SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY: INQUIRY INTO EXTREMIST MOVEMENTS AND RADICALISM IN AUSTRALIA

FEBRUARY 2021

Author: Lydia Khalil

The views expressed in this submission are entirely the author's own, and not those of the Lowy Institute.

TABLE OF CONTENTS

1. INTRODUCTION

In my capacity as a research fellow for the Lowy Institute, I welcome the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into Extremist Movements and Radicalisation in Australia. This inquiry is both relevant and timely, given that we are living in a period of increasing polarisation and disinformation that has contributed to the growth of a diverse array of extremist movements across the ideological spectrum, but particularly among the extreme right. Extensive research has also clearly demonstrated that the pervasive use of digital technology — particularly social media — has played a key role in the radicalisation and mobilisation of extremist actors and has had net negative impacts on our democracy.

As part of my work as a research fellow, I study the emergence and growth of international and Australian terrorist and extremist movements, with a particular focus on the extreme right and jihadist movements, as well as the intersection of technology and extremism.

The Lowy Institute is a highly regarded Australian think tank with a global outlook that produces policy relevant research on both global and Australian foreign policy and national security issues. Extremism is one of those issues that has intersecting global and national dimensions and those global and local components are facilitated via communication technology.

Given the scope of my work in this capacity, I would like to focus the details of this submission on the following term of reference (TOR):

3F) the role of social media, encrypted communications platforms and the dark web in allowing extremists to communicate and organise.

The Joint Committee's timely efforts to examine radicalisation and extremism provide an important opportunity to update Government's understanding around these issues, particularly as technology is accelerating the adaptation, composition and reach of extremist movements. It also provides an opportunity to inform and update the National Counter-Terrorism Strategy, which has not been revised since 2015.

My submission makes the following recommendations:

Recommendation 1: Ensure algorithmic transparency

Government regulation to ensure algorithmic transparency and accountability is a difficult, but much needed, proposition and one where there is precedent through such regulatory efforts as the EU's General Data Protection Regulation (GDPR), which has made transparency fundamental to data processing. That type of regulation could help address not only our concerns around the spread of violent extremism via tech-enabled communication platforms, but also broader concerns around disinformation polarisation, privacy and data protection that impact our democracy. Regulating algorithmic transparency — the concept that factors which influence the decisions made by algorithms should be visible and knowable in a meaningful and fair manner to those who use them — involves a number of technical, political and commercial considerations. Algorithmic transparency also has broader societal and commercial implications beyond how it affects the spread of extremist content online and contributes to radicalisation.

Recommendation 2: Prioritise research funding to study the role technology and social media play in radicalisation and mobilisation

While there has been useful and innovative research on the intersection of technology and extremism, there is still much we do not know. Government should prioritise research funding to study the intersection of technology and extremism in this age of 'big data' and encourage collaboration between social science extremism and terrorism researchers and data scientists via grant schemes.

Recommendation 3: Invest in online diversion and intervention

Government needs to invest in funding for diversion and intervention programs, particularly targeting extreme right-wing ideological adherents. Government should also focus on working with industry and research communities to develop online diversion and intervention programs. Online interventions are particularly important because they are among the few ways to reach so-called lone actors — extremist actors who go on to commit violence or real world harm, are not part of a particular organisation or movement, and yet who emerge from within an online milieu, supported and radicalised via global, as well as parochial, online extremist networks.

Recommendation 4: Synthesise combatting disinformation and combatting extremism

Disinformation is an essential component of extremist narratives. Extremist ideology is, by its very nature, conspiratorial and offers a version of the world based on inaccurate or biased information. Yet often these conjoined issues — extremism and disinformation — are treated separately by Government in terms of analysis and programming. Government should explore ways to conjoin combatting disinformation and countering violent extremism strategies and programs. Government should examine ways in which knowledge and best practice from either effort can be leveraged to combat the other for greater efficiency.

Recommendation 5: Explore the feasibility of digital public infrastructure

Ethan Zuckerman, a former director of the MIT Media Lab and current professor at the University of Massachusetts, has put forward an important argument for the creation of a public internet to get around the corrosive effects of commercial digital technologies. This idea has implications well beyond combatting extremism, but it is directly relevant. Zuckerman writes, "Because we see the dominance of the internet by Google, Facebook, and others as inevitable, the solution space we consider for combatting mis-/disinformation, polarization, and promotion of extremism is overly constrained. Our solutions cannot be limited to asking these platforms to do a better job of meeting their civic obligations — we need to consider what technologies we want and need for digital media to have a productive role in democratic societies." In addition to better regulating big tech, Government should begin to explore ways to offer public alternatives.

Recommendation 6: Invest in inoculation against disinformation and extremist messaging

While conspiracy movements like QAnon may come and go, disinformation that drives extremism and politicisation will remain a problem. Future iterations driven by online disinformation actors and amplifying populations will likely emerge again and Government should plan for this likelihood. 'Inoculation theory' — which claims that individuals can be 'inoculated' from persuasion by pre-exposure to arguments that refute a narrative or idea — has emerged as a promising means to counter disinformation, conspiracy theories and violent extremism ideologies. Inoculation is one potential method Government should consider to combat disinformation and harmful conspiracies.

2. PARTNERSHIP WITH THE GLOBAL NETWORK ON EXTREMISM AND TECHNOLOGY (GNET)

Last year, the Lowy Institute became a core partner of the Global Network on Extremism and Technology (GNET), an academic research consortium that is funded by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative that seeks to better understand and counteract extremist use of technology. Our core partnership with GNET has afforded the Lowy Institute the opportunity to engage with international experts and tech industry stakeholders on a variety of issues related to extremism and technology.

As part of my work convening this core partnership with GNET, I commissioned a number of Lowy Institute Insight articles related to issues of terrorism and technology this year. These reports, such as the recent pieces exploring the unlikely alliance between Australian far-right extremists and Chinese anti-CCP activists, the online right-wing extremist use of the internet in NSW, the spread of extremist messaging from inauthentic accounts as well as the spread of QAnon conspiracies via unexpected online communities, can be found on our *Interpreter* website and form part of an ongoing series.

As part of our GNET partnership, the Lowy Institute has also held a number of workshops that brought together academic, government and industry stakeholders to engage on issues relating to technology and extremism, such as the intersection of online foreign interference and extremism, and the online presence of Australian far-right extremists.

Through our engagement with GNET, we are also conducting an extensive, first of its kind, survey of global scholars and experts in extremism and terrorism studies on issues around extremist use of technology. While the project remains ongoing, preliminary results of the survey reveal that extremism and terrorism researchers examining these issues across the ideological spectrum have found that technology has played a large role in the increase of extremism. When asked if “the use of internet-enabled communications or social media platforms by extremist actors has made it easier to recruit individuals to extremist movements”, 91 per cent of the 110 experts strongly agreed or agreed with that statement. Similarly, 84 per cent agreed or strongly agreed that, “the use of internet-enabled communications and/or social media platforms by extremist actors has made it easier to plan violent attacks or mobilise to offline action”.

This ongoing work with GNET, the GIFCT and broader research efforts examining issues around extremism and technology allow me to advance the following observations for the Committee’s consideration.

3. DEPLATFORMING

Mainstream social media platforms have been, rightly, criticised over the years for being slow and inconsistent in extricating extremist users from their platforms and limiting the spread of extremist content. Under pressure from governments and the broader public, individually and through their joint efforts in the GIFCT, mainstream social media platforms have worked over the years to develop better content moderation mechanisms and to remove users who violate their terms of service — or deplatform them. Recent crackdowns by mainstream social media companies such as Facebook and Twitter have succeeded in removing many accounts and pages promoting extremist content. Most recently, QAnon-related accounts linked to networks that organised and promoted the Capitol siege, including that of former President Trump, were removed by Twitter. In previous years, there was a concerted and coordinated effort to take down Islamic State content that proliferated on social media sites.

That said, the major tech companies have been slow to act in removing extremist content in the first instance, citing their reluctance to become arbiters of speech. However, their delayed response allowed content to spread and the movements to grow before the content was taken down. Moderation effort remains slow and imperfect. The sheer scale of mainstream social media platforms (Facebook alone has 2.8 **billion** monthly active users) makes comprehensive and responsive content moderation nearly impossible. Social media companies across most jurisdictions are also not liable for content their users generate. Since the legal responsibility for user content that leads to offline harm lies elsewhere, companies are not legally incentivised to respond. They may suffer reputational damage, but not legal consequence, though legislation is being considered in a number of jurisdictions that may change this.

Even as more extremist actors are removed from mainstream social media platforms, they do not lose their ability to connect via computer-enabled communications entirely. Deplatforming from mainstream social media has driven extremist actors and groups to alternative communication platforms — or 'alt-tech platforms' — like Gab, Telegram and Parler (which has recently been removed from the Apple App Store and Google Play) to name a few. In contrast to the mainstream social media companies, these platforms are entirely unmoderated spaces. Extremist, particularly white supremacist and far-right, actors have flocked to them.

It is also important to remember that social media, even accounting for alternative social media, does not make up the entirety of the internet. There are other online spaces where extremists gather, including encrypted messaging apps, password protected websites and private message boards. As more deplatformed actors gravitate to those private and/or unmoderated spaces, it is critical to broaden our concept of extremist use of the internet beyond social media.

There is an ongoing debate about the effectiveness of deplatforming extremist actors from mainstream social media platforms. On one hand, deplatforming restricts the ability of extremist actors to communicate with a broad audience and decreases the risk that a member of the community will inadvertently come across extremist content when they are not explicitly searching for it. It reduces not only the spread, but also the production of extremist content. It disrupts social networks as users — both extremist influencers and their followers — attempt to replatform on other sites. Deplatforming also restricts the ability of extremist online influencers and groups to monetise their online presence.

On the other hand, extremist actors who replatform on alternative social media sites with no content moderation, or who move to website forums, end up corralled into even tighter, if thinner, online communities that become echo chambers that can accelerate the violent mobilisation process. These alternative sites are rife with disinformation and hate speech. The fact that deplatformed individuals and groups are excluded from the mainstream also reinforces their outsider status and stokes grievances against government and big tech censorship; they view their removal from mainstream platforms as further justification for their extremism.

At other times, however, extremists maintain a complementary presence on both mainstream and alt-tech platforms. An analysis by Google’s Jigsaw examined how mainstream and alt-tech platforms are often used in tandem by white supremacists. These groups maintain a presence on mainstream platforms and use coded language to circumvent content moderation and explicitly avoid discussion of violence on mainstream platforms, while using alt-platforms to post more extreme content and coordinate and communicate.

4. ALGORITHMIC AMPLIFICATION AND TRANSPARENCY

The recommendation algorithms used by social media companies such as Facebook and YouTube seek out what is engaging to the user, but the algorithms have shallow definitions of what is engaging and relevant. They are based on what the company can measure — watch time, clicks, likes and shares — and not whether content is accurate, useful or helpful. The substance of the content is not factored into the recommendation algorithm. Much of the content that is engaging is also pernicious. Disinformation, hate speech, inflammatory and polarising content and disinformation draw on primary emotions like fear and anger and drive user engagement. Increased user engagement leads to increased profit. Therefore, there is an overriding commercial imperative to keep levels of engagement high — it is part of the business model. This profit motive and lack of government regulation on algorithmic transparency, along with a host of other issues like data protection, privacy and competition, is hindering our ability to combat online radicalisation and extremist use of the internet.

We need more systematic transparency around how content is amplified and how the algorithms work. Big tech companies do not disclose enough information about their algorithms and, as a result, regulators and public alike are largely in the dark. We know exceptionally little about the forces shaping our information environment. Without understanding how social media recommendation algorithms function we will 1) not be able to evaluate how recommendation algorithms may lead users to more extremist content through algorithmic amplification, and 2) not be able to come up with effective ways to counteract their consequences.

Even though the public and Government may not have a full picture of what is happening behind the scenes, internal research by the tech companies shows that their recommendation algorithms lead to extremist content. According to internal Facebook research from 2018, “64% of all extremist group joins are due to our recommendation tools”. The report also acknowledged, “Our algorithms exploit the human brain’s attraction to divisiveness... If left unchecked, [the algorithms would feed users] more and more divisive content in an effort to gain user attention & increase time on the platform.”

Similarly, YouTube recommendation algorithms drive 70 per cent of user watch time. A *Wall Street Journal* investigation also from 2018 found that, “YouTube’s recommendations often lead users to channels that feature conspiracy theories, partisan viewpoints and misleading videos, even when those users haven’t shown interest in such content. When users show a political bias in what they choose to view, YouTube typically recommends videos that echo those biases, often with more-extreme viewpoints.” Since then, YouTube claims it has made changes that address this problem, in part due to advocacy efforts for algorithmic transparency by former YouTube engineers. But externally auditing these efforts is not possible and users are still being recommended disinformation and divisive extremist fringe content, even though YouTube has banned a number of extremists and groups from its site.

5. ONLINE DISINFORMATION AND EXTREMISM

Disinformation and conspiracies disseminated and spread online can radicalise individuals to extremism. This is encapsulated most prominently in the QAnon phenomenon, which emerged as an online subculture around 2017, but grew exponentially during the COVID-19 pandemic, and whose conspiracies most recently culminated in the January 2021 Capitol Siege in Washington, DC. The 6 January Capitol insurrection demonstrated how a networked online conspiracy movement can migrate from the online environment and radicalise individuals to violence. QAnon adherents, narratives and symbols were prevalent in the Capitol Siege, along with other groups and individuals fuelled by online consumption of disinformation claiming that the election was rigged. The Capitol insurrection was the culmination of years' worth of the dissemination and uptake of QAnon theories that began on anonymous online forum 4chan, but then spread and flourished on mainstream platforms.

Conspiracy theories and conspiratorial mindsets are not new and have been identified as a factor in radicalising extremist movements. However, conspiratorial movements or individuals who believe in a conspiracy and are connected online, are now emerging as a stand-alone domestic extremist threat. The US Federal Bureau of Investigation (FBI) has assessed that "Anti-government, identity-based, and fringe political conspiracy theories very likely will emerge, spread, and evolve in the modern information marketplace over the near term…occasionally driving both groups and individuals to commit criminal or violent acts."

In addition to the events around the Capitol Siege, the COVID-19 pandemic has spurred the further proliferation of conspiracy and disinformation online — 5G and 'anti-vax' conspiracies have already inspired a number of plots, attacks and violations of government lockdown measures around the world and here in Australia. Online disinformation has radicalised people to target political leaders, public health facilities and minority communities they believe are responsible for the spread of the virus.

The promotion of conspiracies and disinformation can be understood as a form of attack. For example, some right-wing extremist groups have encouraged followers to spread disinformation online about the coronavirus in order to exacerbate tensions, undermining democracy, government authority and social cohesion. Adherence to QAnon conspiracies can undermine society by dividing communities and families. It has distorted politics and governance because it has seeped into the political class (for example, a number of legislators who promote QAnon theories were elected to the US Congress) and some politicians feel they need to address constituent concerns — no matter how inaccurate — fomented by these conspiracies. It has also hijacked legitimate social welfare advocacy efforts. The recent 'Save the Children' campaign fuelled by QAnon conspiracies is a good example.

Social media and computer-enabled communications have also made these conspiracies participatory and interactive. People are not just passively receiving conspiratorial information by exposure to posts discussing the theories via online conspiracy influencers. Rather, the conspiracy has gone viral and been amplified through a process of gamification — the use of game techniques in non-game contexts.

Conspiracy influencers drop clues for followers to find, believers connect on the internet and compare clues and connections seemingly prove their theory. Gamification also invests the believer even more deeply in the conspiracy. It reinforces the social connection and bonds of conspiracy believers, which further reinforce their conspiratorial worldview. This process can also mobilise believers to commit violence on behalf of those beliefs. QAnon is not the only extremist movement that has employed gamification techniques — jihadist groups such as the Islamic State have also used gamification techniques. Researcher Linda Schlegel, who has examined this phenomenon, has found that elements from games and gaming culture are utilised by a variety of extremist organisations to support their radicalisation and recruitment efforts and that they are used by a variety of extremist actors.

6. SOCIAL MEDIA LOGIC AND RADICALISATION

Social media platforms and other computer-mediated communication tools have enabled extremists to organise and communicate in broader and more efficient ways. Social media platforms have played a significant role in spreading disinformation and fomenting polarisation. They have done so through algorithmic recommendation. But social media and computer-mediated communication has brought even more foundational changes to society and human interaction that have influenced extremism and polarisation.

Scholars José Van Dijck and Thomas Poell have conceptualised the theory of 'social media logic', which states that social media platforms are not neutral platforms, but have in fact changed the conditions and rules of social interaction. The 'logic' refers to "the processes, principles, and practices through which these platforms process information, news, and communication", and how they affect and redefine social interaction. Social media logic affects what we value, how we impart information, and how we measure influence. For example, a blue tick on Twitter confers credibility, even though how one receives verification is not entirely transparent and not based on consistent measures. Content that receives a lot of engagement makes it valuable, regardless of its substance.

Social media logic also affects our social networks; we can now curate our social networks and information flows. We can block accounts we disagree with, limit our follows to like-minded accounts, and place filters on any outside influence that confronts our worldview.

Extremism researcher JM Berger has examined how one aspect of social media logic has contributed to extremism by shattering our consensus reality — the idea that we know what is true and what is real via the confirmation of those around us. In other words, consensus reality is reflected in the assumption that "the more people who agree on a fact, the more we understand it to be real".

But in the social media age, consensus reality, already unstable, has become even more so as different versions of facts and realities fuelled by disinformation and misinformation spin around the web. In this age of uncertainty and with no clear notion of consensus reality, we gravitate more and more to our 'in group' — those within one's social or identity circle, however defined. Sometimes that is accompanied by hostile reactions, even violence, to those in ‘out groups’ — or others who we do not identify with. This shattering of consensus reality, which has occurred largely as a result of our interactions online, has contributed to the growth of extremism via the hardening of views and the consolidation of exclusivist identities.

7. CONCLUSION

A number of issues discussed in this submission have broader societal implications beyond online radicalisation and extremist use of the internet. The study of extremism, however, reveals what broader societal, structural and political issues need to be addressed. Extremism does not arise out of a vacuum, rather it is one response to the world we live in. Likewise, to better combat violent extremism, often the answer lies in understanding and addressing broader societal and political issues. The targeted recommendations provided in this submission, such as online intervention programs and expanding research funding for collaboration with social and computer scientists, address the specific consequence — online extremism — of structural issues in our society. Others, such as regulating algorithmic transparency, exploring the feasibility of public internet infrastructure and inoculating against disinformation, will not only address extremist use of the internet, but also yield broader societal benefits.