THE ONLINE HATE PREVENTION INSTITUTE

Empowering communities, organisations and agencies in the fight against hate.

ONLINE HATE PREVENTION INSTITUTE SUBMISSION TO THE INQUIRY INTO

EXTREMIST MOVEMENTS & RADICALISM IN AUSTRALIA

PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

12 FEBRUARY 2021

OVERVIEW

The Online Hate Prevention Institute, Australia's only harm prevention charity dedicated to tackling online hate and extremism, welcomes the opportunity to respond to this consultation. Civil society organisations like ours play a vital role in monitoring extremism in Australia and mitigating risk.

The Online Hate Prevention Institute has proven expertise in bringing transparency to social media, monitoring and reporting on online extremism, and supporting police, government and other agencies with Open Source Intelligence. Our policy advice and technical recommendations have led to changes to core software by major technology platforms like Facebook and YouTube. Our software tools, research methodologies and policy guidance are recognised as world class. We make the online world a safer place. In light of the rise of extremism fuelled through the internet, the work we do is needed now more than ever.

We believe tech companies, government and civil society must work together to prevent, detect and remove the dangerous content promoting terrorism, violent extremism and incitement which leads to radicalisation. We believe tech companies control the infrastructure and have the greatest capacity and responsibility to respond, but to ensure they do so effectively, we need monitoring and transparency with measurable results. This requires independent assessment and verification in addition to self-reporting. We must create systems that are robust to changes in technology and society. We must create systems which support continual improvement. We must create systems that engage with tech companies, government and civil society.

The Online Hate Prevention Institute was designed to provide an agile response to the online environment. We have developed the tools and expertise to make a real impact and we have a track record, parts of which are discussed in this report, which demonstrates this impact. We are proud to serve on the Australian Government's delegation to the International Holocaust Remembrance Alliance and to be leading a multi-lateral pilot project on behalf of the Australian Government providing new tools to track Holocaust denial and antisemitic content which is commonly associated with white nationalism and the sort of far-right extremism which has been behind recent terrorist attacks overseas.

In response to the terrorist attack in New Zealand a number of governments, include the Australian Government, have signed up to the Christchurch call. This declaration notes the importance of civil society engagement in tackling the spread of extremism. With a solid track record and international recognition, the Online Hate Prevention Institute is perfectly placed to work with government in delivering a response to the horrific attack and subsequent incidents.

We begin with some background on the role we play in providing Australian leadership on the global stage in tackling online and extremism. Next, we briefly discuss our technology capabilities. We then address the terms of reference directly, building on this background understanding.

AUSTRALIAN LEADERSHIP ON THE GLOBAL STAGE TACKLING ONLINE HATE & EXTREMISM

The Online Hate Prevention Institute (OHPI) is Australia's only harm prevention charity dedicated to tackling online hate and extremism. Established in January 2012 we have supported a wide range of government agencies in intelligence gathering, threat assessment and direct intervention actions to prevent the spread of extremist material, incitement to violence and hate speech in Australia.

We are recognised intentionally as a world leader in this space. A few examples:

- In November 2020 we represented global civil society as an invited speaker for the 13th session of the UN Forum on Minorities which was dedicated to the topic of "Hate Speech, Social Media and Minorities".[1]
- We previously presented on this topic for the UNAOC Conference "Tracking Hatred: An International Dialogue on Hate Speech in the Media" in 2015.[2]
- In 2017 the UK's All Party Parliamentary Committee on British Muslims acknowledged the role of our 2013 work on online Islamophobia which "led to calls from politicians for better structures to deal with online hate and for social media platforms to take a greater onus on tackling online hate".[3]
- In 2016 we also provided the first ever transparency report on antisemitism in social media, including incitement to violence, for the Israeli Government's Global Forum for Combating Antisemitism.[4]
- We were also a key source for UNESCO's work on tackling online hate speech and discussed extensively in a number of UNESCO reports.[5]
- Our extensive report on the threat of online radicalisation by the far-right carries a forward from the European Commission.[6]

We have also provided leadership in this space on behalf of Government:

- Our CEO, with the organisations support, has represented the Australian Government at the International Holocaust Remembrance Alliance, and specifically in the Committee on Antisemitism and Holocaust Denial since 2015. We are also responsible for implementation of

---

[1] https://www.ohchr.org/EN/HRBodies/HRC/Minority/Pages/Session13.aspx; Video of our presentation can be seen at: https://ohpi.org.au/address-to-the-united-nations/

[2] Our write up, slides and link to the UN TV video of the presentation can be seen at: https://ohpi.org.au/unaoc/

[3] https://ohpi.org.au/impact-on-islamophobia-ohpi-in-uk-parliamentary-report/

[4] https://mfa.gov.il/MFA/ForeignPolicy/AntiSemitism/Pages/Measuring-the-Hate-Antisemitism-in-Social-Media.aspx

[55] https://ohpi.org.au/ohpi-quoted-in-a-unesco-report-on-online-hate/

[6] https://ohpi.org.au/hate-and-violent-extremism-from-an-online-subculture-the-yom-kippur-terrorist-attack-in-halle-germany/

one of the Australian Government's projects as part of our IHRA membership, a project related to online tools to enable public reporting of online antisemitism and Holocaust denial using the IHRA Working Definition of Antisemitism.

- Our CEO, with the organisations support, served for 9 years as one of the international experts on the steering committee of the Israeli Government's Global Forum for Combating Antisemitism and as co-chair leading its working group on online and media antisemitism. The work of this working group is widely regarded as some of the most significant policy work in the space.

The Online Hate Prevention Institute is a regular participant in dialogues both locally and globally in relation to online hate, extremism, and community resilience. We have presented for the global technical community,[7] Australian meetings of government and industry to tackle online extremism,[8] meetings with AUSTRAC and the major banks AML/CTF representatives,[9] international inter-Parliamentary groups including the International Coalition to Combat Antisemitism and the new Inter-Parliamentary Task Force on Online Antisemitism,[10] parliamentary hearing in Australia[11] and overseas[12].

We have been working in this space since 2012 and our CEO's work goes back to 2004 in relation to search engines and 2008 when he was the first globally to raise the concern about the dangers of social media in spreading incitement and hate and normalising it in society.[13] We were created, in part, to take forward plans to bring transparency to social media and the ways technology companies report on dangerous content.

Over the last eight years various parts of our work have been supported by the Australian Federal Police, the Department of Foreign Affairs and Trade, and the Victorian Department of Premier and Cabinet. We have conducted work related to violent extremism at the request of the Australian Federal Police, Victoria Police and the Federal Attorney General's Department. Our work product has on multiple occasions been passed to other agencies for national security purposes.

---

[7] https://ieeetv18.ieee.org/tackling-cyber-hate-incitement-and-dangerous-fake-news-andre-oboler-ignite-sections-congress-2017

[8] https://www.facebook.com/284088808335015/videos/1800284873382060

[9] https://www.facebook.com/onlinehate/photos/today-our-ceo-dr-andre-oboler-presented-to-a-forum-of-banking-experts-in-the-ant/2817279581682579/

[10] https://ohpi.org.au/inter-parliamentary-task-force-on-online-antisemitism/

[11] https://www.parliament.vic.gov.au/images/stories/committees/lsic-LA/Inquiry_into_Anti-Vilification_Protections_/Transcripts/2020.03.12/2020.03.12_FINAL_TRANSCRIPT_OHPI.pdf

[12] Our CEO Dr Oboler gave key testimony when Italy reformed its laws, https://tandis.odihr.pl/bitstream/20.500.12389/21122/1/06866.pdf and we continue to be engaged by the Italian Government, e.g. most recently, https://ohpi.org.au/italian-government-presentation-on-antisemitism-2-0/

[13] https://jcpa.org/article/online-antisemitism-2-0-social-antisemitism-on-the-social-web/

The 2017 book, Cyber-Racism and Community Resilience,[14] a result of a large ARC project led by Australia's top academic researchers in the online hate space, discusses our work extensively and presents it as a national asset in this space.

We have also provided confidential reports on a range of matters to various parts of Government, sometimes at their request, other times in response to actionable intelligence we discover. We have worked with the Australian Federal Police ("AFP") (and through them the Australian Intelligence Community), the Attorney General's Department ("AGD"), the Department of Foreign Affairs and Trade ("DFAT"), the Department of Veterans Affairs, the Australian Human Rights Commission ("AHRC") and various state government departments and police forces.

As a harm prevention charity, our mandate is public safety. We focus not only on individuals and minority groups, but any group that is being targeted online. Our latest work has focused on online hate targeting politicians and the threat this is posing to democracy. A significant part of our work is specifically focused on tackling online extremism.

INNOVATION – FROM CIVIL SOCIETY TO SUPPORT GOVERNMENT

OHPI was created as a Harm Prevention Charity but also as a technology startup. We were designed to improve public safety by building innovative technical solutions and provide in-depth technical analysis and advice to key stakeholders, including government and industry. Our expertise is recognised by these stakeholders well beyond Australia. Our CEO currently serves on the Global Public Policy Committee of the IEEE, the world largest professional body for engineers and technology professionals, and as a global Vice President of the IEEE Computer Society. In the last three months alone the governments of Sweden, Italy and the Netherlands have reached out to us for our expertise.

This focus goes back to our Dr Oboler early work and to leadership through the Global Forum for Combating Antisemitism convened by the Israeli Foreign Ministry. This work highlighted the threat and worked on compiling global best practices with international stakeholders. A key challenge identified in this work was the need for metrics about online hate, a challenge which led to the development of "Fight Against Hate", a technological solution to provide shadow reporting and gather independent data to monitor the scope of antisemitism in social media and the effectiveness of the major platforms in responding to it. This platform was designed in consultation with international experts and later formally endorsed by the forum. It was launched in Sydney by the Hon. Paul Fletcher MP in 2014.

[14] https://link.springer.com/book/10.1007/978-3-319-64388-5

Figure 1 The Hon Paul Fletcher launching Fight Against Hate in Sydney, December 2014

Following its use to produce the world's first major transparency report on antisemitism in social media for the Global Forum to Combat Antisemitism in 2015, the tool was formally endorsed by a resolution of the gathered experts. A report into Islamophobia followed, sponsored in part by the Australian Federal Police and the Islamic Council of Victoria.

UNESCO's reports "Countering Online Hate Speech" and "World Trends in Freedom of Expression and Media Development: Special Digital Focus 2015" examined Fight Against Hate and praised it as an innovative tool to tackle dangerous online content. The tool was presented at the United Nations in New York, the International Holocaust Remembrance Alliance, the Global Forum for Combating Antisemitism, the Australian Institute of Criminology's Crime Prevention and Communities conference, and a range of academic conferences in Australia and overseas.

The tool has undergone a series of revisions, including one complete rewrite to increase its flexibility. Over 30 developers have worked across 6 major projects on the tool. They have refined and expanded the work of Fight Against Hate and developed the prototype system CSI-CHAT (Crowd Sourced Intelligence— Cyber-Hate and Threats), an analysis platform designed to work in real time with the data from Fight Against Hate. The development has involved consultations with police, the Federal Attorney General's Department, the CSIRO, human rights agencies and leading academics. A 2015 proposal to the Attorney-General's department highlighted how further investment and a partnership with OHPI could see the tool develop into a significant resource for Australia, with data stored locally for added security.

> "OHPI's FightAgainstHate.com has the capacity, in a short timeframe to ramp-up and greatly enhance the government's ability to respond to emerging security threats. If funding is secured in a partnership with government, in combating violent extremism, OHPI and its FightAgainstHate.com system will then be able, to report to government, including via predesigned and configurable reports agreed under the

> partnership with government, and OHPI will be able to provide real time access to selected data to relevant government agencies and law-enforcement bodies as well as a government audited system of access for government to manage and control." – from the 2015 proposal

A map the capabilities that were available, and additional capabilities which could be added under a funded partnership was also included:

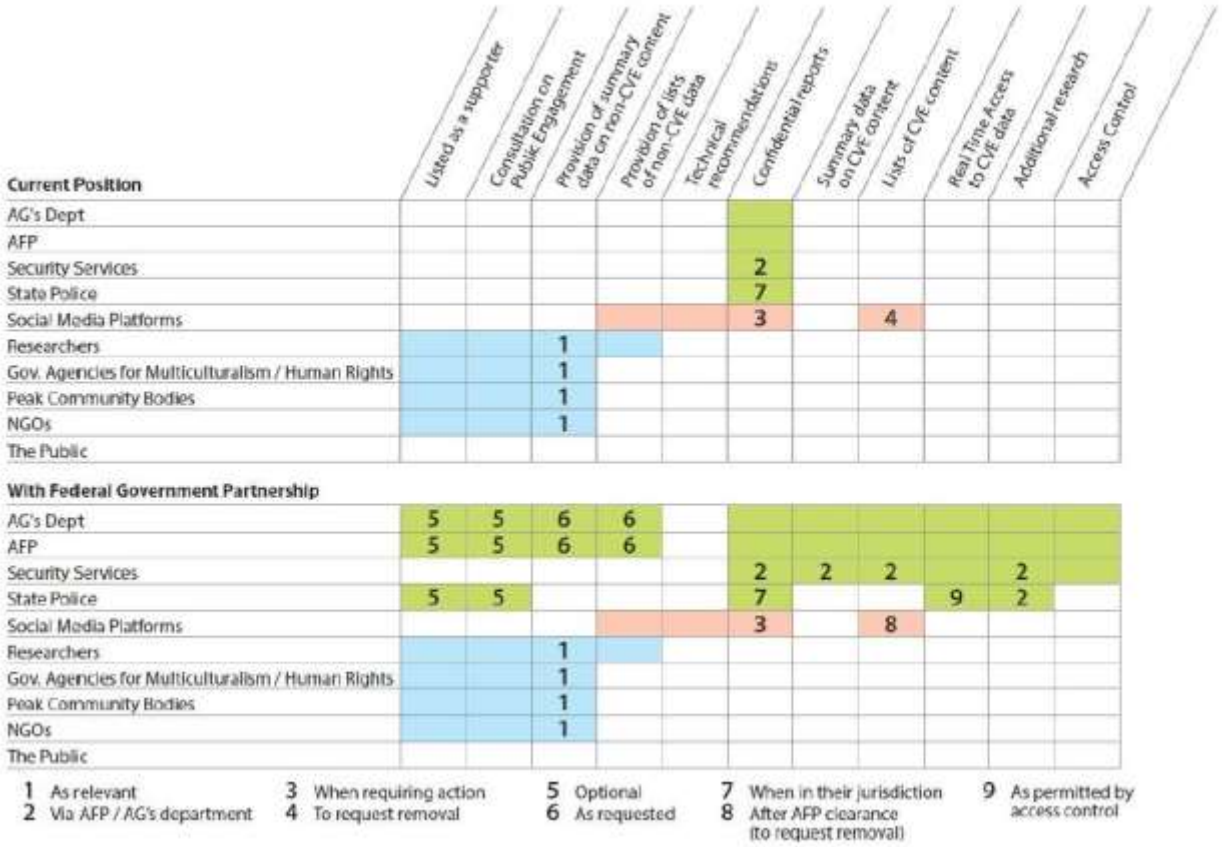

Figure 2 Current and projected capabilities, as per the 2015 proposal

The latest version of Fight Against Hate allows the tool to be embedded as a widget in the websites or Facebook pages of organisations. The categories that can be reported are configurable for each organisation, as is all text within the system – allowing it to be translated and to run in a range of different languages or simply with different wording as appropriate. Federal Cabinet approved a project using this system for the reporting of antisemitism and Holocaust denial as part of Australia's engagement in the International Holocaust Remembrance Alliance. The tools allow civil society to integrate with government, reporting serious incidents, while also acting as a buffer by reducing the need for more sweeping government surveillance to find the same data.

A proposal to alter the software to support police in responding to online threats to public safety during major incidents was presented to the technology companies, the department of Home Affairs, and other stakeholders in 2018.[15]

CRITERIA 1: NATURE AND EXTENT OF THE THREAT

The Australian government has led international calls for stronger action by social media companies to tackle online extremism and particularly the use of the Internet to share abhorrent violent material. Tech companies are being told they need to make their products safe for the public.

> "The rules in the digital world have to be the same as the rules in the physical world. What we expect of companies in the physical world you should expect from companies in the digital world... They have to take responsibility for what they produce and the services they provide and making sure they don't harm people." - Prime Minister Scott Morrison, August 2019

Our CEO, Dr Andre Oboler, has been warning the tech companies they need to lift their game and face up to their public responsibilities for over a decade.

> "The rise of social media over the last seven years has revolutionised communication... Behind these platforms are large corporations who profit from the communication they facilitate, yet take little responsibility over the content. A new approach is needed in which corporations that seek to profit from social media assume public obligations... Only a legal obligation to take reasonable steps in reasonable time will ensure sufficient effort is invested in responding effectively"
> Dr Andre Oboler, Internet Law Bulletin, 2010

TECHNOLOGY PLATFORMS

When it comes to dangerous content, we have strong links with the major tech companies and are usually able to get action far faster than police or other parts of government. This is partly cultural, particularly with US based organisations, as requests from government need to follow strict formal processes while requests from us are treated informally and usually with a spirit of cooperation. This back channel has been used by government on multiple occasions in the interest of public safety.

The platforms recognise and respect our efforts to reach out to them to resolve issues before putting a public spotlight on them. We are entirely independently and when they fail to take appropriate action we shine a spotlight on it, but when they respond quickly and reasonably we are happy to publicly

[15] https://www.facebook.com/284088808335015/videos/1800284873382060

acknowledge this. In light of this, we meet regularly with some of the platforms and have open channels of communication with representatives of many more.

The current exodus of many extremists from mainstream social media platforms to fringe platforms makes it far harder to secure action removing hate and extremist content as the fringe platforms often have no desire to address the problem.

THE THREAT OF LONE WOLF ATTACKS

Our largest concern at present is from lone wolf attacks carried out by those who are not formally part of any group, but who have self-radicalized into white supremacy through online content. Addressing this threat means removing the pathways to radicalisation.

Recently, for example, our action led to Twitter closing a white supremacist account that had been using automation to floor the Australian political discussion (#auspol) with white supremacy messages every day for years.[16] Our efforts led first to the closer of their automation account, then to the closer of the Twitter account itself. Accounts like these send a message of normalisation for white supremacy into society which is designed to encourage people to start searching, reading, and enter a pathway into online radicalization.

Figure 3 One of over 11,000 white supremacist tweets from this one account, all targeting #auspol

The closure of this account reduces the risk of radicalisation. While the content is clearly white supremacist, and therefore promoting an extremist ideology, the content it tweeted was not directly inciting violence. Platforms have recognised the promotion of such ideologies is dangerous even without explicit calls for violence. The law has not yet caught up to this.

QANON

We have a particular concern regarding QAnon who are open to conspiracy theories, and who have been migrating to alternative social media spaces like Gab and Telegram (and previously Parler). These spaces are steeped in white supremacy and the QAnon influx is leading to more people being radicalised from QAnon conspiracies into white supremacy. Our CEO, Dr Oboler, has been assisting the American Jewish Congress with research into this phenomena in the United States.[17] The same factors and pipeline into radicalisation observed there are observed in the Australian context in our own work.

[16] https://ohpi.org.au/extremism-online-the-automation-of-white-supremacy/

[17] https://ajcongress.org/reports/

8CHAN AND SIMILAR PLATFORMS

4chan and 8Kun (former 8chan), as well as many smaller clones of these sites, also continues to pose a significant risk. The /pol/ community on these boards, linked to the 2019 attacks is Christchurch, Poway, El Paso and Halle, continues to be a particular risk. The presence of Australians I these forums is disproportionately high, in past work we were the 4th most common source of traffic to 4chan in absolute terms and a close second to one of the smaller Scandinavian countries on a per capita basis (but far higher than the United States and United Kingdom on a per capita basis). We have examined this threat in detail and outlined a series of recommendations in our Halle Report.[18]

FAR RIGHT & COVID

During times of economic stress the far-right often looks to scapegoat minorities and gains a significant boost from (typically) young men who are finding things difficult. Covid-19 hate started by focusing on the Chinese and Asian communities, and while initial efforts to target the Jewish community did not gain much traction, that is changing with new Covid related hate messaging. Some messaging promotes the idea the Jewish community is behind COVID as a means of control, these are similar to QAnon theories but with the deep state replaced by the conspiracies of Jewish power on which QAnon theories were originally based. Other antisemitic conspiracy theories are based on the idea of Jewish businesses / people profiting from the pandemic. Our earlier work on COVID and online hate was submitted to the Victorian Parliament.[19]

ISLAMIST EXTREMISM & COVID

There is also a rising threat from Islamist extremism with ISIS and al-Qaeda both engaging in online radicalisation through COVID and seeking to use COVID as a trigger to radicalization.[20] This has led to recent attacks in Europe. We don't have evidence of this in Australia, but continued vigilance is warranted as the same online messages will be visible here as well.

CRITERIA 2: GEOGRAPHIC SPREAD AND INTERNATIONAL LINKS

PREVALENCE OF QUEENSLAND

In our work we find most of those engaged in online hate are from Queensland. In 2014 we examined a page opposing a proposed mosque in Bendigo, Victoria.[21] There was a campaign which targeted (online

[18] https://ohpi.org.au/hate-and-violent-extremism-from-an-online-subculture-the-yom-kippur-terrorist-attack-in-halle-germany/

[19] https://parliament.vic.gov.au/images/stories/committees/lsic-LA/Inquiry_into_Anti-Vilification_Protections_/Submissions/Supplementary_submissions/038_2020.06.17_-_Online_Hate_Prevention_Institute_Redacted.pdf

[20] https://ohpi.org.au/why-suddenly-has-islamist-terrorism-made-a-resurgence-in-the-west/

[21] https://ohpi.org.au/the-bendigo-mosque-exporting-hate-to-regional-victoria/

and offline) local council members for approving the mosque. Our researching into those engaged with this anti-mosque group showed that Queensland accounted for 31% of the audience. This was significant larger thank Victoria (where the mosque was based) or the rest of Australia combined (excluding Victoria and Queensland).

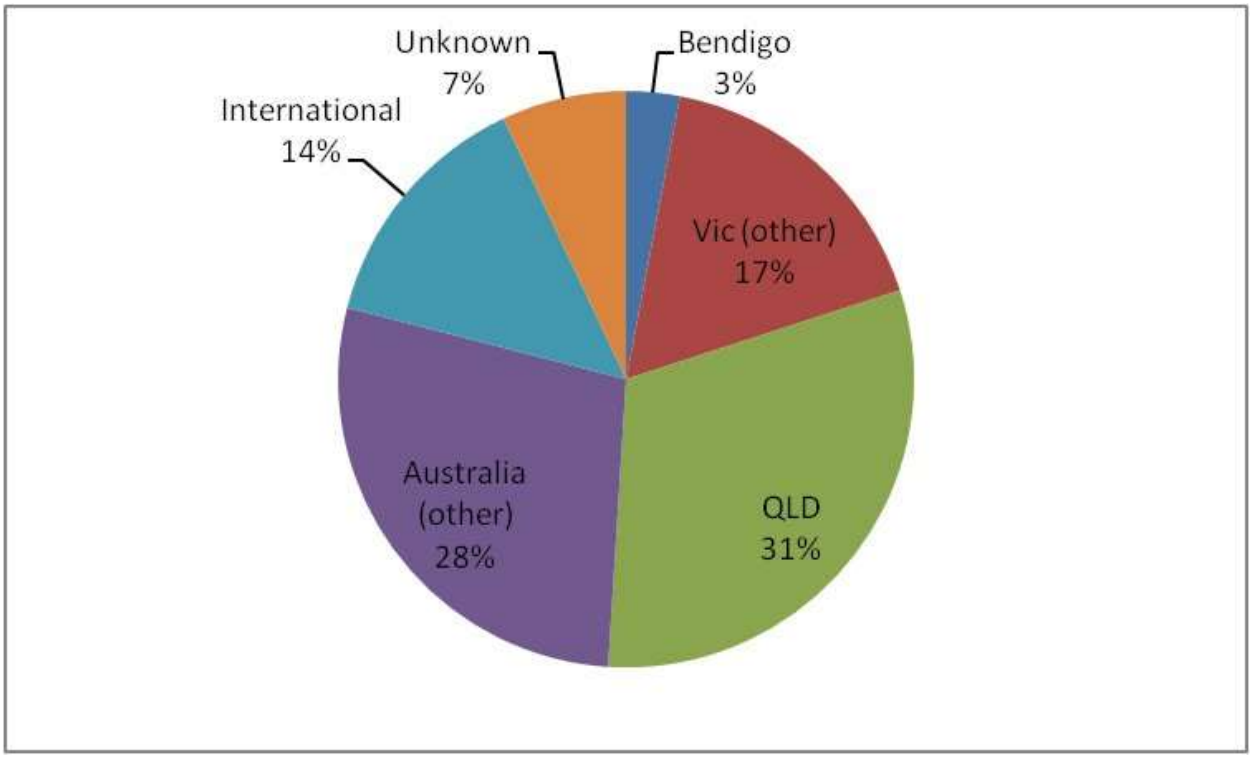

Figure 4 Where people came from in the Stop the Bendigo Mosque page

When we examine SOCINT, we see people from around Australia, but Queensland is almost always disproportionately represented.

ANTIPODEAN RESISTANCE IN VICTORIA & INTERNATIONAL LINKS

In Victoria the local presence of the *Antipodean Resistance* (which since late 2020 has merged into the National Socialist Network) has for some years led to a spike in stickers and posters with hate messages and symbols. We have tracked the group since they were in the process of forming and provided earlier background on them to police and intelligence service as well as releasing some of the information publicly, while redacting the group's name and other identifiers. [22]

This group was started by people radicalized on 8chan's /pol/ (like Brenton Tarrant) and who received instructions there which led them to the now closed neo-Nazi website Iron March. It was on Iron March

[22] https://ohpi.org.au/nazi-groups-poster-campaign-melbourne/

where they posted (see below) their desire to network with others in Australia. Iron March was also central to the neo-Nazi terrorist group Atomwaffen Division based in Texas, USA.

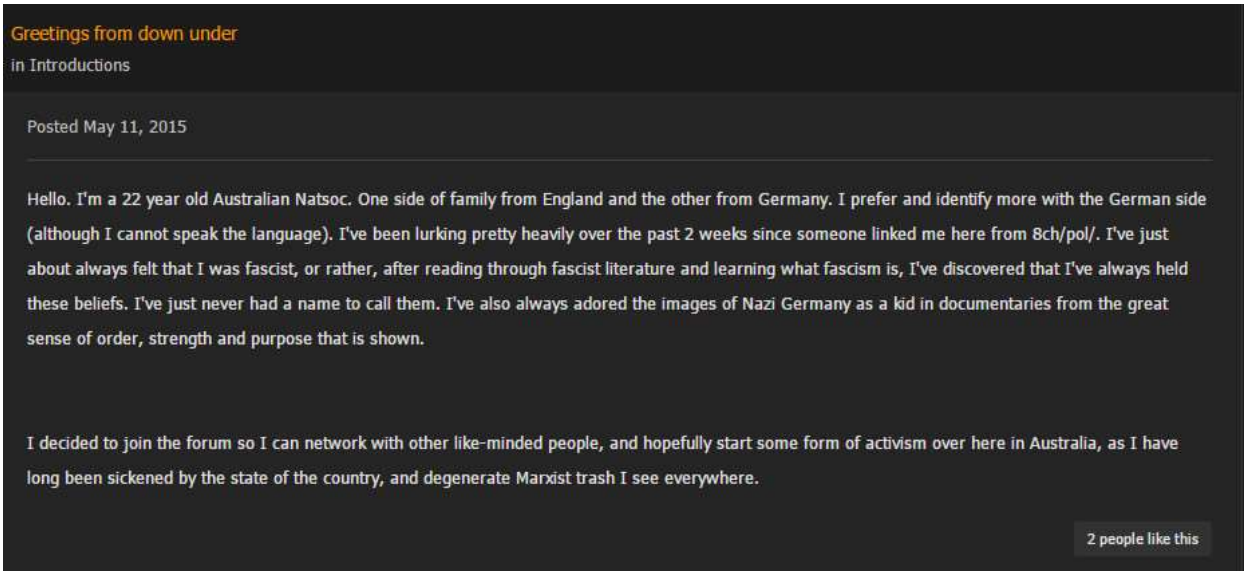

Figure 5 The Iron March Post from Antipodean Resistance's forming

Antipodean Resistance later noted how they were inspired by European groups and took their look and style from them. The Nordic Resistance Movement (centred in Finland), Atomwaffen Division (Texas, USA) and National Action (UK) are some of the groups they claim inspire them / that they are connected with. We note that Twitter did close their account back in 2017 as part of a wider action to de-platform white nationalist groups.[23]

Under their new branding as the "National Socialist Network" they recently received significant media coverage for an Australia Day 2021 trip to the Grampians where they burnt a wooden cross KKK style and engaged in other intimidating behaviour. The trip was clearly to get media attention for the new

[23] https://ohpi.org.au/twitter-getting-tougher-on-hate/

brand given a past trip they made to the Grampians as Antipodean Resistance in 2017 (when that brand was new) had a similar effect.

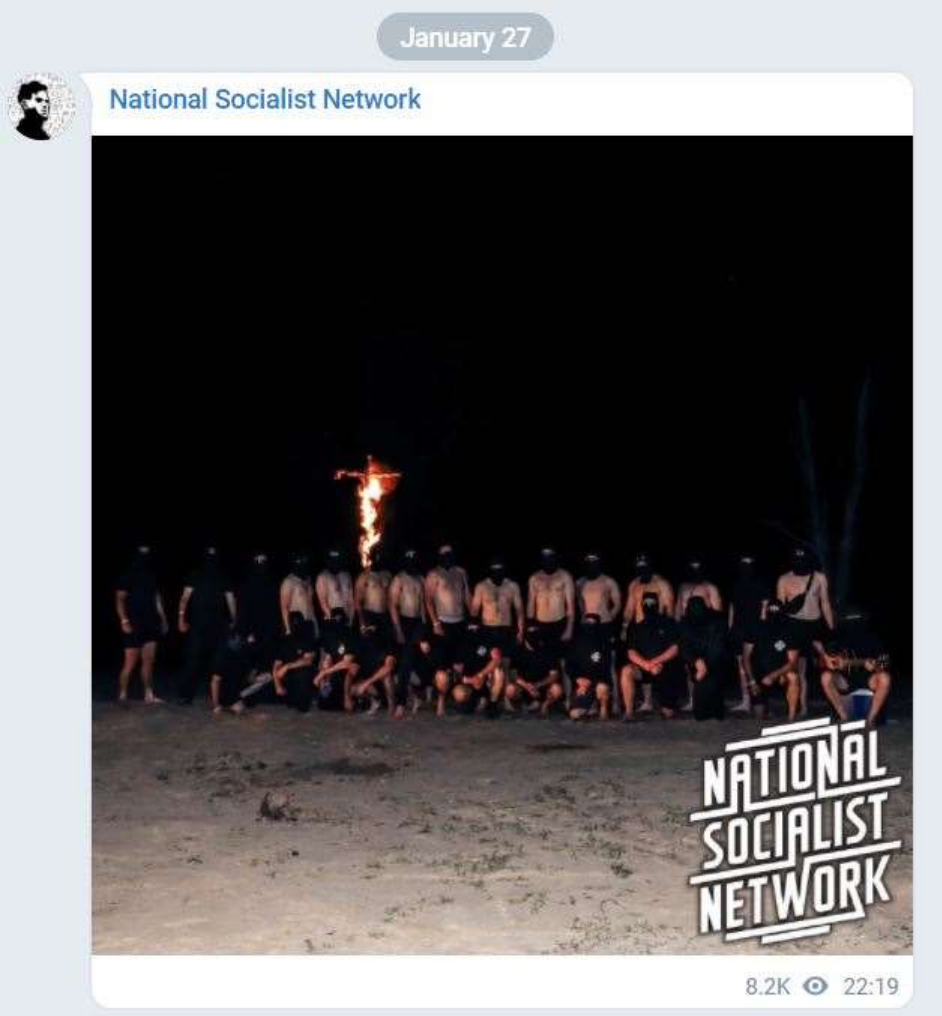

Figure 6 From the National Socialist Network Telegram

SELF-RADICALIZATION

As mentioned, when it comes to the risk of a major terrorist incident, we are most concerned at the risk of internet based self-radicalized individuals who then carry out a lone wolf attack. Such individuals can easily be radicalized and then incited to violence by those based overseas. There is no need for them to form or join local groups here in Australia. In some cases, users are both anonymous and self-identifying as Australian in forums like 8chan. In others, it isn't possible to separate Australian threats from those overseas.

While people on this pathway to extremism are self-radicalized and don't answer to any organisation, they still see themselves as part of broad and international community of like-minded people. This is a

far looser affiliation than terrorist groups of the past, but it does mean attacks in one country can inspire others to action.

CRITERIA 3(A): TERROR ORGANISATION LISTING LAWS

The *most visible* local extremist groups are liable to change names regularly. Media often mistakes activities under a new brand as a sign of growing extremism. In reality it is often the same individuals rebranding themselves. While this tactic was developed to get around bans from social media companies, it may prove equally effective in defeating terror organisation listing laws.

These high visibility "organisations" tend to be centred around one or more high profile individuals who use social media, and when they can mainstream media (often through stunts) as a means to build profile, online followers, and then generate income from online advertising, online sales of merchandise and donations from supporters.

If terror listing laws are to be effective they would need a far lower threshold before an organisation can be added. At present Facebook has far better systems for identifying and banning those who seek to promote extremist ideology than the government. They also maintain better relations with civil society groups working in this space than the government.

If the government wishes to proscribe those promoting extremist ideologies, it may need to focus on the ideology itself and not the name it is being promoted under. White nationalism, QAnon, neo-Nazism, and Islamist extremism, with police, eSafety or others able to determine if a group falls within that ideology, would be far more robust. Given the vast majority of the activity occurs online, a focus on online disruptions of spaces dedicated to such ideologies is critical. It has less impact on fundamental freedoms, ad could therefore be implemented with a lower threshold.

The draft Bill for a new Online Safety Act could be drafted to provide a more general power to eSafety allowing them to require the closure of accounts and termination of services supporting extremist ideologies. Regular transparency reporting to the Parliament on what has been closed and why, along with some kind of appeal process for those whose accounts / websites are closed would help protect fundamental rights under such a system.

CRITERIA 3(B): CAPACITY AND PARTNERSHIPS

The Counter-Terrorism strategy has failed to properly engage with civil society.

A few of the benefits of civil society engagement are:

- Access to information from people who won't give it directly to government.
- Faster responses on time sensitive information and the ability to escalate it to government for priority attention (assuming relationships are in place)
- The ability to add resource in open source intelligence gathering to areas which are lower priority for agencies, but which may turn up high priority information.
- The ability to work with different partner organisation in Australia and overseas to government

- A different type of credibility and trust to government which opens other opportunities.
- Influence which is often greater than government when it comes to technology companies, and an ability to promote change in the public interest and to secure media and public support.
- Access to dialogues with technology platforms and other experts

Hate Prevention Institute requested a wide reaching formal partnership to government (ADG) in 2015. Many of these ideas are still valid and would have, and still can, help enhance Australia's defence in depth against extremism.

We have at times also found ourselves as the conduit for information between state and federal authorities who were unable to communicate directly, or who hadn't been aware of related investigations. We have at times played the role of a clearing house for non-classified intelligence on extremism.

Importantly, working with colleagues in the Washington DC based Counter Terrorism Group, we collaborated on a project in 2020 which found extremist groups from the United States attempting to recruit Australian citizens on local platforms. We were able to provide support in identify the agents and their internet status and history, and report to Australian authorities.

CRITERIA 3(C): IMPACT OF UNPRESCRIBED GROUPS ON DISHARMONY & RADICALIZATION

A significant part amount of concern in the community, indeed media attention on extremism, is caused by groups that are unlikely to be prescribed unless a far broader approach to prescription is take (as mentioned above). These groups make people feel unwelcome and exuded from the community.[24] They create tensions between communities and as we recently discussed in the media, they inspire lawless vigilantism.[25] Most concerningly, we find it is often not the "public figures" of extremism and their posts into social media which are the most extreme, but rather the comments in reply to their posts. They create a space online where extremism, including death threats and incitement, flourish.

Online channels provide a megaphone that greatly increases the harm such individuals and groups can cause, both with what they say and through the interactions among their followers which they facilitate. The spaces they create are the entry point to radicalization.

CRITERIA 3(D): DISRUPTING & DETERRING HATE SPEECH

The Online Hate Prevention Institute has the mandate from the government, as Australia's only dedicated harm prevention charity focused on online hate, to tackle this problem. In addition to our

[24] https://www.parliament.vic.gov.au/images/stories/committees/lsic-LA/Inquiry_into_Anti-Vilification_Protections_/Submissions/038_2020.01.17_-_Online_Hate_Prevention_Institute_Redacted.pdf

[25] https://www.abc.net.au/radionational/programs/breakfast/vigilante-justice-in-australia/13143346

work tackling extremism we have covered a wide range of different types of hate,[26] some the major areas include: Racism in general, Antisemitism, Holocaust denial, Islamophobia, racism against Indigenous Australians, hate directed against the ANZACs and military veterans, serious trolling, cyberbullying, Griefing, Misogyny, and Homophobia.

We welcome the inclusion of discussion on disrupting and deterring hate speech within the terms of reference of this inquiry. Prof. Andrew Jakubowicz from UTS and clearly explained the link between hate speech and extremism as well as the role we play in this space in the Australian context: [27]

> **"Governments often do not see racism as important enough an issue to provide the level of investment necessary for civil society action against it. Organisations such as the Online Hate Prevention Institute, identified globally as innovators in finding and outing racism online, struggle to survive as Australian governments focus on protecting children and tracking terrorist recruitment. While these other related spheres are clearly very important, racism online contributes greatly to both of them, threatening children and justifying in the minds of some their recruitment into violence against their racialised 'enemies'"**

We note that since that was published far more of our work has been focused on countering extremism, the public work is on our website,[28] but far more is already with a range of government agencies and departments and can be made available confidentially to other parts of government on request.

We believe far more needs to be done to disrupt and deter hate speech, particularly online. Disruption through the removal of content and closing of accounts, which also disrupts online networks, has a significant degree of effect. The removal of content and online penalties such as temporary bans help to set norms. Where the content is more serious, the action more prolonged or the people responsible are engaged in a repeated cause of action or the creation of accounts or spaced dedicated to hate, then off-line responses and greater deterrent may be needed. We have discussed this at length in a submission into eSafety.[29] We also make recommendations in our report into terrorism from /pol/ on 4chan, the recommendations are summarized near the front of the report.[30]

---

[26] https://ohpi.org.au/

[27] Jakubowicz, A. 2017. Alt_Right White Lite: trolling, hate speech and cyber racism on social media. Cosmopolitan Civil Societies: an Interdisciplinary Journal. 9(3), 41-60. http://dx.doi.org/10.5130/ccs.v9i3.5655

[28] https://ohpi.org.au/terrorism-violent-extremism/

[29] https://www.communications.gov.au/sites/default/files/submissions/consultation_on_a_new_online_safety_act_-_submission_-_the_online_hate_prevention_institute.pdf

[30] https://ohpi.org.au/hate-and-violent-extremism-from-an-online-subculture-the-yom-kippur-terrorist-attack-in-halle-germany/

We note an additional problem with disrupting hate speech which is the use by Australian hate groups of overseas technology suppliers. The *National Socialist Network*, in Melbourne for example, has a website uses it to promote their views, but also their social media accounts on Telegram and Gab.

Figure 7 Nationalist Socialist Network Website

In addition to the Nazi salute on the front page, and the page promotes the same "white genocide" conspiracy theory of terrorists like Brenton Tarrant. It includes a variant on the 14 words (see Figure 8), the phrase "We must secure the existence of our people and a future for white children", a popular white supremacist slogan coined by the terrorist David Lane of the Order a US terrorist group from the 1980s.[31] Hidden in the code of the page is a swastika (see Figure 9).

The site's domain is registered through Dreamhost, the same company which until recently hosted Parler. Their hosting is with Cyber Cast International, S.A. based in Panama. The company's terms of service prohibit "Under Legal Age nudity or modelling, Illegal drugs and drug contraband, Weapons selling websites, Carding Websites, Phishing Websites, DDoSers, Booters, Stressers, Scanners, Botnets, IP Spoofing" but do not prohibit terrorism or hate speech. In fact, their terms of service suggest that outside of the above, they will refused to take action without a court order from their local courts:

> "Freedom of speech: Panamanian Constitution respect freedom of speech. Consequently, we do not censor our members on the basis of content. The Customer is fully responsible of the content, posts, articles hosted in our servers or network. Complainer should forward copy of competent panamanian court order in order to request content removal,

[31] https://www.adl.org/education/references/hate-symbols/14-words

in the case that this is not possible the complainer will need to work directly with the Website operator to resolve the situation."[32]

Sites with terms of service like these either need to reach an agreement with the Australian government or site wide blocks need to be considered. This is again a matter than could be addressed through the eSafety legislation.

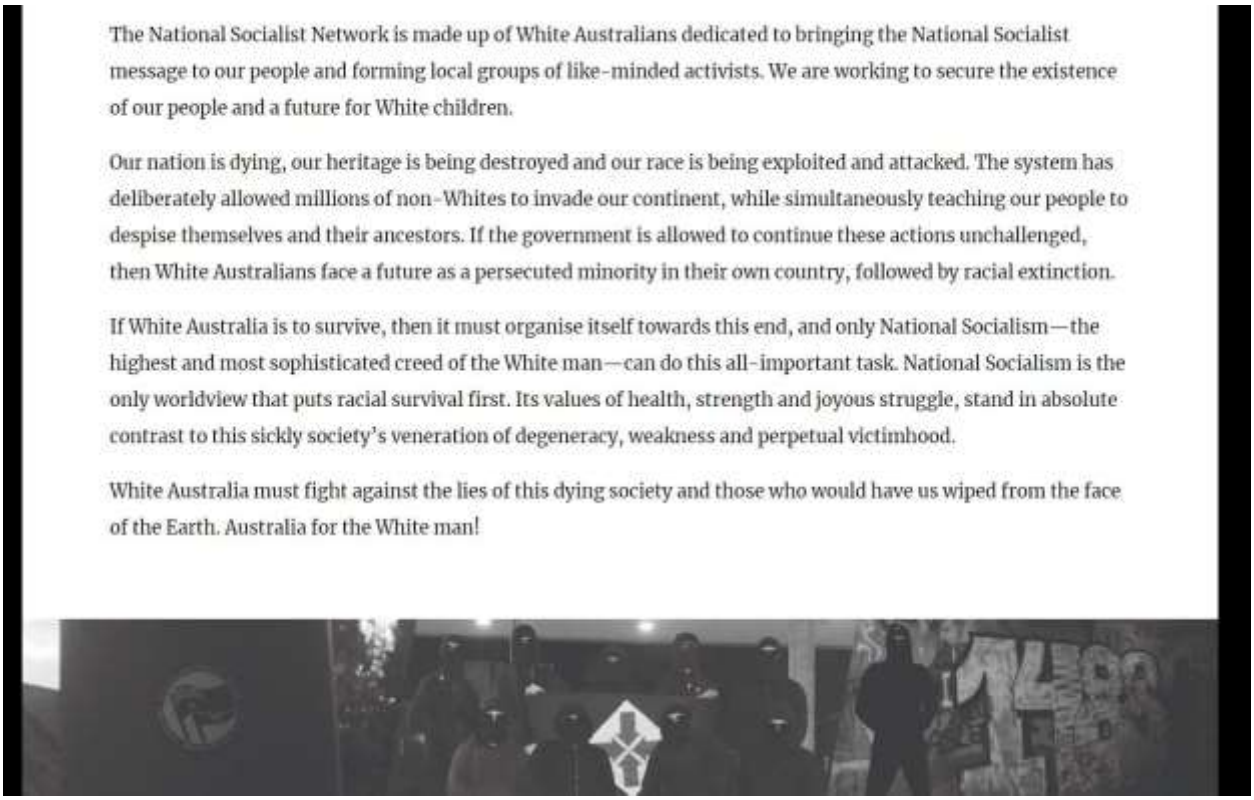

Figure 8 The white nationalist ideology of the National Socialist Network

[32] https://www.ccihosting.com/acceptable-use-policy.html

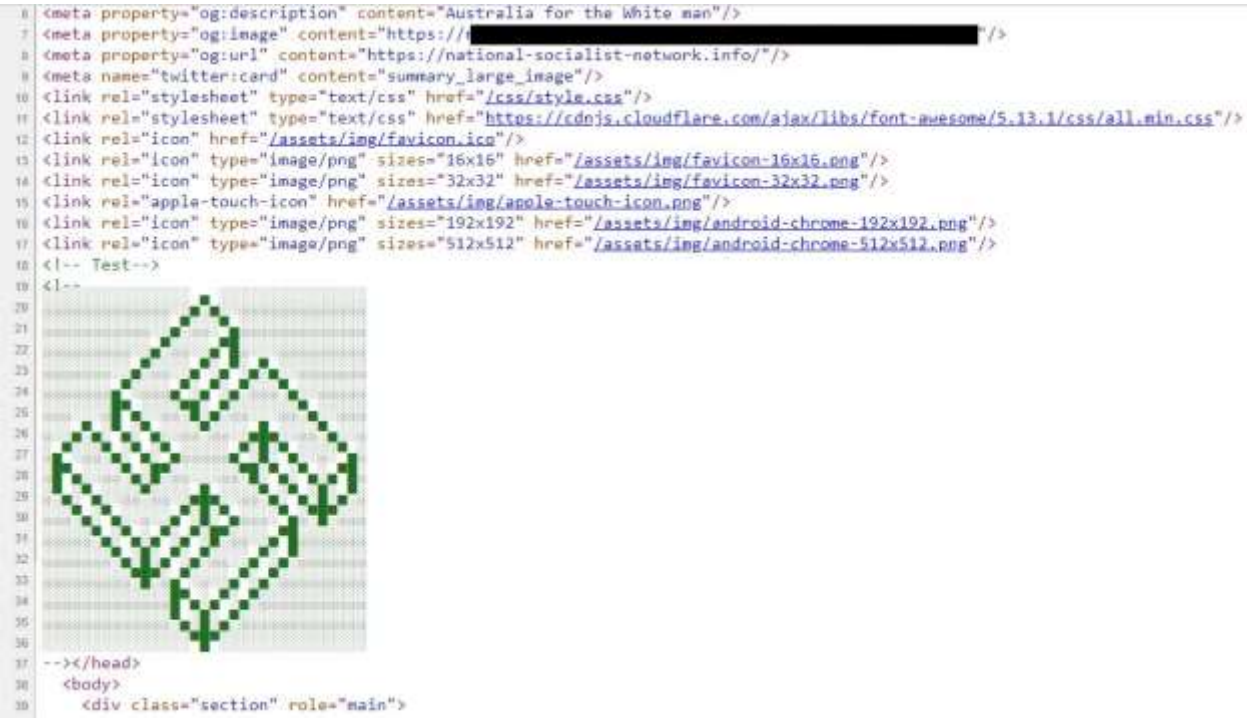

Figure 9 Source code of the National Socialist Network website

CRTIERIA 3(D) (CONT): REGULATING SYMBOLS OF TERRORISM AND EXTREMISM

OHPI has been active on the issue of symbols that are coded hate speech. We have reported and communicated specifically on use of the swastika and internet symbols and letter arrangements that are encoded attacks on various groups.

While we believe there should be a general ability to block or demand removal of content that includes hate systems, we recognise that extremists already readily change their symbols and invent new ones, particularly symbols with duplicate meanings, in order to make such approaches less successful. This approach of coded messages and symbols was developed more to defeat artificial intelligence approaches looking for such symbols than to avoid legal penalties.

Rather the writing symbols into legislation, a consultative committee including experts form government and civil society (both charities and academia) should be established to advise the minister or an appropriate government official on the changing symbols and names that are in use. A system to prohibit such symbols needs to be flexible, rapid and based on consultation.

CRITERIA 3(E): SOCIAL COHESION, CVE AND DIVERSIFICATION OF EXTREMISM

OHPI can attest to the success in the consistent pressuring of social media platforms to adjust their policies and programs to address online hate. In 2020 Facebook briefed OHPI and recognised its efforts in campaigning to ban Holocaust Denial from its platform. A campaign OHPI, and prior its CEO, had been campaigning for over 12 years.

We believe the approach to CVE around 2015, which saw AFP engage more with a wide range of community organisations, was more effective than the current approach. As an organisation that works across many forms of hate and extremism welcome the efforts by various parts of government to reach out to us, but we are concerned that CVE resources have seldom supported civil society groups, and particularly not civil society groups of a general nature (rather than being from specific communities).

We have seen how extremists have changed target, particularly during COVID, but even before that we saw neo-Nazis broadening their reach by focusing on Islamophobia. We need broad base coalition of organisations working in this space and supported by government. At present Facebook is doing more than the government when it comes to convening and supporting civil society groups. This not only leaves government without the support and added value of civil society, but it changes the dynamic ad will make the government's underlying approach harder to implement.

CRITERIA 3(F): THE ROLE OF SOCIAL MEDIA, ENCRYPTED COMMUNICATIONS & DARK WEB

As addressed above we are seeing a shift from mainstream social media platforms (particularly Facebook) to alternative platforms. The exodus from other platforms is slower and proportionate to the platforms efforts to de-platform those with extreme views. The shift to such platforms presents new challenges, but also reduced the reach.

CRITERIA 3(G): OTHER MATTERS

The Australian Constitution, s 51(v) gives the Commonwealth power to legislation with respect to communications including the Internet. As a practical matter, technology companies wish to deal with a single point of contact. It is therefore appropriate that the Commonwealth take the lead in tackling matters of online radicalisation, extremism and the hate speech which can lead to it.

In exercising this power, the Commonwealth should accept referrals of power from the states to enable federal action under the communications power in response to breaches of state law which manifest online. This may relate to orders for the provisions of data (such as IP addresses), the saving of records, the removal of content or the blocking of services. A combination of Federal Police and the Office of the eSafety Commissioner have such powers, but their application is limited (even under the current draft Bill for a New Online Safety Act). This could be broadened to allow action in response to any content, certified by an appropriately authority, to be likely to be unlawful under Commonwealth or state law.

Given the communications power, we also believe the Commonwealth should administer a grants program to support civil society efforts to tackle online hate and extremism. As we presented to the United Nations:

> "In considering how we address online hate, one thing is clear: wishful thinking is not enough. Neither are memes and videos opposing hate, positive initiatives that bring people and communities together, education programs for school, public advocacy or public education. Counter speech is not enough. Empowering young people is not enough.

> These are the dominant approaches of recent years, they are what we have promoted even as the hate continued to rise. If we want to get on top of this problem, we need take it more seriously. We need to invest both economically and through political capital in real solutions."[33]

In the address, with further elaboration in a supporting paper,[34] we outlined areas where investment has in the past proven to be effective:

- Forums that bring together government and civil society allowing for sharing of information, the establishment of relationships and the development of a 360 snapshot view of the current online situation.
- Support for civil society organisations that specialise in tackling online hate and extremism but which are not tied to specific types of hate or specific ethnic / religious communities. The skills needed in this space work across areas of hate and are in very short supply. Hate group and content often shift between targets. A coherent approach is more effective.
- There needs to be incentive and support for specialist civil society organisations to collaborate with community based civil society organisations and the people in these communities who live the reality of the online hate.
- There are definitions, like the IHRA Working Definition of Antisemitism, which can greatly help in identifying hate speech and extremism. Such definitions should be adopted in Australia, just as they have been adopted overseas.

ABOUT THE AUTHORS

DR ANDRE OBOLER

Dr Andre Oboler is the CEO & Managing Director of the Online Hate Prevention Institute. He is an Honorary Associate at La Trobe Law School, a global Vice President of the IEEE Computer Society, a member of the Global Public Policy Committee of the IEEE and an expert member of the Australian Government's Delegation to the International Holocaust Remembrance Alliance.

Andre was formerly a Senior Lecturer in Cyber Security at the La Trobe Law School, intercultural liaison for the Victorian Education Department's independent inquiry into antisemitism, co-chair of the Online Antisemitism working group of the Global Forum to Combat Antisemitism, an expert member of the Inter-Parliamentary Coalition to Combatting Antisemitism and served for two terms with the board of the UK's higher education regulator the QAA. His research interests include online regulation, hate speech and extremism in social media, and the impacts of technology on society.

[33] https://ohpi.org.au/address-to-the-united-nations/

[34] https://ohpi.org.au/wp-content/uploads/2020/11/Oboler-Full-Paper.pdf

He holds a PhD in Computer Science from Lancaster University, and a B. Comp. Sci. (Hons) & LLM(Juris Doctor) from Monash University. He is a Senior Member of the IEEE, a Graduate Member of the Australian Institute of Company Directors and a Member of the Victorian Society of Computers & Law.

MARK CIVITELLA

Mark Civitella is the Chairman of the Board of Directors of the Online Hate Prevention Institute. He is a Lecturer in Strategic Communication at La Trobe University and works as a strategic communication consultant. He is a Fellow of the Public Relations Institute of Australia.

Mark has expertise in countering violent extremism and political communications as well as issue and crisis management. He has consulted widely and worked with Monash University's Global Terrorism Research Centre, Victorian Multicultural Commission, Victorian Imams Network, and trained religious and cultural leaders.

Mark has been a director of a number of communication and research companies. He holds a B.A. (Monash University); Diploma in General and Comparative Literature (Monash University); Graduate Diploma in Public Relations (RMIT University) and is currently Doctoral Candidate at La Trobe University.