CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

CSCRC SUBMISSION:

PJCIS INQUIRY INTO EXTREMIST MOVEMENTS AND RADICALISM IN AUSTRALIA

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: ***Inquiry into extremist movements and radicalism in Australia***

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Parliamentary Joint Committee on Intelligence and Security's *Inquiry into extremist movements and radicalism in Australia*. Such an inquiry is both timely and pertinent given the increasingly complex geopolitical environment, the ongoing effects of the COVID-19 pandemic and the immense impact the internet has, and will continue to have, on communications and the dissemination of information.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding this very important inquiry.

Yours Sincerely,

[redacted]

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
[redacted]

Introduction

Australia is no stranger to extremism. Over time, since the loss of innocence marked by the 1978 bombing of the Sydney Hilton Hotel, through to the rise of Islamic State of Iraq and Levant (ISIL), Australian governments and citizens have increasingly had to grapple with the rise of terrorism and extremist ideologies and their impact on national security and the principles of democracy. And, just as society has evolved during this time, so has the environment in which extremism, radicalism and terrorism proliferate and operate.

Ours is a cyber-enabled world, where messages of hate can be dispersed over the internet with the click of a button and shared with millions; where like-minded radicals can communicate clandestinely via encrypted messaging services and the dark web; and where mass terror events can be broadcasted in real-time to viewers around the world. Hence, "the nexus between terrorism and technology is socially and politically more relevant than ever. Almost every mobilisation and radicalisation process and every violent attack, whether carried out or prevented, has an online component to it". [1]

Perversely, cyber security and the privacy afforded by its evolution has acted as a near perfect conduit for extremists to plan and facilitate. It is a clear example of where the law has failed to keep pace with technological developments.

Frissen rightly points out that "radicalisation is not a linear, step-by-step process, but rather a multifactorial and contextual phenomenon", taking into account active online exposure to extremist materials, moral disengagement and socio-behavioural factors.[2] It is *cyber-enabled* as opposed to *cyber-dependant*, with social media, extremist forums and underground communities playing a key role in fostering connections and bonds and influencing views and behaviours, which ultimately nurture and reinforce extremist ideologies.[3]

As noted by the Director-General of Security, Mike Burgess, in the Australian Security and Intelligence Organisation's (ASIO) 2019-20 Annual Report: "Australia's threat environment is complex, challenging and changing ... Individuals in Australia continue to be radicalised, and

---

[1] https://gnet-research.org/wp-content/uploads/2021/01/GNET-Report-Researching-Extremist-Content-Social-Media-Ethics.pdf, P1
[2] Frissen, Thomas. *"Internet, the great radicalizer? Exploring relationships between seeking for online extremist materials and cognitive radicalization in young adults"*. Computers in Human Behaviour 114 (2021), 1-13
[3] Cherney, Adrian et al. *"Understanding youth radicalisation: An analysis of Australian data". Behavioural Sciences of Terrorism and Political Aggression"*. 2020

the online amplification of radicalisation messages is reaching ever-younger targets".[4] Australia's terrorism threat level remains at 'Probable', with Salafi-Jihadism presenting the greatest threat. However, right-wing extremism has increased, with ASIO indicating about one-third of its counter-terrorism investigations in 2019-20 involved such threats.[5]

In this submission, the CSCRC addresses extremist movements and radicalism in Australia through a cyber lens, with a focus on Salafi-Jihadism and right-wing extremism.
In particular, the CSCRC focuses on:

- The geographic spread of these extremist movements and persons in Australia and their links to international extremist organisations, taking into account the borderless nature of cyberspace;
- The role social media, encrypted communication platforms and the dark web play in allowing extremists to communicate and organise; and
- Further steps that could be taken to disrupt and deter extremism and radicalism online, bolstering the provisions of the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* and highlighting the important role the proposed Surveillance *Legislation (Identify and Disrupt) Bill 2020* could play in combatting such activity.

[4] https://www.asio.gov.au/director-generals-review.html
[5] Ibid 3

Salafi-Jihadism

The geographic spread of extremist movements in Australia and international links

Firstly, it is important to define Salafi-Jihadism, as it is not a philosophy that typifies nor characterises the vast majority of adherents to the Islamic faith. Nor is it monolithic. While ISIL is now the most prominent Salafist group, there is estimated to be more than 60 currently active, including other well-known groups like al-Quaeda, al-Shabaab, Boko Haram and Jabhat al-Nusra.[6]

Maher describes Salafism as "a philosophy that believes in progress through regression ... seeking to bring Muslims back to what is regarded as the 'authentic' and 'pure' Islam of its early generations ... By attempting to emulate the practices of Islam's supposedly golden era, Salafists believe that only they constitute the so-called 'victorious group' or 'saved sect'".[7] There is also a keen focus on the formation of a 'caliphate' – an Islamic state led by a caliph,[8] which operates according to fundamentalist interpretation of shari'a law,[9] and jihad, an armed struggle against outsiders.[10]

In the early years of the 21st century, Islamic extremism in Australia largely existed on the fringes of public consciousness. But that changed with the rise of ISIL and the subsequent rush of homegrown jihadis that fled to Syria, as well as a series of successful and thwarted domestic terror plots.

What these experiences clearly illustrated was the ability of ISIL and its influence to transcend borders much more effectively than other Salafist groups had previously achieved. A key driver was the group's sophisticated media arm, the al-Hayat Media Center and Al Furqan, which leveraged the internet and its worldwide reach to spread slick propaganda.

As noted by *Williams:*

> *"The group's prodigious propaganda output has ranged from feature-length videos, social media networks, published newspapers, and a glossy magazine – Dabiq – through to radio programs and smartphone apps. Content has been produced in English, Arabic, Russian, Urdu, Turkish, and even Hebrew. The group has also staged made-for-media terrorist events, such as the spectacles of beheadings, which specifically target Western audiences ... Unlike*

---

[6] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181221_EvolvingTerroristThreat.pdf
[7] Maher, Shiraz, *Salafi-Jihadism: The History of an Idea*, 2016, Oxford University Press, P7
[8] https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/
[9] https://www.sbs.com.au/news/explainer-what-is-sharia-law
[10] https://www.palgrave.com/gp/book/9780230111608

> *extremist propaganda videos of the past, which were often unsophisticated productions featuring terrorist leaders making long and boring sermons, Islamic State's videos are of a high quality. They use cinematic production techniques, Hollywood-style special effects, 'immersive' video game-style media, and dramatic, apocalyptic narratives to draw the viewer's attention and secure media coverage. The material is available online and disseminated on social media through a network of supporters on Twitter, Facebook, YouTube, Ask.fm, Kik, and Tumblr."*[11]

Exposure to radicalised networks and associates has been identified as a key contributor to individual radicalisation.[12] Hence, the geographic movement of Australian jihadis to Syria had an impact domestically, aided by the internet. This has been illustrated starkly in a number of court cases, whereby radicalisation and incitement of violence via online channels by Australian foreign fighters back to domestic supporters has been proven.

Three examples are the cases of Radwan Dakkak, Omarjan Azari and Zainab Abdirahman-Khalif:

- Radwan Dakkak was arrested on 16 January 2021 for breaching a control order enforced upon his release from prison on 1 January 2021. Dakkak was sentenced to 18 months' prison in December 2020 on two charges of knowingly associating with a member of ISIL, charges he was taken into custody for in 2017.[13] Between 2015 and 2017, Dakkak used social media and other online platforms to communicate with extremists around the world,[14] and was the first person in Australia to be prosecuted for associating with a member of a terrorist organisation. It is alleged that less than two weeks after his release, Dakkak failed to comply with a condition of his control order by accessing material online that supported the carrying out of executions, beheadings and torture.

- On 13 July 2016, Zainab Abdirahman-Khalif attempted to board a flight from Adelaide to Istanbul in a bid to cross the border to Syria and join ISIL but was detained by Australian Border Force officers. It was ascertained that, before purchasing the ticket to Turkey, Abdirahman-Khalif had used her mobile phone on a number of occasions to communicate with three Kenyan women referred to as "the Baaqiya sisters".[15] After examination, the mobile phone was returned to

[11] https://www.lowyinstitute.org/publications/islamic-state-propaganda-and-mainstream-media
[12] Ibid 3
[13] https://www.smh.com.au/national/nsw/two-weeks-out-of-jail-radwan-dakkak-allegedly-accessed-material-that-supported-beheadings-20210116-p56ulg.html
[14] Booth v Dakkak [2020] FCA 1882
[15] R v Abdirahman-Khalif [2020] HCA 36

Abdirahman-Khalif and she was allowed to leave the airport. Within 20 minutes of the phone being returned, she used it to warn one of the Baaqiya sisters not to contact her. On 11 September 2016, the Baaqiya sisters committed a terrorist attack at a Mombasa police station in the name of ISIL, in which they were killed. ISIL claimed responsibility for the attack.[16]

- Actor-turned-terrorist Ali Baryalei travelled to Syria to take up arms in 2013 and rose through the ranks to become one of the most senior Australian members of ISIL. He was also a key recruiter of Australian jihadis, who he communicated with online, encouraging the use of encrypted messaging services like Telegram. One of the young men he mentored was Omarjan Azari, who is currently serving an 18-year sentence for his plan, hatched by Baryalei, to behead up to seven random Australians a month.[17] In planning for the commission of these crimes, Azari often exchanged messages with Baryalei. One such message tendered as evidence at Azari's trial for terror offences read: "Listen, it's gonna be like this. I need you first of all to get a telephone and on that telephone I need you to get Telegram ... We're gonna speak, we're gonna speak through Telegram, Allah willing, because Telegram, apparently, praise be to Allah, is very good..."[18]

Despite COVID-19 and the widespread closure of international borders, it has been widely reported that Salafist groups have taken advantage of the pandemic to drive online recruitment. In August 2020, the UN Security Council noted a spike in ISIL's online activities targeting people in lockdown.[19] ISIL has also used the pandemic to incite terror attacks in the West, using its Al-Naba newsletter to encourage supporters to attack and weaken "infidels" and "apostates" in their time of crisis, and reminding followers Western states "will substantially undercut their ability to wage war on the mujahideen in the coming period".[20]

The role social media, encrypted communications platforms and the dark web play in allowing extremists to communicate and organise

The rapid proliferation of digital technologies and communications has been exploited effectively by Salafi-Jihadists, who were quick to realise the key role social media, encrypted communications and the dark web could play in supporting their activities. This is especially relevant in regard to ISIL, which rapidly adopted the use of digital platforms to organise and assemble. Smart phones have been a game-changer and, as academics have noted,

---

16 https://www.reuters.com/article/us-kenya-attacks-idUSKCN11H0AC
17 Omarjan Azari sentenced to 18 years' jail over plan to behead Australians - ABC News
18 R v Azari (No 12) [2019] NSWSC 314
19 https://www.aspistrategist.org.au/covid-19-and-the-threat-from-islamic-states-online-and-family-networks/
20 https://www.crisisgroup.org/global/contending-isis-time-coronavirus

"virtually all Salafi-jihadists, and many of their supporters, possess smart phones, even in battlefields like Iraq, Syria, Libya, and Afghanistan".[21]

In particular, encrypted messaging services and the dark web pose a significant challenge to law enforcement. While electronic surveillance powers do exist in Australia, they are simply not fit-for-purpose when it comes to the proliferation of encryption and dark web enabled extremism, which is increasing in scope and scale. It is difficult to detect and perpetrators are almost impossible to locate and identify.

In the early days of ISIL, Australian foreign fighters used social media, especially Twitter, to spread propaganda and communicate with other extremists. A defining image is one Khaled Sharrouf beamed around the world from his Twitter account in 2014, of his seven-year-old son holding up the decapitated head of a Syrian soldier. Likewise, Australian peers including Mohamed Elomar and Neil Prakash, began using Twitter and Facebook from Syria, inspiring would-be jihadists back home to join the caliphate. There were women too – Sharrouf's wife Tara Nettleton and Melbourne teenager Zehra Duman – urging Australians to travel to Syria while posing beside luxury cars and holding machine guns. These foreign fighters also used Twitter to incite homegrown violence. For example, Duman tweeted: "Kill kuffar in alleyways, stab them and poison them. Poison your teachers. Go to haram restaurants and poison the food in large quantities".[22]

Social media platforms, where jihadis from around the world were increasingly active, were forced to take action, with Twitter reporting in 2016 it had removed 125,000 terror-related accounts.[23] While this was undoubtedly the right course of action it proved a double-edged sword, forcing these extremists to find more clandestine ways to communicate.

Telegram and other encrypted messaging services

Telegram remains the "platform of choice" for Salafi-Jihadists,[24] with a spike in its use after Twitter cracked down on jihadi content. In addition to end-to-end encryption, Telegram has a suite of features that make it attractive. It allows multiple levels of communications, from private to public, via one platform, and even features a self-destruct timer that allows messages to permanently disappear after a stipulated period.[25] In addition, while some of Telegram's policies have changed and its operators have begun to collaborate (to an extent) with law enforcement,[26] it is unlikely Salafi-Jihadists will migrate from the platform in the foreseeable future given its features, familiarity and ease of use.

---

[21] Ibid 6, P 29
[22] https://thenewdaily.com.au/news/world/2019/10/08/zehra-duman-isis/
[23] https://www.bbc.com/news/world-us-canada-35505996
[24] https://gnet-research.org/wp-content/uploads/2020/11/GNET-Report-Migration-Moments-Extremist-Adoption-of-Text%E2%80%91Based-Instant-Messaging-Applications_V2.pdf P1
[25] Ibid 6 P33
[26] Ibid 22 P5

It is worth noting that the terror cell responsible for plotting and carrying out the murder of Sydney accountant Curtis Cheng in October 2015 used WhatsApp – another encrypted chat platform – to communicate in relation to the crime. The group – known as The Bricks Forum – were all under heavy counter-terrorism surveillance at the time. For them, WhatsApp offered a cloak of secrecy, a way to evade authorities. While intelligence operatives could piece together some parts of the puzzle, vital pieces were missing. This was because authorities did not have the powers necessary to access these encrypted communications.

Telegram is but one of many encrypted messaging apps favoured by Salafi-Jihadists – others include Surespot, Signal, Wickr, Kik, ChatSecure, BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat and TamTam.[27] There is also a high risk that if, as planned, Facebook adopts end-to-end encryption across its services, it will act as a new forum through which extremists can conceal their communications and activities.

In a concerning prediction, Jones et al have noted that moving forward, "Salafi-jihadist groups will likely migrate to new platforms and services to disseminate their messages. Many of these companies may not be Western-based like Twitter, YouTube and Facebook, but might instead move around—with servers in undisclosed locations—to evade law enforcement and intelligence agencies".[28]

Examples: Encrypted messaging apps and use by Salafi-Jihadists
• In 2007, al-Qaeda released an encryption tool named "Asrar al Mujahideen," or Mujahedeen Secrets.
• In 2010, al-Qaeda-linked operatives in Germany encrypted their communications using Mujahedeen Secrets.
• Between 2014 and 2015, Junaid Hussain, a British ISIL operative and member of a group nicknamed "Legion" by the FBI, was a prolific user of the encryption messaging app Surespot. He provided Islamic State sympathisers in the UK Kingdom with bomb-making tips and encouraged them to carry out attacks.
• The perpetrators of the November 2015 Paris attacks used encryption to communicate with each other. Messaging services Whatsapp and Telegram were found on the phones of the suspects.

Source: The Evolution of the Salafi-Jihadist Threat, P 58

The dark web

The dark web is not like the surface web, the external interface of the internet most people are familiar with. And, while it does serve altruistic purposes, such as giving a voice to

[27] Ibid 22 P1
[28] Ibid 6 P33

people living under oppressive regimes, the dark web is overwhelmingly a place of ill intent. It is part of the internet that evades indexing by search engines, instead requiring the use of an anonymising browser (like Tor) that routes traffic through multiple servers, encrypting it along the way. To help ensure anonymity, dark web browsers isolate sites to prevent tracing, automatically clear browsing history, prevent surveillance of connections, clone or dupe users' appearances to avoid fingerprinting and relay and encrypt traffic three times as it runs across the network.

Given the anonymity the dark web affords, it is unsurprising it has been exploited by Salafi-Jihadists, who can communicate securely through dark web platforms. In August 2015, ISIL published a 15-page 'how-to guide' in its French online magazine Dar al-Islam, highlighting the importance of secure communications and instructing users how to connect to the Tor network to hide internet addresses and locations, encrypt emails, and perform other functions.[29] The dark web also provides a platform for other terrorist activities such as the dissemination of propaganda, fundraising through cryptocurrencies and the buying and selling of weapons and other illicit goods.[30]

The dark web and terrorism
• After the 2015 Paris attacks, ISIL announced its Isdarat website, a propaganda archive, would be moved to the dark web due to increasing pressure on surface web sites.
• It is believed the guns used for the 2015 Paris attack were bought on the dark web from a German vendor, DW Guns.
• In June 2017, the UN's disarmament chief warned that terrorists and non-state actors were using the Dark Web to seek tools to make and deliver weapons of mass destruction.

Source: The Evolution of the Salafi-Jihadist Threat, P 40

Future developments

As law enforcement agencies in Australia and the world continue to grapple with the challenges to counter-terrorism posed by encryption and the dark web, there is no doubt Salafi-Jihadists will continue to seek new and innovative ways to conduct counter-surveillance. Hence, while the introduction of laws to help authorities overcome the difficulties posed by deep encryption are undoubtedly necessary, it would be naïve to believe extremists will not pivot to new methods.

[29] Ibid 6 P58
[30] Ibid 6 P39

Some scholars have predicted "the decentralised web seems to be the next logical step not only for IS, but also for other (violent) extremists online trying to evade authorities and take-downs".[31] This would in effect mean groups would be able to store data and communicate via their own servers, mitigating the effect of content takedown by creating an independent, decentralised storage network outside the grasp of service providers and law enforcement.[32]

It is also likely Salafi-Jihadists will move to encrypted platforms produced outside the West, shifting to those produced in less stringently governed locations like the Middle East, North Africa, East Africa and the Sahel.[33] To this end, it is also likely such groups will move to build their own encrypted platforms or purchase already developed platforms from the dark web.[34]

Right-wing extremism

The geographic spread of extremist movements in Australia and international links

Right-wing extremism (RWE) is not easily defined. Nor is it as well organised geographically or internationally as per other forms of radicalism and extremism.[35]

As the United Nations (UN) noted in 2020, RWE:

> *is a not a coherent or easily defined movement, but rather a shifting, complex and overlapping milieu of individuals, groups and movements (online and offline) espousing different but related ideologies, often linked by hatred and racism toward minorities, xenophobia, islamophobia or anti-Semitism. Although extreme right-wing terrorism is not a new phenomenon, there has been a recent increase in its frequency and lethality, with some individuals, groups and movements pursuing transnational aims in a national context, drawing on international networks, ideas and personalities and seeking to mobilize others, often using the internet.*

Furthermore, according to the *Global Terrorism Index 2020*, RWE attacks in North America, Western Europe and Oceania increased 250 per cent between 2014 and 2020.[36] The Index also highlights the dispersed nature of RWE, with violent attacks more likely to be carried out by individuals unaffiliated with a specific group.[37]

---

[31] Ibid 22 P23
[32] Ibid 22 P23
[33] Ibid 6 P37
[34] Ibid 6 P37
[35] https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf P2
[36] https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf P3
[37] Ibid 36 P3

Despite the scattered nature of RWE, there is evidence it is becoming increasingly transnational, a trend fuelled by digital platforms and the internet. According to the UN, RWE movements amplify and recruit both online and offline, enabling them to "improve their tactics, develop better counter-intelligence techniques, solidify their violent extremist views and broaden their global networks".[38]

In an Australian context, owing to a dearth of court rulings in relation to RWE, it is difficult to build a clear picture of how radicalisation occurs and is reinforced. However, several recent cases indicate the key role the internet and, likely, international links, play in RWE. The radicalisation and online interactions of Christchurch terrorist, Australian Brenton Tarrant, will be explored separately.

- In December 2020, Tyler Jakovac was arrested in Albury and subsequently charged with urging violence against members or groups and advocating terrorism. Jakovac – who police said held neo-Nazi, white supremacist and anti-Semitic views – was arrested after allegedly expressing support for a "mass casualty event, and potentially his involvement in that event".[39] Police said Jakovac used private social media groups to discuss such plans with like-minded individuals and had used social media to access RWE material, including bomb-making materials.[40]

- In March 2020, two brothers, Joshua and Ben Lucas from the NSW south coast, were arrested and charged in relation to an alleged terror plot to attack an electrical substation. Counter-terror investigators were alerted to the brothers through several online posts allegedly containing RWE political and anti-government ideology.[41]

- In September 2016, Ricky White set fire to a Christian church in Taree while conducting a letterbox drop for an RWE group he was leader of in Australia, Right Wing Resistance (RWR). RWR originated in New Zealand and, via online channels, White was asked to grow the group in Australia. He had previously been a member of other RWE groups Combat 18 and Blood and Honour. White was convicted of the arson attack in December 2016 and, after his release, was subject to an extended

[38] Ibid 35 P4
[39] https://www.smh.com.au/national/nsw/teenager-arrested-over-alleged-terrorism-offences-in-nsw-20201209-p56m0q.html
[40] https://www.theaustralian.com.au/breaking-news/teenager-18-arrested-by-counter-terrorism-police-in-albury/news-story/8e53856dba75e4fb9e621da8811b235a
[41] https://www.abc.net.au/news/2020-03-16/man-charged-over-allegedly-planning-terror-attack/12058756

> supervision order (ESO) for breaching parole conditions by accessing neo-Nazi materials online.[42]

It is also worth noting the findings of the *Mapping Networks and Narratives of Online Right-Wing Extremists in NSW* project,[43] which was undertaken after the Christchurch terror attack. For the project, anonymised data was collected from Twitter (37,422 tweets from 3,321 users), Gab (1,357,391 toots from 23,836 accounts) and a sample of archived message boards on Reddit, 4chan and 8chan (now named 8kun), and analysed to generate insights into RWE in NSW.[44] It found that, while fluid and relatively disjointed, RWE groups in NSW were active and shared commonalities,[45] combining an online and offline presence and illustrating "the desire and ability to link with their compatriots abroad, particularly in North America (including Canada), the United Kingdom, and Europe ... Connectivity has been established online and through limited travel".[46]

The role social media, encrypted communications platforms and the dark web play in allowing extremists to communicate and organise

There is clear evidence of the pivotal role the digital world has played in RWE radicalisation and terrorist attacks. As noted by Sold and Junk, RWE terrorists Brenton Tarrant (Christchurch, New Zealand) and Stephan Balliet (Halle, Germany) "took advantage of social media platforms not only to gather and distribute information, and to network and stage, but also to exchange ideas with like-minded people and sometimes even to share an attack live for thousands of viewers".[47] Likewise, Anders Breivik (Norway) was an active consumer of RWE online content and member of multiple extremist forums.[48]

Shanahan has observed that:

> *Although hateful and extreme, the right-wing extremist milieu is a highly social space. Social connections are created and maintained around shared values and norms engendering positive experiences for those involved in the networks. The content often conceals its revolutionary anti-government agenda behind appeals to nationalism and 'traditional' Australian values. These extremist perspectives are often presented through online content that is entertaining, provocative and supposedly ironic.*[49]

---

[42] State of NSW v White (Final) [2018] NSWSC 1943
[43] https://zenodo.org/record/4071472#.YCCtJugzaUn
[44] https://www.lowyinstitute.org/the-interpreter/after-christchurch-mapping-online-right-wing-extremists
[45] Ibid 43 P18
[46] Ibid 43 P21
[47] Ibid 1 P5
[48] https://journals.sfu.ca/jed/index.php/jex/article/view/28
[49] Ibid 44

Likewise, a recent Canadian study, which was based on interviews with former RWEs, found participants believed the internet played a key role in their radicalisation, providing them with access to a breadth of extremist material and the ability to meet and share content with like-minded individuals, reinforcing RWE beliefs.[50] Researchers state:

> *Following their initial exposure to violent extremist content online, study participants commonly reported that, because they wanted to feel like part of a group, they continued to use the internet to access a variety of forms of extreme right-wing content to indulge their 'newfound curiosity' in violent extremist ideologies. In fact, half the study participants spent a significant amount of time online every day accessing extremist content and immersing themselves in violent extremist ideologies during their process of violent radicalisation ... The majority of the study participants further added that, during their process of radicalisation to violence, they increasingly immersed themselves in ... RWE networks via online discussion forums, chatrooms and social media platforms.*[51]

Interestingly, participants felt that while involved with RWE, their online and offline identities were inextricably linked, as opposed to being two separate personas.[52]

8kun, 4chan, Reddit and Parler

Lesser-known platforms have proved popular with RWEs, especially chat forums 8kun (previously 8chan), 4chan and Reddit. Parler, which has a similar format to Twitter, has also surged in popularity with RWEs.

Launched in 2018, Parler is being investigated for its role in mobilising the insurrection of the US Capitol on 6 January 2021. Carolyn Maloney, chair of the House Committee on Oversight and Reform, asked the FBI to review Parler's role "as a potential facilitator of planning and incitement related to the violence, as a repository of key evidence posted by users on its site, and as a potential conduit for foreign governments who may be financing civil unrest in the United States".[53]

Following the insurrection, Google banned Parler from Google Play, and Apple suspended it from the App Store. Amazon then suspended Parler from its web hosting service AWS, in effect taking the site offline and forcing it to find a new web host. It has since partially returned online.

---

[50] Gaudette et al, *The role of the internet in facilitating violent extremism: Insights from former right-wing extremistsl*, Terrorism and Political Violence, 2020, P6
[51] Ibid 50 P8
[52] Ibid 50 P11
[53] https://www.theguardian.com/technology/2021/jan/21/parler-capitol-attack-fbi-investigation-congress

Chat forums, 8kun (previously 8chan), 4chan and Reddit have also proved fertile grounds for RWEs. 8kun in particular has been linked to white supremacism, neo-Nazism and anti-Semitism, and was frequented by the Christchurch terrorist and the perpetrators of back-to-back RWE terror attacks in the US in 2019.

Telegram and other encrypted messaging services

Like other groups of violent extremists, encrypted messaging platforms have played a key role for RWEs in concealing communications, sharing propaganda and planning violence. For RWEs, Telegram and Gab Chat are the most popular platforms.[54]

Lesser known than Telegram, GabChat's policy (and key attraction) is that offensive and hateful speech is not grounds for content removal and, while the platform will cooperate with the US Government on lawful requests for user data, it will not provide such data to other governments and third parties.[55]

It has also been widely reported that, amid the shutdown of Parler in the wake of the Capitol insurrection, many RWEs in the US switched to Telegram to communicate.

Brenton Tarrant

On Friday 15 March 2019, Australian right-wing terrorist Brenton Tarrant stormed two mosques in Christchurch, New Zealand – the Al Noor Mosque and the Linwood Islamic Centre – murdering 51 people and injuring 40. The terror attack was livestreamed on Facebook and in the hours before the attack, Tarrant published his 'manifesto' online.

Tarrant was a lone actor, which generally typifies violent RWE extremists, and as a result slipped under the radar of authorities. He was also a prolific user of the internet, where he gathered RWE material, was active on the dark web and was a contributor to RWE forums including 4chan and 8chan.

The Royal Commission of Inquiry into the Terrorist Attacks on Christchurch Mosques,[56] undertaken by the New Zealand Government in the wake of the attacks, clearly illustrates how Tarrant relied on the internet for planning and execution:

- Tarrant was one of 120,000 followers of the United Patriots Front Facebook page. United Patriots Front was a far-right group based in Australia (disbanded in 2017) and, across 2016-2017, Tarrant made about 30 comments on its Facebook page. At that time, the United Patriots Front was led by Blair Cottrell, a convicted RWE, whom Tarrant expressed support for.[57]

[54] Ibid 24 P18
[55] Ibid 24 P18
[56] https://christchurchattack.royalcommission.nz/the-report/download-report/download-the-report/
[57] Ibid 56 P179

- Tarrant also expressed support for Blair Cottrell on the True Blue Crew Facebook page, another Australian RWE group. The True Blue Crew is another far right Australian group.[58]
- Tarrant was a member of The Lads Society Facebook page, another RWE group, and became an active member online.
- Tarrant took steps to minimise his digital footprint to avoid detection by law enforcement. For example, he removed the hard drive from his computer (which has not been located) and tried to delete emails.[59]
- Tarrant bought RWE books, ebooks and accessories online. The books purchased were *Fascism: 100 Questions Asked and Answered* by Oswald Mosley, *The Decline of the West* by Oswald Spengler and *A Short History of Decay* by E M Cioran.[60]
- A copy of Anders Breivik's manifesto, a list of online accounts and passwords and deleted firearms videos downloaded from the internet were found on an SD card in Tarrant's drone.[61]
- Tarrant told authorities he had accessed the dark web to make purchases. He used Virtual Private Networks (VPNs) when travelling and was familiar with Tor browsers. He was also familiar with how to encrypt emails.[62]
- Tarrant identified YouTube as a significant source of information and inspiration. He also frequented RWE discussion boards on 4chan and 8chan.[63]
- It is believed Tarrant's Facebook was set to private until the hours before the attack, because if some posts had been visible authorities may have been alerted to the impending attack.[64]
- It could not be determined whether posts Tarrant made to his Twitter account on 13 March 2019 were public or protected, but at the time of the attack they were public.
- Tarrant's manifesto was unable to be seen until he posted links to the platforms where it was uploaded.[65]

The Inquiry noted that:

> *We have no doubt that the individual's internet activity was considerably greater than we have been able to reconstruct. The style in which his manifesto was written indicates fluency in the language customarily used on extreme right-wing websites*

[58] Ibid 56 P179
[59] Ibid 56 P188
[60] Ibid 56 P193
[61] Ibid 56 P193
[62] Ibid 56 P193
[63] Ibid 56 P193
[64] Ibid 56 P229
[65] Ibid 56 P230

> *and associated memes and in-jokes. The individual confirmed to us that he visited 4chan and 8chan and it is likely that he contributed comments (although we have no direct evidence of this). He also visited other sites and discussion boards where there was discussion promoting extreme right-wing and ethno-nationalist views similar to his own and sometimes supporting violence. He also spent much time accessing broadly similar material on YouTube.*[66]

In the wake of the attack, Tarrant has been lauded in RWE online groups as "the Kiwi Kebab Killer", in reference to his manifesto, in which Tarrant referred to himself as a "kebab removalist".[67]

It is important to note that, while in the real world Tarrant was a loner, online he had become part of a community of like-minded individuals, with whom he had developed a sense of belonging and kinship. It was within this narrow and destructive ideological milieu that Tarrant was supported and encouraged and, while not an organised terror group per se, this online community was undoubtedly a key driver in inspiring Tarrant's terrorist attack.

COVID-19

COVID-19 has proved a boon for RWE worldwide, driven by the ubiquity of social media platforms. Misinformation and disinformation regarding the virus have flourished on digital platforms, amplified, intensified and reinforced throughout worldwide lockdowns. This exploitation of mistrust and fear have sown panic in the minds of citizens worldwide, with a marked impact in the US, leading to an exponential rise in far-right rhetoric. This rhetoric is built on a swirl of unconnected and sometimes loosely linked conspiracy theories, which continue their rampant spread across the digital universe.

There are multiple strains of this online-driven right-wing extremism. 'Soft' extremism, which proliferates on mainstream social media platforms such as Instagram and Facebook, acts like a gateway to more extreme, hard right views. Targeting young, white mothers by peddling QAnon narratives about saving children from a vast paedophilia ring of global elites,[68] while incorporating the conventional marketing tactics of social media 'influencers',[69] QAnon proponents have had viral success at building audiences among new demographics and spreading COVID-19 related misinformation.

---

[66] Ibid 56 P234
[67] https://gnet-research.org/2020/05/21/how-the-far-right-uses-memes-in-online-warfare/
[68] QAnon conspiracists believe in a vast pedophile ring. The truth is sadder | QAnon | The Guardian
[69] QAnon Influencers Amass Mom Following On Instagram (buzzfeednews.com)

Increasingly and disturbingly, it is not just rhetoric. Adherents across the spectrum of far-right groups are now calling for violent action on this front.[70] This is evident in the Boogaloos, which, like many other far-right movements, gained currency online. Initially protesting COVID-19 lockdowns and government 'control', the Boogaloos have pitted themselves against the law enforcement community, anticipating an impending, second civil war. Despite a fringe element of white supremacy,[71] Boogaloo adherents have been careful to distance themselves from neo-Nazism and racism, repeatedly articulating their anti-racist stance, instead capitalising on their ability to manipulate citizens' fears of loss of liberty. This has greatly benefitted their movement. Given their seemingly more innocuous stance to other far-right movements, the Boogaloos have proven highly successful at attracting individuals who would normally not subscribe to extreme ideology.[72]

Other, more disturbing varieties of RWE have emerged, suggesting not only that violent action might be in order, but that anarchical behaviour and guerrilla warfare tactics be deployed. This is to dismantle the (perceived) impending New World Order, led by far-right bogeymen, George Soros,[73] Jacob Rothschild and Bill Gates.[74] Tapping into a simmering online vein of discontent, long fuelled by rising inequality and globalisation, far-right extremists claim that the pandemic is a tool used by global elites to foment racial tension and "put the planet on lockdown, bankrupt the planet, invoke martial law, then BOOM, the third temple emerges".[75] Followers are being incited to resort to violence, with far-right chat rooms awash with advice about how to exploit widespread citizen mask-wearing to carry out attacks under the cover of anonymity. A message on end-to-end encrypted messaging platform Telegram, advised attackers to "wear a breathing mask, they won't question it" in order to "tip water towers, blow up bridges, railroads and sewage treatment plants".[76]

Some RWEs have taken it further. Picking up on the sentiment that COVID-19 is a weapon promulgated by the Jews[77] or the Chinese, online chatter urges supporters to deliberately undertake biological warfare. An 8chan post urged others that "if you get infected with the corona virus, go visit your local synagogue and hug as many Jews as possible, cough on all the door knobs, rails, pens, etc".[78]

---

[70] Kruglanski et al, *Terrorism in the time of the pandemic: exploiting mayhem*, Global Security: Health, Science and Policy, 2020, P 127
[71] The Boogaloo Movement Wants To Be Seen as Anti-Racist. But It Has a White Supremacist Fringe | Middlebury Institute of International Studies at Monterey
[72] Ibid 70 P 127
[73] Why is billionaire George Soros a bogeyman for the hard right? - BBC News
[74] How Bill Gates became the voodoo doll of Covid conspiracies - BBC News
[75] Ibid 70, P 126
[76] Ibid 70, P 127
[77] The Conspiracy Theory to Rule Them All - The Atlantic
[78] Ibid 70, P 127

Further steps that could be taken to disrupt and deter extremism and radicalism online

The *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, which was swiftly enacted by the Federal Government in the wake of the Christchurch terror attack, was a pioneering and pivotal move aimed at reducing the use of online platforms to transmit acts of violence.[79] Violent abhorrent material is defined as that which captures a terrorist act involving serious harm or death, murders or attempts to murder, torture, rape and violent kidnapping.[80] The Act created two new criminal offences aimed at internet service providers and hosting and content providers – failure to report and failure to remove violent abhorrent material – holding them responsible for reporting and removing such material.[81] Large financial penalties and imprisonment apply in the case of conviction and, to the best of the CSCRC's knowledge, no charges have been laid under the Act. This may serve to demonstrate the Act's deterrent effect.

Australia has also led the way globally with the *Telecommunications and Other Legislative Amendments ('Assistance and Access') Act 2018*, which introduced measures to better equip law enforcement and intelligence agencies to deal with the challenges posed by ubiquitous encryption.[82]

The CSCRC submits the proposed *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*,[83] which seeks to introduce new law enforcement powers to enhance the ability of the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC) to combat serious online crime, will, if passed, play a key role in countering violent extremism and radicalisation. The Bill has three key components, allowing for data disruption warrants, network activity warrants and account takeover warrants. If passed, authorities will no longer have to ask serious criminals for permission to access accounts, as is the current case in some circumstances. It presents a clear opportunity for Australia to ensure domestic laws are properly aligned with digitally-perpetrated activities, allowing lawful access to data and devices where it is appropriate to do so.

Lastly, given the globally-interconnected nature of online extremism and radicalism, there is a clear opportunity for Australia to ensure that domestic laws – laws with real-world consequences – are aligned with those of our key allies and trading partners, and infused

---

79 https://www.ag.gov.au/sites/default/files/2020-03/AVM-Fact-Sheet.pdf, P1
80 Ibid 79 P2
81 https://www.legislation.gov.au/Details/C2019A00038
82 https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_504ca495-f6b2-46bb-a4a2-9ce169ba2616/upload_pdf/692183_Revised%20Explanatory%20Memorandum.pdf;fileType=application%2Fpdf
83 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6623

with the democratic ethos our nation was founded upon. Accordingly, the CSCRC submits that the leveraging of existing and emerging international intelligence sharing relationships is advisable to present united perspectives on combatting online radicalism and extremism. On this front, Australia's enduring relationship with our Five Eyes allies remains pivotal for our national security. Our commitment to this alliance was reiterated in the 2018 Five Country Ministerial[84] which outlined the Five Eyes' resolve to work together to counter the threat of extremism and terrorism. Australia is also a member of the Quad (the Quadrilateral Security Dialogue), an emerging, informal strategic forum between Australia, Japan, US and India, which offers another avenue for Australia to advance its security interests on the world stage. As noted, ensuring strong international collaboration on this issue will provide a harmonised viewpoint on effective ways to respond to extremism and radicalism, especially as it operates in the digital domain.

[84] Five country ministerial 2018 (homeaffairs.gov.au)