Executive Summary

A new form of terrorism emerged in 2019. Incubated by a globalised, toxic, anonymous online culture, incitement to hate now all too frequently leads to violent extremism that manifests offline, and has cost the lives of dozens of innocents, including children. Participants and spectators of this newly forged online culture encourage, support and celebrate the serious crimes that they commit, and revel in the chaos and destruction they inflict.

At the centre of the online culture discussed in this report is '/pol/' (short for "politically Incorrect"), a board found on Image Board serves such as 4chan, 8chan and others. It is not so much a place as a community with its own culture; one that has turned decidedly toxic then increasingly extreme in recent years. It is community where everyone is anonymous so the cost of shifting to a new server causes only the smallest disruption.

There have been four terrorist attacks in 2019 directly linked to /pol/. The attacks in Christchurch (New Zealand), Poway (California, USA), El Paso (Texas, USA) and Halle (Germany) each began with a post to an imageboard that announced that the attack was imminent, and provided links to both a manifesto and a livestream feed to watch the attack unfold. While the minority groups that have been the targets of these attacks have varied, what remained consistent was the link back to /pol/.

This report opens with an introduction in part one that establishes the links between the attacks, the image board community and the culture of /pol/ in particular. This is a new form of online extremism. One based on anonymity, leaderless resistance (where attackers choose their own targets as part of a larger campaign), and an ideology of hate build up through conspiracy theories, memes, and the idea of red pilling in which only those who conform to the culture and its ideology of antisemitism, misogyny, racism and a myth of an embattled but superior white race under threat of replacement, are considered enlightened. It is a culture which in 2019 turned violent not once but four times. It is a culture where the attacks that occurred carried calls for further violent action. This threat needs to be taken seriously as there is no reason to believe we have seen the last of these deadly attacks.

We continue our introduction with a discussion of regulation, Internet exceptionalism and the shift to greater recognition of national sovereignty when it comes to Internet regulation. This background is essential to understanding later parts of the report which examine the position taken by 8chan, the platform which hosted the

/pol/ board used to announce the three attacks prior to Halle. Even after repeated uses of its platform to promote terrorism, 8chan continued to advocate against restricting the hate speech which spread the culture of extremism. They held that only the posts announcing an imminent attack should be removed. The response by governments and industry (particularly CloudFlare and Voxility), and 8chan's response to those actions will a critical case study in future discussions of the Internet and its regulation.

The final part of our introduction discusses the nature of hate speech itself. This provides essential background to the many recommendations we present in this report to aid stakeholder address the problem of online hate and incitement through a more integrated approach of government, platform and civil society action. The problem is not just incitement to violence, but also incitement to hate itself.

In the second part of the report we introduce the Halle attack and provides an analysis of the attacker, the material he posted online and the online elements of his attack. This is followed by the third section which gives a detailed look at the manifestations of antisemitic that appear in the attacker's communications. We use the International Holocaust Remembrance Alliance's Working Definition of Antisemitism to aid this analysis.

The fourth section looks at the response to the attack. We examine the response on /pol/, the spread of the attacker's material online. We also examined the response by the technology sector, governments and civil society. Our analysis looks at Google, Twitch, Cloudflare, and Facebook among others. We also look at civil society, including Tech Against Terrorism and GIFCT. We congratulate the stakeholders involved for their response, but also highlight areas where there are opportunities for improve. In compiling this report we have consulted with many of them and thank them for their cooperation and the information they have shared.

In the fifth section we trace the origins of the recent rise and influence of a globalised, toxic, anonymous online culture, and offer a comprehensive introduction to its key characteristics. We also provide new insight into the subcultural core of this new kind of online extremism through a close examination of '/pol/'. We highlight how its early culture promoted of Nazism, racism, and xenophobia but did so as a form of trolling. Those who took what was said seriously would soon be turned on by the mob. We discuss how this changed under a concerted effort by neo-Nazis from Stormfront to co-opt /pol/ to their ideological war of hate. As /pol/ absorbed this deeper and more sincere form of hate, it fused it with its own culture. /Pol/ gained substantial momentum and its influence spread across multiple boards and sites. We also look more broadly at the culture based on hate, including Gamergate, weaponised memetics, the Alt-Right, the politics and history of 8chan, and more. We trace the development of the toxic online culture which intersects with /pol/ as /pol/ shifted from hate speech to hate action including terrorism.

Throughout this report, we offer recommendations for a range of stakeholders that can be implemented to improve the efficacy of dealing with this new form of terrorism. We provide an extensive series of practical recommendations for Australian and international publics, civil society, governments, private enterprises and organisations, as well as for the introduction, revision and refinement of extant regulations, policy and legislation.

Although the management of these incidents is gradually improving, there remains a substantial gap between the promises for greater action which have been made publicly and the reality. It is in this gap where incitement festers, that the process of radicalisation proceeds unabated, and the risk of further attacks grow. Any effective response will require the active participation, cooperation and investment of governments, technology companies, and civil society as partners, with a shared interest, in combating what has become a significant threat to our globalised societies.