different analysis occurs when working within a data-poor environment or with poor data. This is usually conducted in after a major terrorist or extremist event and using only publicly available information. Analysis can be made quite quickly during short term operations at the microscale, but there are very few longer-term or longitudinal studies at the macroscale.

The Relative Immaturity of Racially or Ethnically Motivated Violent Extremists Could Be Exploited

In this report, we have focused on IMVE because global trends and data indicate that it continues to persist as a foremost concern in the VE landscape, including the online landscape. Ideologically motivated violent extremists continue to work at a high tempo, often in connection with or in ideological support of global brands such as al Qaeda and IS. As the conflict zones in which these organisations are engaged morph and evolve, it is to be expected that ideologically motivated violent extremists will continue to do the same globally and online. Therefore, it is important to appreciate the interplay between distant conflicts and local ideologically motivated violent extremists that is reflected in in the ebb-and-flow conceptualisation.

This reality leads us to consider how we could directly leverage the research findings of our focus on IMVE to REMVE, which is of increasing concern in English-language-speaking environments. As evidenced in previous chapters, we assert that IMVE virtual ecosystems have evolved through sophisticated adoption and adaption of technology and online behaviours. This evolution might be in response to the relentless pursuit of IMVE actors and campaigners after 11 September 2001. Nevertheless, examination of the evolution renders a much more advanced understanding of how other VE ecosystems might also evolve. As policymakers and practitioners, we must learn to understand how situations of both IMVE and REMVE are simultaneously true and how they can feed off and learn from one another. There might be implications for REMVE, the ecosystem which is arguably in a place of relative immaturity in terms of how it exploits digital technology and the online world. By leveraging our knowledge of IMVE actors, we might be able to build better responses to the REMVE ecosystem as it evolves because of the attention it is currently attracting from governments. This leads to our fifth recommendation: Map REMVE ecosystems against a variety of IMVE systems to determine their relative maturity and identify likely trajectories along which they might progress.

A Grand Strategy for National Security Might Be Required

Beyond linking different VE ecosystems, governments should recognise that VE does not occur separately from other events and issues. Just as governments increasingly look at how to better manage the concurrence of events in other areas (e.g. between disaster management, national resilience, and democracy), they might need to better understand, for example, any
interplay between terrorism, extremism (non-state-based action), and foreign interference (state-based action), particularly because of the opportunities presented in the online world for these lines to blur.\textsuperscript{157}

As a result, and by way of example, policymakers might need to determine the potential for foreign interference to occur in the facilitation of targeted VE. Our final recommendation is that collaboration between disparate groups across this landscape is fundamental to improving situational awareness. As a priority, the interplay and overlaps between terrorism, extremism, foreign interference and misinformation and disinformation should be investigated.

Beyond the use of violence, targeted VE could manifest in different ways that are socially and politically harmful over the long-term depending on whether the context was REMVE (conspiracy theories, antigovernment rhetoric, truth decay, etc.) or IMVE (antidemocratic rhetoric and the cultivation of social polarisation, etc.). The interplay of this set of issues is deserving of further research. Countering either would involve strategies that address both disinformation and institutional mistrust, although for the latter very different institutions would be involved for REMVE and IMVE. It might be this mistrust that causes people to look to REMVE or IMVE for solutions.

\textbf{Conclusion}

VE online is increasingly characterised by the exploitation and manipulation of online and offline systems, the ability to maintain influence and connectivity in sophisticated ways and a complex and inextricable interface with broader national security issues. The gamut of stakeholders involved in CVE will need to recognise the requisite capacity for addressing this multifaceted and dynamic landscape and the need to prioritise efforts and resources. Situational awareness is required now more than ever and across a spectrum of interrelated areas, rather than simply pivoting to the current priority. Although the ebb might represent a lesser physical threat than flow, it provides opportunities to build resilience, better understand how an event might arise, develop warning times, and better plan and prepare for terrorist shocks. There should be incentive to pursue these ends: The VE ecosystem represents a danger that has the potential to threaten society.

\textsuperscript{157} Butler, 2022.
Appendix. Case Studies: Buffalo and Bratislava

The May 2022 attack in Buffalo and October 2022 attack in Bratislava both illustrate the ease of access that racially and ethnically motivated violent extremists have to online ecosystems that support their beliefs and plans for violence.

Case Study 1: Buffalo

On 14 May 2022, an attacker killed ten Black people and injured three others at a supermarket in Buffalo, New York. According to the New York State Attorney General’s subsequent report, the attacker used ‘Discord to keep a private journal for months, where he wrote down his hateful beliefs and developed specific plans for equipping himself and perpetrating his massacre. He livestreamed his attack through both Twitch and Discord.’ With regards to ideology, ‘[t]he Buffalo shooter’s indoctrination into internet hate culture is most strongly linked to his use of 4chan.’

Case Study 2: Bratislava

In a more recent example, on 12 October 2022, an individual attacked a LGBTQIA+ bar in Bratislava, Slovakia, killing two and injuring another before dying by suicide. Reflecting the extent to which REMVE-inspired attackers influence one another, the Bratislava attacker had been heavily influenced by the Buffalo attacker. He claimed in a manifesto that the Buffalo attacker had ‘managed to damage the cohesiveness and safety of an entire community. Enough attacks like this, or individual attacks on a large enough scale against a small enough group, can easily uproot an entire community’. In the manifesto he gives ‘special thanks’ to the founder of 8Chan and references his ‘switch to Telegram’. 8Chan was created in 2013 by Fredrick


162 Juraj Krajčík, A Call to Arms, 2022, p. 18.

163 Krajčík, 2022, p. 63.
Brennan, although he later stepped away from the project and disowned it.\textsuperscript{164} The platform was embroiled in multiple controversies because it hosted REMVE content.\textsuperscript{165}

However, according to the ADL:

\begin{quote}
[U]nlike prior mass shooters, who have generally uploaded their hate-filled screeds to fringe platforms like 4chan and 8chan, the Bratislava gunman uploaded his manifesto to multiple anonymous file sharing sites before disseminating a link to it on Twitter . . . . According to a review of his social media presence, the shooter had maintained a Twitter account since April 2021, on which he publicly shared white supremacist rhetoric and imagery for over a year.\textsuperscript{166}
\end{quote}

The interplay with other platforms is evident, as

\begin{quote}
[a]mong his tweets were racist slurs, white supremacist 4chan screenshots, posts glorifying other mass shooters and Nazi war criminals as heroes, and several images of the Nazi sonnenrad symbol, which has been used by white supremacists and other mass shooters, including the Buffalo and Christchurch shooters. The attacker also used Twitter to repeatedly hint at plans for carrying out an act of mass violence.\textsuperscript{167}
\end{quote}

The attacker appears to have recognised the ability to reach audiences on Twitter while being uber critical of the platform’s values. He would claim that, ‘Social media from the West and East—Twitter, Instagram, Tiktok—has done its dirty work, and the decline is now accelerating.’\textsuperscript{168}

\begin{flushleft}
\textsuperscript{164} Brennan, Frederick R., ‘About Me’, webpage, undated.


\textsuperscript{166} Anti-Defamation League Center on Extremism, \textit{Bratislava Shooter Promoted White Supremacist Content on Twitter for Over a Year}, ADL Blog, 14 October 2022.

\textsuperscript{167} Anti-Defamation League Center on Extremism, 2022.

\textsuperscript{168} Krajčík, 2022, p. 13.
\end{flushleft}
**Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AQAP</td>
<td>al Qaeda in the Arabian Peninsula</td>
</tr>
<tr>
<td>CT</td>
<td>counter terrorism</td>
</tr>
<tr>
<td>CVE</td>
<td>countering violent extremism</td>
</tr>
<tr>
<td>DWeb</td>
<td>decentralised web</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>IMVE</td>
<td>ideologically motivated violent extremism</td>
</tr>
<tr>
<td>IS</td>
<td>Islamic State</td>
</tr>
<tr>
<td>JNIM</td>
<td><em>Jama’at Nasr al-Islam wal Muslimin</em> (Group for the Support of Islam and Muslims)</td>
</tr>
<tr>
<td>REMVE</td>
<td>racially and ethnically motivated violent extremism</td>
</tr>
<tr>
<td>RMVE</td>
<td>religiously motivated violent extremism</td>
</tr>
<tr>
<td>Tor</td>
<td>The Onion Router</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>VE</td>
<td>violent extremism</td>
</tr>
</tbody>
</table>
References

4chan, homepage, undated. As of 22 May 2023:
https://www.4chan.org

8kun, homepage, undated. As of 22 May 2023:
https://8kun.top/boards.html


Anti-Defamation League Center on Extremism, ‘Bratislava Shooter Promoted White Supremacist Content on Twitter for Over a Year’, *ADL Blog*, 14 October 2022.


Australian Security Intelligence Organisation, ‘Director-General’s Annual Threat Assessment’, webpage, 17 March 2021. As of 22 May 2023:


Bodó, Loránd, and Inga Kristina Trauthig, *Emergent Technologies and Extremists: The DWeb as a New Internet Reality?* Global Network on Extremism and Technology, 1 August 2022.


Clifford, Bennett, Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States, Program on Extremism, George Washington University, 2021

Clifford, Bennett, and Helen Powell, Encrypted Extremism, Inside the English-Speaking Islamic State Ecosystem on Telegram, Program on Extremism, George Washington University, June 2019.


Conway, Maura, Ryan Scrivens and Logan Macnair, Right-Wing Extremists’ Persistent Online Presence: History and Contemporary Trends, International Centre for Counter-Terrorism, October 2019.


Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes, United Nations Counterterrorism Community, 29 October 2022.


Gilbert, David, ‘8chan Is Back from the Internet Grave—and It Has a New Name’, *Vice News*, 9 October 2019.


Global Internet Forum to Counter Terrorism, ‘GIFCT’s Hash-Sharing Database’, webpage, undated-a. As of 22 May 2023: https://gifct.org/hsdb/
Global Internet Forum to Counter Terrorism, ‘Story’, webpage, undated-b. As of 22 May 2023: https://gifct.org/about/story/


Hoffman, Bruce, ‘The Use of the Internet by Islamic Extremists’, testimony before the House Permanent Select Committee on Intelligence, RAND Corporation CT-262-1, 4 May 2006. As of 22 May 2023: https://www.rand.org/pubs/testimonies/CT262-1.html


Hutchinson, Jade, Julian Droogan, Lise Waldek and Brian Ballsun-Stanton, Violent Extremist and REMVE Online Ecosystems: Ecological Characteristics for Future Research and Conceptualization, Resolve Network, August 2022.

I’lам Foundation, homepage, undated.


Jihadology, ‘Frequently Asked Questions’, webpage, undated. As of 22 May 2023: Jihadology.net/about/faq/


Krajčík, Juraj, A Call to Arms, 2022.


Schmid, Alex P., Violent and Non-Violent Extremism: Two Sides of the Same Coin? International Centre for Counter-Terrorism, May 2014.


Tech Against Terrorism, ‘About Tech Against Terrorism’, webpage, undated-a. As of 22 May 2023:
https://www.techagainstterrorism.org/about/

Tech Against Terrorism, ‘Welcome to the Knowledge Sharing Platform’, webpage, undated-b. As of 22 May 2023:
https://ksp.techagainstterrorism.org/

Telegram, ‘Bots: An Introduction for Developers’, webpage, undated. As of 22 May 2023:
https://core.telegram.org/bots/

Tor Project, ‘History’ webpage, undated. As of 22 May 2023:
https://www.torproject.org/about/history/


https://www.rand.org/pubs/research_reports/RR453.html


https://www.youtube.com/watch?v=7knxgWSEgr8

https://www.rand.org/pubs/perspectives/PEA1458-1.html


In this report, the authors seek to understand how violent extremists behave in an increasingly complex online ecosystem. This ecosystem, which is characterised by technological innovation and diversification of platforms, offers significant utility and advantages to violent extremists. By interrogating the variety of tactics and strategies being used globally, the authors have identified gaps in the understanding of the expansive contours of the violent extremism (VE) online landscape. The study highlights the extent to which these challenges require enhanced policy settings.

Violent extremists have learned to adjust their behavioural posture through a variety of tactical measures to evade common counters. Although law enforcement agencies are conscious of how enforcement and denial actions change behaviours, there will always be a trade-off between keeping extremists where they can be monitored online and deplatforming them to reduce potential harm. Some of the ongoing adaptations of violent extremists are illustrated in this report, using case studies and examples from a variety of different platforms. At the strategic level, the authors dissect the ways in which violent extremist networks engage across alternative-technology and mainstream platforms according to the opportunities afforded by each platform. Developing a greater, more detailed understanding of the online VE landscape is imperative because of the extraordinary proliferation of VE activity online.