



Online Hate  
Prevention Institute

ABN 65 155 287 657

# HATE AND VIOLENT EXTREMISM FROM AN ONLINE SUB-CULTURE

THE YOM KIPPUR TERRORIST ATTACK IN HALLE, GERMANY

ohpi.org.au  
info@ohpi.org.au  
facebook.com/onlinehate  
twitter.com/OnlineHate  
youtube.com/user/OnlineHate



Andre Oboler, William Allington  
and Patrick Scolyer-Gray



This work is licensed under a Creative Commons Attribution-  
NonCommercial-NoDerivatives 4.0 International License.





Hate and Violent Extremism from an Online Sub-Culture: The Yom Kippur Terrorist Attack in Halle, Germany

By Andre Oboler, William Allington and Patrick Scolyer-Gray

ISBN: 978-0-6487426-0-9 (eBook)



A catalogue record for this book is available from the National Library of Australia

Published in Melbourne by:

Online Hate Prevention Institute

E-mail: [ohpi@ohpi.org.au](mailto:ohpi@ohpi.org.au)

Website: <http://www.ohpi.org.au>

©2019 Online Hate Prevention Institute

This publication is copyright. Other than for the purpose of and subject to the conditions prescribed under the Copyright Act, no part of this publication may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording, or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquires should be addressed to the publishers.

This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/). Under the license you are welcome to upload copies of this report to other sites, or to make hard copies of the report, provided the report is reproduced in full and your use is not for a commercial purpose. This notice serves as prior written permission to the extent covered by the license.

**For other uses, please contact OHPI.**

## **Dedication**

**To those murdered in /pol/ related terror attacks in 2019 in Halle, El Paso, Poway, and Christchurch**

Jana Lange and Kevin S.

Jordan Anchondo, Jordan Anchondo, Arturo Benavides, Mario De Alba, Jessica Coca Garcia, Memo Garcia, Angie Englisbee, Leo Campos, Maribel Hernandez, Javier Amir Rodriguez, Ivan Manzano, David Johnson, Maria Flores, Raul Flores, Jorge Calvillo Garcia, Alexander Gerhard Hoffman, Luis Alfonso Juarez, Maria Eugenia Legarreta Rothe, Elsa Libera Marquez, Maribel Loya, Gloria Irma Marquez, Margie Reckard, Sarah Esther Regaldo Moriel, Adolfo Cerros Hernandez, Teresa Sanchez, Angelina Sliva-Elisbee and Juan Velazquez.

Lori Gilbert-Kaye

Mucad Ibrahim, Khalid Mustafa, Hamza Mustafa, Sayyad Milne, Ramiz Vora, Arif Vora, Atta Elayyan, Lilik Abdul Hamid, Areeb Ahmed, Tariq Omar, Muhammad Suhail Shahid, Syed Jahandad Ali, Haroon Mahmood, Farhaj Ahsan, Maheboob Khokhar, Muhammad Haziq Mohd-Tarmizi, Ansi Alibava, Ozair Kadir, Haji Daoud al-Nabi, Ali Elmadani, Husna Ahmad, Naeem Rashid, Talha Naeem, Amjad Hamid, Kamel Darwish, Linda Armstrong, Mohammed Imran Khan, Mohamad Moosid Mohamedhosen, Junaid Ismail, Abdelfattah Qasem, Ashraf Ali, Ashraf Ali Razat, Mathullah Safi, Hussein Al-Umari, Musa Vali Suleman Patel, Ashraf al-Masri, Hussein Moustafa, Mounir Soliman, Zeeshan Raza, Ghulam Hussain, Karam Bibi, Abdukadir Elmi, Mohsin Al Harbi, Osama Adnan Youssef Abukwaik, Mojammel Hoq, Mohammed Omar Faruk, Mohammed Abdusi Samad, Muse Nur Awale, Ahmed Gamal Eldin Mohamed Abdel Ghany, Zakaria Bhuiya and Zekeriya Tuyan.

**They will be remembered.**



## Foreword

On 9 October 2019 in Halle, Germany, a heavily armed far-right extremist attacked the Jewish community. Only a door that did not give way saved the Jewish community from possibly the biggest massacre after the Shoah. Two people were killed and Germany added to the list of terror attacks against Jewish Europeans – on Yom Kippur. Antisemitism has many expressions but online it finds the most fertile ground. Radicalisation has built up in recent years and connects antisemites worldwide to share and reinforce their conspiracies.

Halle showed us that radicalisation online leads to murder in the real world. Be it Pittsburgh or Poway, El Paso or Christchurch or a medium-sized town in the centre of Germany. The way to radicalisation is paved with antisemitic conspiracies labelling Jewish communities as the sources of evil, oppression and domination. Sometimes subtle, sometimes humorous and sometimes overt. Antisemitism has become the engine that drives far right racism, anti-Muslim hatred, xenophobia, homophobia and anti-gender movements. Only when we are able to decode this language and raise awareness about the intersectionality between antisemitism and other forms of hatred, will societies understand the need to react more forcefully.

The European Commission has proposed a regulation on countering terrorist content online within one-hour of detection. Our cooperation with internet companies in the EU Internet Forum is yielding concrete results. After Halle, all the 200 variants of the video and the manifesto, including the soundtrack used to glorify the attack, were removed within a couple of hours. Thanks to the Code of Conduct on Online Hate Speech, a collaborative process between IT companies, civil society and Member States, 89% of notifications are now reviewed within 24 hours and 72% of the content deemed to be illegal hate speech is removed.

I thank the Online Hate Prevention Institute (OHPI) for bringing together this valuable study and the useful recommendations. Only by better studying the phenomenon we are able to fight back. As President of the European Commission Ursula von der Leyen said: “Antisemitism is a poison for our community. And it is up to all to fight it, to prevent it and to eradicate it. The fight against antisemitism is as much for every other part of our community as it is for Jewish people. (...) We must all do our part. The Jewish community is not alone.

**Katherina Von Schnurbein**

**Coordinator on Combatting Antisemitism**

**European Commission**

## 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 servers 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 a 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 built 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 be 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 stakeholders 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 provide 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 antisemitism 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.



## The Online Hate Prevention Institute and Report Authors

Established in 2012, the Online Hate Prevention Institute (OHPI) is an Australian Charity on the Australian Government's Register of Harm Prevention Charities. We are a world leader in combating online hate and a critical partner who works with key stakeholders to improve the prevention, mitigation and response to online hate and extremism.

We invite organisations and agencies interested in using our tools, engaging us for consultation, or in developing longer term partnerships to combat online hate and extremism to [contact us directly](#).

Our online reporting tools accommodate multiple languages and are exceptionally flexible, are easy to configure in order to combat many different types of hate, and can be licensed at affordable prices. They are accessible to organisations of any size yet offer results powerful enough to support large NGOs and government-based human rights agencies. Under an existing arrangement, a limited number of free licenses are available for community organisations based in Victoria, Australia.

### **Our Work Needs Your Support**

OHPI depends on public donations to make our work possible. We are a small charity operating with limited resources, but we are proud of the formidable impact our work has had in the ongoing battle to rid the Internet of online hate and extremism. Every donation makes a real difference to us. Donations are accepted globally. Donations of at least two dollars from Australian tax payers are tax deductible. Corporate and government support for our work would also be welcome.

**Donate now:** <http://ohpi.org.au/donate/>

## The Authors

### Dr Andre Oboler

Dr Oboler is CEO of the Online Hate Prevention Institute and a Senior Lecturer in Cyber Security in the Law School at La Trobe University. He has worked at the leading edge of international efforts to combat online hate and extremism since 2004. His work on online manifestations of antisemitism, Islamophobia and racism against Indigenous Australians, as well as his development and implementation of tools and methodologies for monitoring online hate, are internationally recognised.

Dr Oboler served as a co-chair of the Global Forum to Combat Antisemitism and co-led it's working group on antisemitism on the Internet and in the Media from 2008 to 2017. Since 2015 he has served as an expert member of the Australian Government's delegation to the International Holocaust Remembrance Alliance. Dr Oboler has also served as an expert to the Inter-Parliamentary Coalition to Combat Antisemitism and as a Distinguished Visitor for the IEEE Computer Society.

Dr Oboler holds a PhD in Computer Science from Lancaster University (UK) and a Juris Doctor from Monash University (Australia). He has also completed a Post-Doctoral Fellowship at Bar-Ilan University (Israel). He is a Senior Member of the IEEE and a member of the IEEE Computer Society and the IEEE Society for the Social Implications of Technology.

### **Dr Patrick Scolyer-Gray**

Dr Patrick Scolyer-Gray is an OHPI Research Fellow and a Research Fellow in Cyber Security and Decision Making at Deakin University's Centre for Cyber Security Research and Innovation (CSRI). Patrick brings a distinctively social scientific approach to his work in his research focus areas of protective security and information warfare.

Patrick received his PhD in 2019 for research into the notorious and fully anonymous online forum 4chan. His work tends to take a mixed-methods research approach, often integrating immersive ethnographic techniques, and focusses on topics such as deception, media manipulation, cyberwarfare, social engineering, and information warfare.

Patrick holds a Bachelor of Arts (Honours) degree in sociology and anthropology and a PhD in Sociology from La Trobe University. He is a member of the Australian Information Security Association and the Australian Sociological Association.

### **William Allington**

William Allington is an OHPI Research Fellow and a PhD candidate with the Department of Hebrew, Biblical and Jewish Studies at the University of Sydney. He is in the final stages of his PhD thesis on the topic of antisemitism online. His PhD research examines how the internet has qualitatively changed antisemitism and how young people react to encountering antisemitic material in online spaces. His honours thesis is focused on the transition of Holocaust denial to the internet.

He is the twice recipient of the John Rector Scholarship in Jewish studies and the 2018 runner up for the University of Sydney 3 Minute Thesis competition. William's research on Holocaust denial has been published as "Holocaust Denial Online: The Rise of Pseudo-Academic Antisemitism on the Early Internet", in the Journal of Contemporary Antisemitism. In addition to his studies, William has performed interactive learning sessions about Holocaust denial at schools in Sydney, NSW where he poses as a Holocaust denier to simulate the experience of encountering Holocaust denial in person, and then leads students through strategies to combat Holocaust denial. William holds a BA (Hons) in Jewish Studies.

## **Acknowledgements**

The authors thank the LawTech group at La Trobe University for a meeting in which the recommendations in this report were workshopped. The report was shared in draft form with a wide range of experts and stakeholders for feedback and comment prior to its public release. This provided academic peer review, industry consultation, government consultation and community consultation all of which have enhanced the final report. We thank all those involved in the review for their efforts.

OHPI thanks our donors for their assistance in making work like this possible. We would also like to acknowledge the support we receive from our professional advisers Logicca Chartered Accountants and Frankel Lawyers. Andre Oboler thanks the Directors of OHPI for the important role they play, as volunteers, in overseeing and helping to develop this important charity.

## Statements on this Report from Stakeholders and Experts

### **Katherina Von Schnurbein, European Commission Coordinator on Combatting Antisemitism**

“Halle showed us that radicalisation online leads to murder in the real world. Be it Pittsburgh or Poway, El Paso or Christchurch or a medium-sized town in the centre of Germany. The way to radicalisation is paved with antisemitic conspiracies labelling Jewish communities as the sources of evil, oppression and domination... I thank the Online Hate Prevention Institute (OHPI) for bringing together this valuable study and the useful recommendations. Only by better studying the phenomenon we are able to fight back.”

### **Chin Tan, Race Discrimination Commissioner, Australian Human Rights Commission:**

“The recent report of the Online Hate Prevention Institute, *Hate and Violent Extremism from an Online Sub-Culture*, is sobering and troubling reading. The report makes an important contribution to on-going work to identify, address and combat the role of online hate in terrorist acts. This research carefully outlines the connection between online hate and acts of terrorism in places of worship. Protecting the right of all people to safely and freely practice their religion remains an enduring challenge. The impact of online hate on this right is an area of major focus for me as Race Discrimination Commissioner. I commend OHPI’s focus on practical measures to meet the challenge of online hate and encourage positive action to progress their implementation.”

### **Julie Nathan, Research Director, Executive Council of Australian Jewry:**

"The OHPI report on Halle is much more than an account of the attack on a synagogue in Germany and the murder of bystanders. The report is composed of information that has been thoroughly researched and is comprehensive in its coverage and details of murderous attacks that have occurred in 2019 in the USA, NZ and Germany. The report also highlights the online origin of the attackers, and how sections of the online world are conveyor belts which encouraged the murderous attacks that occurred in 2019. Importantly, the report includes many recommendations to tackle online hate propaganda and methods to minimise the influence and scope of the attackers and their online manifestos and videos. "

### **Prof. Megan Squire, Dept. of Computer Science, Elon University:**

“I commend the Online Hate Prevention Institute for its recent report on the Halle shooting in October 2019. Anti-Semitism is unfortunately flourishing online, as are other types of hate and bias. Real-world violent incidents such as the Halle shooting are the natural outgrowth of a social media landscape that is completely overrun with hateful, violent rhetoric. This report smartly connects the dots between the recent rise in authoritarian, nativist views worldwide and the concurrent intensification of a toxic online culture that thrives on and perpetuates disinformation, hate, and violence. The recommendations in the report are clear and concise. Governments, social media companies, and civil society groups would do well to take the recommendations to heart and redouble their efforts to implement as many as possible.”

**Associate Professor Greg Adamson, University of Melbourne & former president of the IEEE Society on the Social Implications of Technology:**

“Hate speech in the online world teaches us once again that humans must take responsibility for the way we use technology. Drawing a line between freedom of speech and incitement to violence is one of the greatest challenges of the Internet. For some years now the Online Hate Prevention Institute has been a leading voice in examining and addressing this balance. I commend the authors for this effort, and encourage you to read it and consider its recommendations.”

**Maria Sirbu, VP of Business Development, Voxility:**

"The Online Hate Prevention Institute's report is comprehensive and very well documented. The important points are analyzed and discussed. We congratulate the Institute on this work and hope to see more initiatives like this one from civil society as well as real measures by Internet authorities to address the identified threats”

**David Matas, Honorary Senior Counsel to B'nai Brith Canada**

“A sequence of armed attacks in the United States, New Zealand, and Germany has highlighted the rise of a new form of internet spread terrorism. The report by the Online Hate Prevention Institute is a cutting edge look at this threat, which tells us not only the danger it poses but also how to counter it. The report is a wake-up call, an insightful analysis, and a thorough presentation of available remedies. Understanding and combating the threat of online hate and terrorism requires an understanding of both the internet and incitement to hatred and terrorism. The Online Hate Prevention Institute has the welcome and unusual ability to address both together in a meaningful and convincing way.”

**Prof. Louis de Koker, La Trobe LawTech, La Trobe Law School:**

“The linkages between online extremism and terrorism narrowed in 2019, resulting in four terrorist attacks that authorities were unable to prevent. The 2019 attacks were designed to inspire like-minded people to plan further incidents. Many more people will be exposed to violence if our governments and the service providers fail to collaborate. Governments also need to enlist the assistance of netizens to combat online extremism more effectively. The Online Hate Prevention Institute is commended for its report on hate and violent extremism from an online sub-culture. This report is a good example of the contribution that civil society can make to inform government policy regarding the detection of and response to online extremism. This report does however more: It arms readers with information and insights about online extremism that they can use to monitor their own online fora for indications of concern. The report contains a number of recommendations that requires serious consideration by governments, regulators, service providers and civil society.”

**Thilo Troschke, Chair, Council of Christians and Jews (Victoria):**

“It seems that there is absolutely no end to online hate as new major incidents of killings worldwide, sparked by deranged, deluded and twisted minds expressing themselves through online hate speech, appear in the news virtually on a weekly basis. All the more is it important to single out these incidents and educate as many people as possible about the reasons and consequences of such online hate. To this end the report on “Hate and Violent Extremism from an Online Sub-Culture: The Yom Kippur Terrorist Attack in Halle, Germany” by the Online Hate Prevention Institute must be commended for its extremely thorough research and comprehensive coverage of this subject matter. The numerous and very detailed recommendations contained in the report provide a road map to dealing with the insidious epidemic of online hate. Bit by bit these recommendations must be taken up by government as well as by private organisations to make significant inroads towards the elimination of hate in our communities. The Council of Christians and Jews of Victoria has proudly partnered with the Online Hate Prevention Institute to roll out a Tackling Hate Speech Program in 2020 to Christian and Jewish congregations to enable them to call out, and actively tackle, online hate. The above report demonstrates the great capability of the Online Hate Prevention Institute to deal with these issues.”

**Nikki Marczak, Atrocity Prevention Coordinator, Asia Pacific Centre for the Responsibility to Protect:**

“This report tackles a new and especially egregious form of extremism that combines online hate speech with real world violence, targeted against particular groups. As a scholar of atrocity crimes, it is clear that the internet forums discussed in the report are allowing for the spread of hatred against groups of people because of who they are, and inciting violence and murder. While the report explores individuals who committed violence linked to online hate speech, this is also occurring at a macro level, with internet incitement fuelling the flames of genocide. The report effectively highlights the problem and offers achievable recommendations.”

**Dr Hiruy Gebreegziabher and Maya Borom, Leads for the Global Research Network Think Tank Programme in Crime & Terrorism, UK:**

“This comprehensive report provides an excellent description of an online subculture which is facilitating hate crimes and violent extremism. Instead of generalised labelling of social media sites, which are obviously manifestations of individual freedom and privacy, the report focuses on clearly identified “online subcultures” which is facilitating terrorist crimes inspired by hate and extremism beyond the capacity of legitimate counter-terrorism surveillance. The technical recommendations regarding the various digital platforms that can facilitate hate and violent extremism are sufficient to work towards identification, reporting and appropriate management of content. The report also identifies positive obligations on relevant governmental, NGOs and other interested parties working in this space to provide clear mechanisms that can be utilised to stop the spread of hate speech and violent extremism. Great work.”

**Prof. Gail Mason, Sydney Law School, The University of Sydney**

“This report by the Online Hate Prevention Institute is an outstanding achievement. Despite the burgeoning and ongoing expression of inter-group hatred on the internet and other digital media, we still do not know anywhere near as much as we need to about the links between online hate and acts of violent extremism. This report makes an invaluable contribution to our knowledge of online subcultures and how best to tackle the hatred they promote.”

**Prof. Raphael Cohen-Almagor, Department of Politics, University of Hull**

“I have read Dr Oboler’s extensive report with great interest. The report is very thorough and important. Hate and terrorism are of significant concern worldwide. Increasingly, the relationships between hate speech, hate crime and terror is becoming very clear... Indeed, what is important in this report is that Dr Oboler makes concrete recommendations for action. I agree with him that 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 hate and terror that have become a significant threat to our globalised societies... More than 25 years after the Internet entered its mass commercial phase, we can now conclude that self-regulation does not work. Self-regulation does not work when offline media is concerned, and it is certainly failing online. Governments must step in and enforce cohesive and protective rules of conduct to prevent harm, protect vulnerable populations and save life. Now that we have learned the hard way the consequences of having a powerful free highway of technology, I join Dr Oboler in thinking it is time for change.”

## Summary of Recommendations

The following sections summarise recommendations that appear with background explanation and context throughout this report.

### Recommendations to Create a Partnership Between Industry and Government

Number	Page	Recommendation
20	57	Serious hate speech, that which makes threats of violence or incites either violence or hatred, should be immediately reported to authorities. Other forms of hate speech should be removed by the platform, but a log of the incident including the user's account and IP address should be recorded. Users should be informed when a platform takes action against them and should be warned repeated breaches could lead to a report being made to authorities. Where platform sanctions prove ineffective at altering behaviour, the history of breaches and IP address of the user should be referred to authorities.
21	58	Once a user has been referred to authorities by a platform, a summary of any further hate speech incidents involving that user on that platform should be notified to authorities periodically (for example monthly) by the platform.
22	58	Once a user has been referred to authorities, the authorities should seek to convert the IP address into details of the account holder and add it to the record. Where the account holder is a company, the company should be notified with a request to identify the specific user.
23	58	Where a company cannot provide information on the person who committed a breach of the law against serious or repeated hate speech, assistance should be provided. Where a company will not provide information on the person who committed a breach of the law against serious or repeated hate speech, the company itself should be liable to corporate fines.
24	58	Users referred to authorities by platforms for repeated breaches that do not involve incitement to hate or violence should initially be issued a warning, potentially after a discussion with authorities centering around user actions. Further breaches should lead to escalating fines. If fines fail to provide a deterrent, more serious measures including imprisonment should be available.
25	58	Legal exemptions should be provided for researchers from government agencies and departments, academia and civil society engaged in testing the effectiveness of both platform and government agency responses. Such exemptions may require prior approval of the research by one or more authorised people or agencies who are independent of the enforcement system.

### Recommendations for Content Services

Number	Page	Recommendation
3	27	All services that allow users to upload or post content should have clearly visible mechanisms for reporting to the service provider any content that violates the terms of such services.
19	56	All companies that allow hosting of user generated content should have a process to receive reports from the public related to material promoting terrorism and this process should ensure rapid review.

4	27	All services that allow users to upload or post content should allow content to be reported anonymously to the service provider and by anyone who can see the content. If content is visible without having an account, then it should be reportable without having an account.
5	27	To assisting with lawful counter terrorism investigations, all services that allow users to upload or post content should maintain logs for at least 24 hours. Where a user reports content, log details related to the original uploader / poster of that content should be maintained for a further period of at least 7 days.
7	30	Livestreaming and video hosting sites should provide reporting options that allow the rapid identification, and a priority response, to reports of actual violence, extremism or unfolding crime.
8	30	Platforms should publish their target response time for reviewing and responding to reports of content flagged by users as potential violent extremist content or whichever broader category the platform chooses which includes violent extremist content. Platforms should also publish their average response time to reports in this category on a regular, e.g. monthly, basis.
11	47	When a violent extremist attack is livestreamed the platform that was used to stream the incident and / or host the initial video of the incident should provide transparency on exactly when the livestream and/or video was first reported to them and when exactly they acted to remove it.
12	47	Platforms should take all reasonable steps to facilitate and encourage the reporting of material depicting and promoting violent extremism, as well as all other reasonable steps to identify such material themselves. They should expeditiously remove such material once they become aware of it. Provided the above steps are taken, there should be a clear safe harbour, protecting platforms from liability for material they are unaware they are hosting.
37	109	Hosting services that do not outright prohibit the use of their services to incite hate, should at a minimum ensure they do not serve content inciting hate to users in countries where such incitement is unlawful.

We additionally make the following recommendation, but flag it as particularly controversial:

36	109	Content services should create mechanisms that enable them to restrict access to specific content on their service for users from countries where that content is illegal. This will ensure content services have the technical capacity to respect national sovereignty and comply with national laws. There may be circumstances where a content service refuses to comply with national laws, for example, if the national laws conflict with customary international law, international treaties to protect human rights, or legal obligations in the content services own jurisdiction.
----	-----	--

This goes to the question of state sovereignty and the role of Internet technology as a disrupter. Foreign interference that undermines a government's power or control is justifiable in circumstances where the power is being used contrary to universal human rights. Other cases are more controversial as they may advance the interests of some states against the interests of others. Questions of cyber dissidents, whistle blowers and Smart Power come in to play. A general discussion can be seen in Section 1.2.



## Recommendations for Suppliers to Content Services

Number	Page	Recommendation
1	25	Where an image board is hosted in a country and the site, or a board within it, actively promotes hate speech which is unlawful in that country, the hosting provider once it is aware of this, should take action to terminate the hosting.
2	25	Where a domain name is registered in a country, and the owner actively uses the site at that domain for the purpose of promoting hate speech which is unlawful in that country, the domain name should be terminated by the domain name registrar.
32	105	Decisions by technology companies not to do business with a site should be such that a change to the ownership, brand, domain name or IP address will not circumvent the ban.
34	105	All companies providing Internet infrastructure should have clear terms of service which prohibit the use of their service for inciting hate or violence. They should also give notice that the service may be terminated without notice for serious breaches of this rule. Companies may further wish to require that any customer they provide a service to, includes a similar statement in its terms of service.

## Recommendations for Law Makers

Number	Page	Recommendation
6	28	Laws and policies designed to prevent the spread of extremist material need to be flexible enough to cover content consisting of a link which directly or indirectly will lead to the material.
38	109	Governments should consider law reforms to create a system of sanctions that could be imposed on companies outside their jurisdiction who, after suitable notice, continue to provide unlawful content inciting hatred or violent extremism to users in that country, in breach of the country's law. Such law reform could also create sanctions that impose penalties for any company within the country's jurisdiction who engage in business with a company on the sanctions list.

## Recommendations for Executive Government

Number	Page	Recommendation
35	107	Governments continue to contribute to the costs of security for Jewish communal institutions and provide additional support at times of increased risk such as during Yom Kippur.
33	105	Decisions by governments to restrict access to a site should be robust enough that a change to the ownership, brand, domain name or IP address of the banned site will not circumvent the restriction. Government may need to monitor and update identification details to enforce such restrictions.

## Recommendations for Civil Society

Number	Page	Recommendation
--------	------	----------------

18	56	Civil society organisations should redact or avoid naming hosting services that are making terrorist content available, but should confidentially report such content to key stakeholders in government, industry and civil society.
9	33	Those responding to antisemitic manifestations and incidents should make use of the International Holocaust Remembrance Alliance's <i>Working Definition of Antisemitism</i> .

### Recommendations for Australia

Number	Page	Recommendation
10	33	Australia should join with other IHRA member countries in formally adopting the International Holocaust Remembrance Alliance's <i>Working Definition of Antisemitism</i> for domestic use.
26	63	The eSafety Commissioner should refer all unclassified Abhorrent Violent Material for classification by the Classification Board. This should become a standard part of the process when new Abhorrent Violent Material is identified.
27	63	The eSafety Commissioner should refer to the Classification Board for classification the manifesto documents from the terrorist attacks in Halle, Poway and El Paso as was done in the case of Christchurch.
28	63	The eSafety Commissioner should announce when terrorist related material that has a risk of going viral has been given an RC rating and should advise the public to report any online copies to the eSafety Commissioner and not to share it.
29	63	In Australia, consideration should be given to creating a civil penalty regime for sharing material classified RC that promotes terrorism. Suitable exemptions should apply for those acting reasonably and in good faith for the purpose of journalism, scientific research or law enforcement.
30	63	The Classification Board should restore the previous tool that allowed more detailed interrogation of Classification Board decisions, specifically, it should allow all decisions in a given period for a particular classification, to be listed.
31	63	The Classification Board should ensure either the title or a useful description is provided for material which is given an RC classification. This is necessary as the public cannot comply with a ban if the banned content cannot be identified.

### Recommendations for Specific Companies or Organisations

Number	Page	Recommendation
14	53	Google should commit to supporting the "Christchurch Call" across all parts of the business without exception. This includes preventing Google's search engine being used to access material promoting terrorism.
15	55	Through the Global Internet Forum to Counter Terrorism (GIFCT), technology companies should provide a contact mechanism that is staffed 24/7 and available to assist any platform whose technology is abused to share manifestos or live streaming.
16	56	Access to the <i>Terrorist Content Analytics Platform</i> should be available to researchers after they are vetted, to ensure they represent legitimate research efforts in government, academia or civil society.

17	56	The <i>Terrorist Content Analytics Platform</i> or a similar service should offer a tool for archiving and preserving online content for use by law enforcement and in legal proceedings. Adding content should be available to the public, but accessing archived content should be restricted to vetted people from government, academia and civil society.
13	51	Telegram should join GIFCT and implement a system to remove videos from its platform which are registered in the GIFCT Hashing database.

### Recommendations for the Public

Number	Page	Recommendation
39	113	The public are urged not to share content from terrorist attacks such as manifestos or videos. If seen, this content should be reported to the relevant authorities, in Australia this being the eSafety Commissioner.

# Contents

Foreword.....	i
Executive Summary.....	ii
The Online Hate Prevention Institute and Report Authors .....	iv
Statements on this Report from Stakeholders and Experts .....	vi
Summary of Recommendations.....	x
1 Introduction .....	1
1.1 Violent Extremism from a Toxic Online Culture .....	1
1.2 Internet Regulation .....	3
1.2.1 Origins of the Internet and Its Inherent Resistance to Regulation .....	4
1.2.2 The Death of Internet Exceptionalism .....	6
1.2.3 Assertions of Sovereignty and the Shift to Government Regulation .....	8
1.2.4 Doctrinal Principles of Internet Regulation.....	10
1.3 Hate Speech and Incitement.....	11
2 The Halle Attack .....	14
2.1 The Attacker.....	15
2.2 The Post Announcing the Attack.....	15
2.3 The Manifesto .....	16
2.3.1 マニフェスト.....	16
2.3.2 Read This First .....	18
2.3.3 DoKumentation .....	20
2.4 Technology the Attacker Used.....	23
2.4.1 The Announcement: Meguca.org .....	24
2.4.2 The first Document Hosting Service: anonfile.com .....	25
2.4.3 The second Document Hosting Service: The Dark Web.....	27
2.4.4 The Live Streaming and Video Hosting Service: Twitch .....	29
3 Antisemitism in the Halle Attack.....	30
3.1 The IHRA Working Definition of Antisemitism.....	31
3.2 Manifestations of Antisemitic in the Halle Attack .....	33
3.2.1 The objective, location and timing of the attack .....	33
3.2.2 Racial slurs.....	34
3.2.3 The Greedy Jew trope .....	35

3.2.4	Holocaust denial.....	36
3.2.5	The ZOG Conspiracy Theory.....	38
3.2.6	Redemptive Antisemitic Worldview .....	39
4	Responses to the Halle Attack .....	40
4.1	/pol/ and the Image Boards .....	40
4.1.1	Use of /pol/ to Spread the Manifesto and Video.....	40
4.2	/pol/ Fake News and Trolling .....	42
4.3	Misidentification of Kohlchan .....	44
4.4	Response from the Technology sector .....	45
4.4.1	Twitch.....	46
4.4.2	Telegram .....	49
4.4.3	Google .....	51
4.4.4	GIFCT's Responsive Action .....	53
4.4.5	The Tech Sectors Response in General .....	55
4.5	Government Action.....	56
4.5.1	Germany.....	56
4.5.2	Australia .....	58
4.6	Civil Society Action: Online Hate Prevention Institute .....	63
5	A Culture Leading to Violent Extremism: The Image Boards and /pol/ .....	64
5.1	Image Board Origins.....	64
5.2	The Rise of 4chan.....	70
5.3	/pol/ the “Politically Incorrect” Board and its Evolving Antisemitism.....	71
5.3.1	Antisemitic Alterations to Ben Garrison Cartoons.....	73
5.3.2	The Antisemitism Meme of the Jew .....	75
5.3.3	A shift in /pol/’s antisemitism.....	77
5.4	Gamergate and the Rise of 8chan.....	83
5.5	Harnessing the Culture for Real Politics: The Rise of the Alt-Right .....	86
5.5.1	Political origins .....	86
5.5.2	Harnessing the Online Subculture .....	87
5.5.3	Campaigning for Trump .....	87
5.5.4	Implosion.....	94
5.6	Terrorism on 8chan’s /pol/ .....	96
5.6.1	Christchurch.....	97

5.6.2	Poway .....	98
5.6.3	El Paso, the closure of 8Chan and the Congressional Inquiry.....	101
5.6.4	Return as 8kun .....	104
6	Responding to the Online Sub-Culture of Hate and Violent Extremism.....	105
6.1	Hardening Targets to Reduce Antisemitic Attacks.....	105
6.2	Taking Down the Online Infrastructure of Extremism .....	107
6.2.1	Lessons from Cloudflare’s termination of 8chan .....	108
6.2.2	The broader campaign to disconnect 8chan.....	109
6.3	Tackling the toxic culture .....	112
6.4	Future Work.....	113

# 1 Introduction

## 1.1 Violent Extremism from a Toxic Online Culture

In 2019 we saw the rise of a new form of violent extremism. It manifests as deadly violence that targets minorities in the real world, but it is the result of a particularly toxic sub-culture of hate created on the Internet, spread via the Internet and whose manifestations are designed for its own Internet based audience. This is not the story of online hate in general but a dossier on the hate and violence of one specific online community.

The attack on the synagogue in Halle was the fourth in a series of similar attacks. The first was an attack during Friday prayers on two mosques in Christchurch, New Zealand.<sup>1</sup> The second was an attack on a synagogue in Poway, near San Diego in the United States.<sup>2</sup> The third attack in a Walmart car park in El Paso, Texas in the United States, during which immigrants, specifically Mexicans and Hispanics more generally, were the primary target.<sup>3</sup> This most recent attack in Halle was aimed primarily at the Jewish community, was planned at a time and location to maximise Jewish casualties, but women, Muslims, Christians, Communists, people of colour, police officers and “traitors” were also on the list of targets.

Though attacking a range of different targets, there is a direct connection between the attacks. The Poway attacker’s manifesto makes direct reference to Brenton Tarrant, the individual who carried out the attack in Christchurch. The Poway attacker writes in his manifesto that he “scorched a mosque in Escondido with gasoline a week after Brenton Tarrant’s sacrifice” and that he spray painted “For Brenton Tarrant -t. /pol/” in the mosque’s parking lot. He continues, “Tarrant was a catalyst for me personally. He showed me that it could be done.” The El Paso attacker’s manifesto also references the Christchurch attack opening with, “In general, I support the Christchurch shooter and his manifesto”. The Halle attack does not make a direct reference to the previous attacks but comes from the same online community and follows the same approach taken by the previous attackers.

The four attacks are examples of violent extremism resulting from online self-radicalisation. This is made explicit in the Christchurch manifesto, in which the author writes, “From where did you receive/research/develop your beliefs? The internet, of course. You will not find the truth anywhere else.” This is, of course, an oversimplification. It was not simply a matter of searching the Internet which radicalised these individuals, but rather the experience of becoming embedded within a toxic and fully anonymous online community.

That community, originally created on 4chan, is spread across a range of sites and platforms. It is a culture which has coordinated significant cyberbullying and harassment campaigns, encouraged people to commit suicide while streaming live, and which calls for race wars and genocide. What started as a culture of irony designed to shock new visitors and celebrate freedom of speech online, gradually

---

<sup>1</sup> Andre Oboler, 2019. *New Zealand Terrorist Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/new-zealand-terrorist-attack/>, accessed 12 December 2019.

<sup>2</sup> Andre Oboler, 2019. *San Diego Synagogue Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/san-diego-synagogue-attack/>, accessed 12 December 2019.

<sup>3</sup> Queenie Wong & Richard Nieva, “El Paso massacre shines light on 8chan, a racist troll haven”, *CNET*, at <https://www.cnet.com/news/el-paso-shooting-shines-light-on-8chan-a-racist-troll-haven/>, accessed 12 December 2019.

shifted to the serious promotion of hate, incitement to violence and an ideology of right-wing extremism. It has become a culture where the response to a post announcing an intended terrorist attack is to wish the poster luck and a “high score”, that is, a higher number of casualties.

Readily available equipment and online services have been used to livestreaming and then share videos of the attacks. The approach, first used in the Christchurch attack, is modelled on online gaming, particularly first-person shooters. It allows others to participate by either watching live or viewing and sharing videos of the attack once it concludes. This glorifies the attacker and gives them an audience for their “achievement”. The Halle attacker took this one step further with a page in the manifesto listing a range of game like “achievements” including “Chosen to die”, where the goal was to “Kill a jew” [sic], “Think of the children!” where the goal was to “Kill a kikelett” (a pejorative label created in this sub-culture for a Jewish child), “Cultural Appropriation”, where the goal was to “Stab a muslim” [sic] and “Crossed out”, where the goal was to “Kill a Christian” [sic].

The attacks were all announced on image boards. The first three on the “politically incorrect” board /pol/ on 8chan. 8chan has since been forced offline and the Halle attack was announced on an image board called Meguca.org. They contain messages directed to those they see as their compatriots within this culture of hate. The attacker in Halle wrote in a document pointing to his livestream “Thank you for all the good time anon” and referenced 8chan specifically. The El Paso attacker posted on 8Chan referring to the readers as “brothers”. The Poway post begins, “It’s been real dudes. From the bottom of my heart thank you for everything. Keep up the infographic redpill threads”. The Poway manifesto says, “To the true anons out there (you know who you are). You are the product of /pol/—the product of unadulterated truth. You are my brothers and the best dudes out there”. The Christchurch post describes members of this sub-culture as “top blokes and the best bunch of cobbles a man could ask for” and begins with the words, “Well lads, it’s time to stop shitposting and time to make a real life effort post”.<sup>4</sup> The attacks, with their livestream feeds promoted to the online community in /pol/ were seen by the attackers as a continuation of the online discussion, an ultimate contribution to a discussion with calls to be ever more hateful and more extreme.

The actions of the attacker were not meant to end the discussion, but to keep it going. The Christchurch post called on the online community to “do your part by spreading my message, making memes and shitposting as you usually do”. The Halle post called for a copy of the manifesto accessed through the Dark Web to be seeded, a call for those who download it to keep their clients open and host copies so others can more readily access it. The Poway post includes a list of songs the attacker planned to play, provided “in case they take down my livestream too soon”, which he describes as “very meme-able songs” saying “you should have no problem”. This is an indirect call to make and spread memes about the attack. In the last line of his post he declares “Meme magic is real” reinforcing this.

The manifestos posted along with the live streams sought to incite further attacks. The Christchurch manifesto gave as one reason for the attack, “To show the effect of direct action, lighting a path forward for those that wish to follow”. It also encouraged readers to “Make your plans, get training, form alliances, get equipped and then act” and to remove any doubt it adds, “the time for a political solution has long since passed” making it clear this is a call to use violence for a political purpose – the definition

---

<sup>4</sup> Andre Oboler, 2019. *New Zealand Terrorist Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/new-zealand-terrorist-attack/>, accessed 12 December 2019.



of terrorism. The Poway manifesto says “I have complete trust and certainty that all of you after reading this will begin planning your attack on the enemy—and you’ll attack again, and again, and again—until either we win, or we die. I know you will do this because you’re true anons.” The Halle manifesto directly called on readers to kill Jews, Muslims, Christians, Communists, people of colour and traitors. The last page of one of the documents jokingly offers a free cat-girl to those that become a “techno-barbarian” and in the fine print adds “You need to kill at least one jew to qualify”.

It is not just the attackers themselves. The first comment after the post about Poway reads “Based. Get the high score.” That form of encouragement to someone about to carry out an attack may reinforce their conviction that there is a crowd of supporters and that mass murder is seen as acceptable by the community they have identified with. That message is also seen by others, reinforcing the attackers call for further attacks and making it appear like there is a silent majority backing that call. This is a toxic subculture with the capacity to self-perpetuate its own growth: It is extremism that justifies, validates and supports itself in its efforts to incite further terrorism.

There have been other deadly terrorist attacks in 2019 which are not from this particular online culture. The attack on three Churches in Sri Lanka on Easter Sunday and the attack on the Tree of Life Synagogue in Pittsburgh to name just two. While we mourn all those needlessly lost to acts of terrorism, this report focuses specifically those connected to the /pol/ community. After four attacks so far, and with little reason why there would not be more, this community must be recognised as a specific threat. Given its technical and ideological features and the methods of its attackers, it is best recognised as a new form of terrorism and one which will need new solutions if it is to be stopped.

In this report, we begin with a focus on the attack in Halle, Germany. As in our past work, we will briefly outline the incident then examine the online post announcing the attack, the manifesto accompanying the attack, the technology used, the online response and the reaction of those responding to the attack and seeking to contain it. This will be followed by an in-depth discussion of the antisemitism present in attack and a more detailed discussion of the online community which has led to this extremism. Throughout the report we will provide recommendations for key stakeholders to help prevent the growth of such extremism in the future and to improve responses when incidents do occur.

## 1.2 Internet Regulation

In this report we advocate for greater cooperation between governments, technology companies and civil society. Within the context of this cooperation we believe technology platforms, with input from civil society, may choose to be proactive in removing harmful content. While the law in a particular country may not recognise a certain group as deserving of protection from hate speech, a technology platform could adopt a global position in its community standards that, nevertheless, provides such protection within the confines of that platform even in countries where there is no legal protection.

More controversially we argue that the law is the ultimate backstop and, with a few exceptions, companies that impact the people within a particular country’s borders should respect the laws of that country. That is, if the law grants a particular group protection from hate speech, a technology platform should take action to prevent hate speech against that group from appearing to people in that country. We reject the idea that a platform could hold its community standards above the law when the two come into conflict. We also reject the idea that a platform could choose a jurisdiction and conform only to the laws of that jurisdiction, while ignoring the laws in the countries where its audience is based.

There are of course exceptions. There may be circumstances where a content service provider is unable to support compliance with national laws, for example, where such support would contravene laws or breach legal obligations in the content service provider's own jurisdiction. National laws may also infringe upon rights recognised in the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights or similar international, regional or national instruments. Infringement in this case does not mean they stroke a different permissible balance, for example between free speech and hate speech, but rather that they are entirely incompatible with such international instruments. Such exceptions should be rare, and states may well respond by seeking to block access to the platforms concerned within their territory.

It is our view that outside of exceptional circumstances, the rule of law and recognition of the sovereignty of nations requires platforms to conform to the law of the places where their audience resides. This concept is today widely accepted by major platforms, though it is implemented to varying degrees of effectiveness. The problem, which is directly relevant to this report, is how countries should handle platforms who work around their laws, for example, platforms that provide a forum for Germans to illegally glorify Nazism, or New Zealanders or Australians to access the Christchurch shooting video which both countries have declared prohibited content. Such sites may claim the continue a long history of online opposition to regulation, but they are problematic in the context of today. States may legitimately block such platforms as a last resort.

Ideally what we recommend later in this report, at Recommendation 35, is that:

Content services should create mechanisms that enable them to restrict access to specific content on their service for users from countries where that content is illegal. This will ensure content services have the technical capacity to respect national sovereignty and comply with national laws. There may be exceptional circumstances where a content service refuses to comply with national laws, for example, if the national laws conflict with customary international law, international treaties to protect human rights, or legal obligations in the content services own jurisdiction.

Given the controversial nature of this recommendation we provide in the following sections (1.2.1 to 1.2.4) a detailed background discussion which leads to this position.

### 1.2.1 Origins of the Internet and Its Inherent Resistance to Regulation

The early Internet grew out of ARPANET, the network of the Advanced Research Projects Agency (ARPA) established as part of the US Department of Defence to engage in blue sky research with potential military applications.<sup>5</sup> The system, which was essentially completed in 1972,<sup>6</sup> was both designed and used by high-profile researchers working in elite institutions.<sup>7</sup> There was a collaborative ethos by those building the system and a strong demands for modifications and innovation which went beyond the intended purpose of the system.<sup>8</sup> Responsibility for the network was transferred to the Defense

---

<sup>5</sup> John Naughton, 2016. "The evolution of the Internet: from military experiment to General Purpose Technology", *Journal of Cyber Policy*, volume 1, number 1, pp. 5-28, p. 7.

<sup>6</sup> Ibid 8.

<sup>7</sup> Ibid.

<sup>8</sup> Ibid 9.

Communications Agency in 1975, and in 1983 the agency split the system creating MILNET for military communications while ARPANET would continue to support research.<sup>9</sup>

The shift in control back to universities and research institutions and was “an essential first step towards achieving ARPA’s goal of transferring the network to civilian control”.<sup>10</sup> Access to ARPANET was limited to certain institutions and which was seen as “increasingly perceived as irritating and dysfunctional” by those in the developing field of Computer Science.<sup>11</sup> This led to the creation of the Computer Science Network (CSNET) in the early 1980s by US National Science Foundation (NSF) and its infrastructure eventually became the backbone to ARPANET as well.<sup>12</sup> Commercial use of the network was prohibited under National Science Foundation’s ‘acceptable use’ policy.<sup>13</sup>

By 1994 the National Science Foundation decided the network needed to be privatised in order to allow commercial exploitation.<sup>14</sup> In privatising the network, the decision was made to have many smaller companies, Internet Service Providers, cooperate in running the backbone rather than entrusting the system as a whole to a major technology or telecommunications company.<sup>15</sup> The emerging technology and culture developed in a manner that deliberately sought to resist centralised control and government control in particular.

The Internet had finally, after significant effort, broken away from the restrictive control that had been applied by various parts of government. The early commercial Internet was “essentially a geek preserve, with a social ethos that was communal, libertarian, collaborative, occasionally raucous, anti-establishment and rich in debate and discussion”.<sup>16</sup> The ethos of the early Internet is best displayed in “A Declaration of the Independence of Cyberspace” posted by John Perry Barlow on February 8<sup>th</sup>, 1996:

---

*“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather... You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.”<sup>17</sup>*

---

This 1990s view sees the Internet as having an “exceptional” nature which made it not susceptible to regulation by the laws of nation states.<sup>18</sup> Some legal scholars went as far as to argue that the Internet

---

<sup>9</sup> Ibid 10.

<sup>10</sup> Ibid 11.

<sup>11</sup> Ibid 11.

<sup>12</sup> Ibid.

<sup>13</sup> Ibid.

<sup>14</sup> Ibid 12.

<sup>15</sup> Ibid.

<sup>16</sup> Ibid 12.

<sup>17</sup> John Perry Barlow, “A Declaration of the Independence of Cyberspace,” at <https://www.eff.org/cyberspace-independence>, accessed 18 December 2019.

<sup>18</sup> Jack Goldsmith and Tim Wu, 2006. *Who Controls the Internet: Illusions of a Borderless World*. New York: Oxford University Press, p. viii.

has its own sovereignty and should have its own laws that reflected its “special character”.<sup>19</sup> The view that the internet was something apart and needed protection from government regulation also gained ground in the courts. In *ACLU v Reno* (1996) US Federal Judge Stewart Dalzell wrote that, “[a]s the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion. ...The absence of governmental regulation of Internet content has unquestionably produced a kind of chaos, but as one of plaintiffs' experts put it with such resonance at the hearing: ‘What achieved success was the very chaos that the Internet is. The strength of the Internet is that chaos’”.<sup>20</sup>

### 1.2.2 The Death of Internet Exceptionalism

Jack Goldsmith and Tim Wu, writing in 2006, considered the 1990s perception of Internet exceptionalism in which “many believed that nations could not control the local effects of unwanted Internet communications that originated outside their borders, and thus could not enforce national laws related to speech, crime, copyright, and much more.”<sup>21</sup> Reflecting on the decade since 1996 which had “shown that national governments have an array of techniques for controlling offshore Internet communications, and thus enforcing their laws, by exercising coercion within their borders,” they rejected this view and warned of the death of Internet exceptionalism.<sup>22</sup>

Goldsmith and Wu predicted the internet would become bordered, splitting apart to conform to local conditions, including language, content and norms.<sup>23</sup> They predicted the Internet would “differ among nations and regions that are increasingly separated by walls of bandwidth, language and filters”, reflecting “top-down pressures from governments that are imposing national laws on the Internet within their borders” and “bottom-up pressures from individuals in different places who demand an Internet that corresponds to local preferences”, as well as by the efforts of technology companies to meet those demands.<sup>24</sup> While noting that many will “lament the death of the borderless Internet”, Goldsmith and Wu state that “the geographically bordered Internet has many underappreciated virtues”, including meeting the demands of the citizenry that governments prevent them from harming each another, and to protect them from harm from abroad.<sup>25</sup> They argue that the “bordered Internet accommodates real and important differences among people in different places, and makes the Internet a more effective and useful communications tool as a result”.<sup>26</sup>

Goldsmith and Wu note that as “governments increase their control, they replicate their vices on the Internet”.<sup>27</sup> They discuss China’s effort at political control and economic self-aggrandisement, but also

---

<sup>19</sup> David Post and David Johnson, 1996. “Law and Borders – The Rise of Law in Cyberspace,” *Stanford Law Review*, volume 48, pp. 1367-1402, Online at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=535](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535), accessed 18 December 2019, pp. 1400-1401.

<sup>20</sup> *American Civil Liberties Union v. Reno*, 929 F. Supp. 824, 883 (ED Pa. 1996), at <https://law.justia.com/cases/federal/district-courts/FSupp/929/824/1812782/>.

<sup>21</sup> Jack Goldsmith and Tim Wu, 2006. *Who Controls the Internet: Illusions of a Borderless World*. New York: Oxford University Press, p. viii.

<sup>22</sup> Ibid.

<sup>23</sup> Ibid.

<sup>24</sup> Ibid.

<sup>25</sup> Ibid.

<sup>26</sup> Ibid.

<sup>27</sup> Ibid.

the risk in democratic countries of “corruption and imperfections of the political process”.<sup>28</sup> These potential problems did not dissuade them from the view that “on the whole decentralized rule by nation-states reflects what most people want.”<sup>29</sup>

The shift to a “bordered Internet” was significantly slowed with the rise of Web 2.0 and social media. Those responsible for placing harmful content on the Internet no longer needed their own domain or physical servers. Their IP address and location would often be masked by the technology companies. The argument for shutting down a website when the owner was using it for harmful activities after refusing to desist or take remedial action was greatly weakened when it was not the site owner but instead the visitors to the site who engaged in harmful activities or uploaded harmful content. The idea of penalising the company and other users of the platform for actions of a small minority abusing the technology, for example, by taking down a service for non-compliance, was seen as a disproportionate response. Technology companies also argued they were incapable of taking effective action given the volume of content on their services, or that it would be prohibitively expensive, and that efforts to increase obligations on them would therefore stifle innovation.

Technology companies also sought to maintain a unified approach across their platforms. The bottom up pressure Goldsmith and Wu expected, where individuals would want the Internet to reflect their local preferences and companies would seek to meet this demand, was strongly resisted by the growing companies. This was most evident in Facebook’s resistance to banning Holocaust denial in spite of public calls for such measures, and even in countries where such content was illegal.<sup>30</sup> Their initial position was that country specific rules were not possible, though they later revised this position saying they would block access to content in countries where the content was illegal. As their spokesperson, Barry Schnitt, explained:<sup>31</sup>

---

*“When dealing with user generated content on global websites, there are occasions where content that is illegal in one country, is not (or may even be protected) in another. For example, homosexual content is illegal in some countries, but that does not mean it should be removed from Facebook. Most companies approach this issue by preventing certain content from being shown to users in the countries where it is illegal and that is our approach as well. We have recently begun to block content by IP [the “address” of a computer on the internet] in countries where that content is illegal, including Nazi-related and holocaust denial content in certain European countries.”*

---

---

<sup>28</sup> Ibid ix.

<sup>29</sup> Ibid.

<sup>30</sup> Andre Oboler, 2009. “Facebook, Holocaust Denial, and Anti-Semitism 2.0”, *JCPA: Post-Holocaust and Anti-Semitism*, August 2009. Online at <http://jcpa.org/article/facebook-holocaust-denial-and-anti-semitism-2-0/>, accessed 12 December 2019.

<sup>31</sup> Ibid.

This set the precedent,<sup>32</sup> and the same approach was used in blocking access to the ‘Everybody Draw Mohammed Day!’ Facebook page in Pakistan,<sup>33</sup> and in India.<sup>34</sup> The approach was, however, inconsistent in its application. While German hate speech laws saw refugees as a protected group, Facebook’s community standards, as they stood in 2015, did not.<sup>35</sup> The gap led to anti-immigrant content remaining online for weeks, or never being removed, much to the frustration of the German Government.<sup>36</sup> The online hate was linked by researchers to a rise in offline violence against refugees.<sup>37</sup> In February 2016 Facebook admitted it had made a mistake, Mark Zuckerberg apologised saying that, “learning more about German culture and German law has led us to change our approach” and refugees became a protected group on Facebook.<sup>38</sup>

### 1.2.3 Assertions of Sovereignty and the Shift to Government Regulation

Following the introduction of a voluntary agreement between major technology platforms and the German government, tests were carried out by the government to assess the level of compliance in removing hate speech reported by regular users.<sup>39</sup> The results were disappointing, with one test showing a 46% removal rate, and the other just 39%.<sup>40</sup> The German government then introduced the *Network Enforcement Law* which outlined 21 types of “manifestly illegal” content which platforms were required to quickly remove.<sup>41</sup> The law, passed in June 2017, requires platforms to remove manifestly

---

<sup>32</sup> Helen A.S. Popkin, 2010. “Free Speech vs. Hate Speech on Facebook,” *NBC Connecticut* (19 May), at [https://www.nbcconnecticut.com/news/politics/free\\_speech\\_vs\\_hate\\_speech\\_on\\_facebook/1864429/](https://www.nbcconnecticut.com/news/politics/free_speech_vs_hate_speech_on_facebook/1864429/), accessed 19 December 2019.

<sup>33</sup> Reuters, 2010. “Facebook admits censoring content in Pakistan,” *Reuters* (2 June), at <https://www.reuters.com/article/urnidgns852573c40069388000257735003099ea-idUS126971660620100601>, accessed 19 December 2019.

<sup>34</sup> John Ribeiro, 2010. “Facebook prevent Indian access to anti-muslim group,” *IDG News Service* (24 May), at <https://www.cio.co.uk/it-leadership/facebook-prevent-indian-access-to-anti-muslim-group-3224505/>, accessed 19 December 2019.

<sup>35</sup> Amar Toor, 2015. “Facebook will work with Germany to combat anti-refugee hate speech”, *The Verge* (15 September), at <https://www.theverge.com/2015/9/15/9329119/facebook-germany-hate-speech-xenophobia-migrant-refugee>, accessed 19 December 2019.

<sup>36</sup> Katrin Bennhold, 2018. “Germany Acts to Tame Facebook, Learning From Its Own History of Hate”, *The New York Times* (19 May), at <https://www.nytimes.com/2018/05/19/technology/facebook-deletion-center-germany.html>, accessed 22 August 2019.

<sup>37</sup> Karsten Müller and Carlo Schwarz, 2018. “Fanning the Flames of Hate: Social Media and Hate Crime”, Working Paper Series: Centre for Competitive Advantage in the Global Economy, Warwick University. Online at [https://warwick.ac.uk/fac/soc/economics/research/centres/cage/manage/publications/373-2018\\_schwarz.pdf](https://warwick.ac.uk/fac/soc/economics/research/centres/cage/manage/publications/373-2018_schwarz.pdf), accessed 19 December 2019.

<sup>38</sup> Christina Beck, 2016. “Mark Zuckerberg confronts ‘hate speech’ in Germany and at Facebook”, *Christian Science Monitor* (27 February), at <https://www.csmonitor.com/USA/Society/2016/0227/Mark-Zuckerberg-confronts-hate-speech-in-Germany-and-at-Facebook>, accessed 19 December 2019.

<sup>39</sup> Katrin Bennhold, 2018. “Germany Acts to Tame Facebook, Learning From Its Own History of Hate”, *The New York Times* (19 May), at <https://www.nytimes.com/2018/05/19/technology/facebook-deletion-center-germany.html>, accessed 22 August 2019.

<sup>40</sup> Ibid.

<sup>41</sup> Ibid.

illegal content within 24 hours if its illegality is obvious, or within 7 days if a determination on the nature of the content is more difficult.<sup>42</sup> The law provides for fines of up to €50 million for non-compliance.<sup>43</sup>

Facebook said “It is perfectly appropriate for the German government to set standards”, but argued that it, Facebook, did *not* want to be the arbiter of what breached the standards.<sup>44</sup> German officials rejected this by arguing that the platforms were already the arbiters when it came to compliance on their platform.<sup>45</sup> Gerd Billen, the secretary of state for Germany’s Ministry of Justice and Consumer Protection, said that the question was “Who is sovereign? Parliament or Facebook?”<sup>46</sup> This highlights that this was not a negotiation on how to proceed (as occurred when voluntary agreements were created), but an assertion of the rights and powers of state sovereignty.

A similar assertion of sovereignty was made by the Australian Government in 2019 following the Christchurch attack when new criminal provisions were created with significant penalties for technology platforms, whether inside or outside Australia, that failed to expeditiously remove ‘Abhorrent Violent Material’ they made visible in Australia. ‘Abhorrent Violent Material’ is a term defined in the legislation which included video recorded by a terrorist of their violent attack. Australia has also been active in asserting its rights over taxation, passing the *Multinational Anti-Avoidance Law* in 2015 to “ensure that multinationals pay their fair share of tax on the profits earned in Australia”.<sup>47</sup> On introducing the law the government explained that, “some multinational entities engage in deliberate tax avoidance, exploiting legal loopholes to pay less tax than the law intended”.<sup>48</sup> Google is the latest to reach a settlement with the Australian Taxation Office after agreeing in December 2019 to pay a \$481.5 million settlement, this follows previous settlements by Apple, Facebook and Microsoft.<sup>49</sup>

Sir Tim Berners Lee, the inventor of the World Wide Web, has also supported the notion of government intervention. In 2018 he called for a “legal or regulatory framework that accounts for social objectives”.<sup>50</sup> He warned that the companies society was relying on to fix a growing list of online

---

<sup>42</sup> AFP, 2017. “Germany imposes €50 million fines on social media firms that don't delete hate speech”, *The Local.de* (30 June), at <https://www.thelocal.de/20170630/germany-imposes>, accessed 12 December 2019.

<sup>43</sup> Ibid.

<sup>44</sup> Katrin Bennhold, 2018. “Germany Acts to Tame Facebook, Learning From Its Own History of Hate”, *The New York Times* (19 May), at <https://www.nytimes.com/2018/05/19/technology/facebook-deletion-center-germany.html>, accessed 22 August 2019.

<sup>45</sup> Ibid.

<sup>46</sup> Ibid.

<sup>47</sup> Australian Taxation Office, 2017. “Combating multinational tax avoidance – a targeted anti-avoidance law,” *Australian Taxation Office* (10 August), at <https://www.ato.gov.au/Business/International-tax-for-business/In-detail/Doing-business-in-Australia/Combating-multinational-tax-avoidance---a-targeted-anti-avoidance-law/>, accessed 23 December 2019.

<sup>48</sup> Explanatory Memorandum to the *Tax Laws Amendment (Combating Multinational Tax Avoidance) Bill* 2015, at [https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5549\\_ems\\_f2f9c061-45d9-4f1f-b8f9-eb140cdc08ae/upload\\_pdf/503830.pdf;fileType=application/pdf](https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5549_ems_f2f9c061-45d9-4f1f-b8f9-eb140cdc08ae/upload_pdf/503830.pdf;fileType=application/pdf), accessed 23 December 2019.

<sup>49</sup> Jack Gramenz, 2019. “Google pays \$481.5 million settlement to tax office but still doesn’t think it’s done anything wrong,” *News.com.au* (19 December), at <https://www.news.com.au/technology/online/google-pays-4815-million-settlement-to-tax-office-but-still-doesnt-think-its-done-anything-wrong/news-story/f4468d258c007637524bc5ee27989cf4>, accessed 23 December 2019.

<sup>50</sup> Tim Berners Lee, 2018. “The web is under threat. Join us and fight for it,” *Web Foundation* (12 March), at <https://webfoundation.org/2018/03/web-birthday-29/>, accessed 19 December 2019.



problems were “built to maximise profit more than to maximise social good”,<sup>51</sup> and that the Web itself has changed and was now “compressed under the powerful weight of a few dominant platforms”.<sup>52</sup>

In March 2019, Facebook’s founder, Mark Zuckerberg, took a similar position writing, “I believe we need a more active role for governments and regulators. By updating the rules for the Internet, we can preserve what’s best about it — the freedom for people to express themselves and for entrepreneurs to build new things — while also protecting society from broader harms.”<sup>53</sup> In the area of hate speech, however, he went on to call for a more standardised approach and for “third-party bodies to set standards governing the distribution of harmful content and to measure companies against those standards” to ensure the volume of hate that remained online was minimized.<sup>54</sup> While we support the approach we note the lack of localisation to national laws. By contrast, he was very direct in saying “legislation is important for protecting elections”.<sup>55</sup> It highlights that at least for hate speech, there is still a push for global rules, but with some greater engagement by governments, even as some exceptions based on national law emerge in countries like Germany and now potentially France.

Ultimately governments have the power and authority to regulate online activities that have an impact within their borders. Their power comes from their ability to make and enforce laws, and their authority results from their sovereignty. In a digitally connected world, it is increasingly evident that the idea of a country’s sovereignty territory is being reinterpreted to include online communications with people within the country’s physical territory. This is the only way nations can meet the increasing demands of their citizens for an online experience which takes account of the “real and important differences among people in different places” which Goldsmith and Wu highlighted.<sup>56</sup>

#### 1.2.4 Doctrinal Principles of Internet Regulation

As governments move to regulation there are a number of legal doctrinal principles which ought to be considered.<sup>57</sup> Some of the key concepts are outlined here and are considered in the recommendations made in this report.

The *principle of generality* which holds that it is better to have laws that apply in all circumstances rather than laws that are specific to the online context.<sup>58</sup> Under this principle it would be better, for example, to prohibit the dissemination of a terrorist manifesto than to prohibit the hosting of a manifesto in an online service.

---

<sup>51</sup> Ibid.

<sup>52</sup> Ibid.

<sup>53</sup> Mark Zuckerberg, 2019. “Mark Zuckerberg: The Internet needs new rules. Let’s start in these four areas.” *The Washington Post* (31 March), at [https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f\\_story.html](https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html), seen 23 December 2019.

<sup>54</sup> Ibid.

<sup>55</sup> Ibid.

<sup>56</sup> Jack Goldsmith and Tim Wu, 2006. *Who Controls the Internet: Illusions of a Borderless World*. New York: Oxford University Press, p. viii.

<sup>57</sup> Andre Oboler, 2014. “Legal Doctrines Applied to Online Hate Speech”, at <http://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf>, accessed 12 December 2019.

<sup>58</sup> Jonathan Clough, 2010. *Principles of Cybercrime*. Cambridge: Cambridge University Press, p. 15.



The *principle of inclusion* suggests that it should not be possible to escape the law by acting online rather than in the real world.<sup>59</sup> This creates a need for laws that enable technical solutions to overcome what would otherwise be technical barriers in applying the general law. Such laws might, for example, make it easier to identify an online user or require the preservation of digital evidence.

The *principle of appropriate adaptation* states that laws targeted at the Internet specifically are appropriate when there is an “impact on the nature of the conduct or its prevalence” as a result of harmful behaviour going online.<sup>60</sup> The risk of content inciting violence spreading online to a large audience, creating a significant likelihood that it would be seen by someone susceptible to the message and willing to act, under this principle would justify special laws to ensure rapid removal of such content in order to contain the spread and reduce the risk.

As a corollary to the principle of appropriate adaptation, the nature and prevalence of conduct online can at times make non-criminal responses in practice more effective than a criminal response.<sup>61</sup> Where sanction by online platforms can discourage negative behaviour, for example the posting of hate speech, these sanctions ought to be preferred to legal remedies. The volume of problems that need to be addressed might otherwise overwhelm the justice system. It is this principle which suggests platforms should make the initial call on classifying content as the volume of decisions their business model creates exceeds what the justice system can handle.

The *principle of necessary criminalisation* holds that when responses short of the criminal law would be ‘ineffective, impractical or insufficient’, a criminal response is justified.<sup>62</sup> The conclusion then is that “the criminal law is needed as a final response to online hate speech”,<sup>63</sup> and represents the endgame of a linear series of escalating responses.

### 1.3 Hate Speech and Incitement

The need to carefully define what is regulated speech and what is protected as free speech is a common concern in this field. When it comes to incitement to violence, and specifically incitement for others to carry out violent attacks, the situation is clear, and the speech is clearly unlawful. There are, however, some related issues we would like to highlight.

The first is that incitement to violence against a person or group is unlawful regardless of who the person or group is. It applies at all times to all people. Such incitement to violence is a criminal act.

More extreme cases of incitement against a group can tip into incitement to genocide or ethnic cleansing. States have taken on obligations to protect their people from genocide and ethnic cleansing,

---

<sup>59</sup> Neal Kumar Katyal, 2001. “Criminal law in cyberspace”, *University of Pennsylvania Law Review*, volume 149, pp. 1005-1007, p. 1003.

<sup>60</sup> Jonathan Clough, 2010. *Principles of Cybercrime*. Cambridge: Cambridge University Press, p. 16.

<sup>61</sup> Andre Oboler, 2014. “Legal Doctrines Applied to Online Hate Speech”, at <http://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf>, accessed 12 December 2019.

<sup>62</sup> Jonathan Clough, 2010. *Principles of Cybercrime*. Cambridge: Cambridge University Press, p. 16.

<sup>63</sup> Andre Oboler, 2014. “Legal Doctrines Applied to Online Hate Speech”, at <http://www.austlii.edu.au/au/journals/ANZCompuLawJl/2014/4.pdf>, accessed 12 December 2019.

including protecting them against incitement to genocide and ethnic cleansing. As noted in the 2005 *World Summit Outcome* adopted by the UN General Assembly:<sup>64</sup>

---

*“Each individual State has the responsibility to protect its populations from genocide, war crimes, ethnic cleansing and crimes against humanity. This responsibility entails the prevention of such crimes, including their incitement, through appropriate and necessary means.”*

---

In addition to incitement to violence, we recommend that incitement to hate also be removed. Message spreading hate against an individual or group may not be explicitly violent, but they create an environment in which the risk of violence increases. This risk is amplified in online echo chambers where the veracity of the hate is magnified and may drive some to take it to the next level by engaging in violent actions. This is what we have seen repeatedly now from /pol/.

In this report we occasionally use the phrase “serious hate speech”. This is used in the same context as in the *Racial and Religious Tolerance Act 2001* (Vic) where it refers to hate speech with the added element of threatening or inciting others to threaten physical harm towards the target or their property.<sup>65</sup>

More broadly, we encourage countries that have not already done so to adopt the *Additional Protocol to the Convention on Cybercrime*.<sup>66</sup> The additional protocol is specifically concerned with online racism and xenophobia. It defines “racist and xenophobic material” to mean:<sup>67</sup>

---

*“any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.”*

---

The explanatory report to the Additional Protocol explains “advocates” to mean “a plea in favour of hatred, discrimination or violence”, “promotes” to mean “an encouragement to or advancing hatred, discrimination or violence” and “incites” to refer to “urging others to hatred, discrimination or

---

<sup>64</sup> *Resolution on the 2005 World Summit Outcome*, GA Res 1, UN GAOR, 60<sup>th</sup> sess, UN Doc A/RES/60/1 (2005), Para. 138. Online at <https://www.un.org/en/genocideprevention/about-responsibility-to-protect.shtml>

<sup>65</sup> *Racial and Religious Tolerance Act 2001* (Vic) ss 24, 25..

<sup>66</sup> *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, opened for signature 28 January 2003 (entered into force 1 March 2006) (‘Additional Protocol’). Online at <https://rm.coe.int/168008160f>, accessed 12 December 2019.

<sup>67</sup> *Ibid*, Art. 2(1).

violence”.<sup>68</sup> Hatred itself is defined as “intense dislike or enmity” while violence is described as an unlawful use of force.<sup>69</sup>

The additional protocol calls on signatory states to pass national laws to make the intentional and without right distribution of racist and xenophobic material online a criminal offence.<sup>70</sup> There are additional provisions calling for criminal offences for: racist and xenophobic threats;<sup>71</sup> racist and xenophobic motivated insult;<sup>72</sup> the denial, gross minimisation, approval or justification of genocide or crimes against humanity;<sup>73</sup> or intentionally aiding and abetting someone engaged in one of the other offences.<sup>74</sup>

The additional protocol provides a useful idea of hate speech being speech which “advocates, promotes or incites hatred, discrimination or violence” against targeted group and outlines some of the groups a state may protect, but it is by no means a complete list. Which groups a state protects is up to the law makers of that state and it will vary between states. Technology platforms seeking to comply with a state’s law need to be familiar with the legislation that protects various groups, what it protects them from, and what the thresholds are.

In most cases companies should be able to apply the rules with little difficulty. Where a company is in doubt, it should be possible to seek a ruling from a relevant government authority. If unhappy with the ruling, a platform should be able to challenge the ruling in court and set a precedent to guide further cases. Over time this would add greater certainty in each country. If a government is unhappy with the direction their courts are taking, they can of course amend the law.

The standards set by law in a particular country are the minimum level of protection which platforms should afford to people from that country. There is nothing preventing platforms setting a higher standard through their terms of service. This will protect additional groups in society, but will also allow for greater international consistency which may help platforms retain users and reduce complexity and costs.

There is a need for caution when creating new laws that limit speech and impact on constitutional and civil rights. A balance must be struck between competing rights and where the right to freedom of expression is appropriately limited, reasonable exceptions should be protected for journalism, research, art, the protection of legal rights, etc. Many nations have in fact already struck what they regard as a reasonable balance with appropriate exceptions. The question we focus upon here is how those existing laws, set by nation states, ought to be enforced online. Where the balance is contested, we hope this

---

<sup>68</sup> “Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems”, at <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680989b1c>, accessed 23 December 2019.

<sup>69</sup> Ibid.

<sup>70</sup> *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, opened for signature 28 January 2003 (entered into force 1 March 2006) (‘Additional Protocol’), Art 3. Online at <https://rm.coe.int/168008160f>, accessed 12 December 2019.

<sup>71</sup> Ibid, Art 4.

<sup>72</sup> Ibid, Art 5.

<sup>73</sup> Ibid, Art 6.

<sup>74</sup> Ibid, Art 7.

report provides a basis for understanding the very real links between online hate and real-world violence. Any calibration of rights must take this into account.

We note that this report, like all our reports, includes many examples of hate speech. Documenting such hate is an important research activity and a key part of deconstructing and challenging the hate. Such work is undertaken around the globe by both civil society organisations and governments. We note in particular the excellent work of ODIHR (the Office for Democratic Institutions and Human Rights) in collating such reports on an annual basis from civil society organisations in countries within the Organisation for Security and Co-operation in Europe (OSCE). The use of images from videos created by violent extremists is another matter entirely. We have not included images from the Halle attacker's video in this report, nor have we included images of the attack from other sources. While an example of hate speech can help someone recognise future appearances of the same or similar hate speech, an image of a past attack adds little of value in the context of our work. In another context, for example security training for responding to such attacks, the assessment may well be different. When the law permits an exception so hate speech or extremist material can be reproduced for a legitimate purpose, it is essential researchers are clear on their purpose and on the value that using content providers in the context of their work.

Finally, on the topic of hate speech, we note that this report specifically highlights the very real dangers which can emerge from hate speech in a toxic environment where the hate echoes and magnifies until it emerges as violence. When a particular group regularly engages in hate speech, and that group is connected to multiple deadly attacks, there comes a point where future words of hate said in that group could reasonably be expected to have some likelihood of contributing to expected future violence. In such a context, those words may take on a different meaning and might be considered closer to action than speech as the group slowly edges towards the next attack. Seen in this light, a new understanding of online spaces like /pol/ might be established even in the United States. If such a point can be reached, it will only be after the results of further scholarship and legal consideration. One thing we hope to provide in this report is some of the background which can assist in these considerations.

## 2 The Halle Attack

On October 9, 2019, as Jews around the world gathered in synagogues for Yom Kippur prayers, the synagogue in Halle, Germany, became the target of a terrorist attack.

The attacker tried to force his way in with guns and explosives. He timed his attack for Yom Kippur, the holiest day of the Jewish year, the day with the highest synagogue attendance. It is also the day when security is at its highest. It was the security precautions which kept the attacker out and the community safe. From inside, the community called the police, barricaded the doors and watched the unfolding attack through the synagogue's CCTV monitors.

Unable to get in, the attacker diverted to nearby targets of opportunity. A woman walking past was shot in the back and killed. He drove off and when he spotted a kebab shop he muttered "that'll do" and proceeded to attack it. In the shop he executed a man by shooting him at point blank range. Like Christchurch, the attacker hung out on 8chan, posted a manifesto online and livestreamed his attack. He was arrested and is currently facing two counts of murder and nine counts of attempted murder.

## 2.1 The Attacker

Stephan Balliet is a 27 year old German.

**He is a Holocaust denier.** His live stream opens with him making a statement denying the Holocaust.

**He is an antisemite.** His attack was targeted at Jews, one part of his manifesto says "KILL ALL JEWS!" in size 60 font. Another part of his manifesto refers to Jews as "kikes" and makes use of an antisemitic conspiracy theory about Jewish power, he is obsessed with killing Jews saying, "If I fail and die but kill a single jew, it was worth it".

**He is a white supremacist.** His manifesto speaks about suppressed Whites, literally "supressed Whites" [sic] and "anti-Whites".

**His is a misogynist.** He [makes misogynistic comments](#) in the video before driving to the Synagogue. His manifesto repeatedly speaks about "white men" (rather than the "white race" or "white people"). He tells white men to "dedomesticate" themselves.

**He appears to have been a regular on 8chan.** One of the documents he uploaded refers specifically to 8chan and he wrote "Thank you for all the good time anon". In the video he describes himself as "Anon". This use of Anon (short for Anonymous) is the name users appear under in 4chan / 8chan and similar message boards.

**He was part of the online subculture obsessed with Japanese culture.** He refers to himself as a "weeb" (someone obsessed with Japanese culture) in the live feed. One of his manifesto documents has the filename in Japanese characters and which contained anime.

The German newspaper "Bild" described him [as a Neo-Nazi](#). Germany's Attorney General and Minister of Justice, Christine Lambrecht, [described his actions](#) as a "right-wing extremist terrorist attack".

## 2.2 The Post Announcing the Attack

The attack was announced on the meguca.org imageboard. The original post was made at 11:57am (local time in Germany) on Wednesday 9th of October. The screen capture shown below shows a time stamp of 12:57 pm as it was captured by a person in the next timezone and the boards adjust to display post times in local time for all users. An archived copy showing the correct local time has been viewed. The post was made just 6 minutes before the first emergency call.

The post reads (with some redactions):

---

*"For all of you, who live in no fun countries, this may be of interest.  
Over the past years I built and tested different improvised weapons. I found that the  
best gun to make is... All you need is a weekend worth of time and 50\$ for the  
materials. Cartridges can be made from... most important of all It's reliable. All other  
weapons I tested were not, ... a pain in the ass to build... 3D printed plastic lower and  
will share the files with you. Besides the .stl and freecad files for... there is a small  
guide and some pictures in it, all in all around 50mb.  
Here in the link to the upload: ...  
And here is the magnet link: ...*

*I would appreciate seeding, but only if your local ZOG won't van you for it.  
Of course, there are dozens of improvised designs out there, so what's special with  
mine? Simple, I prefer live testing: <https://www.twitch.tv/spilljuice>"*

---

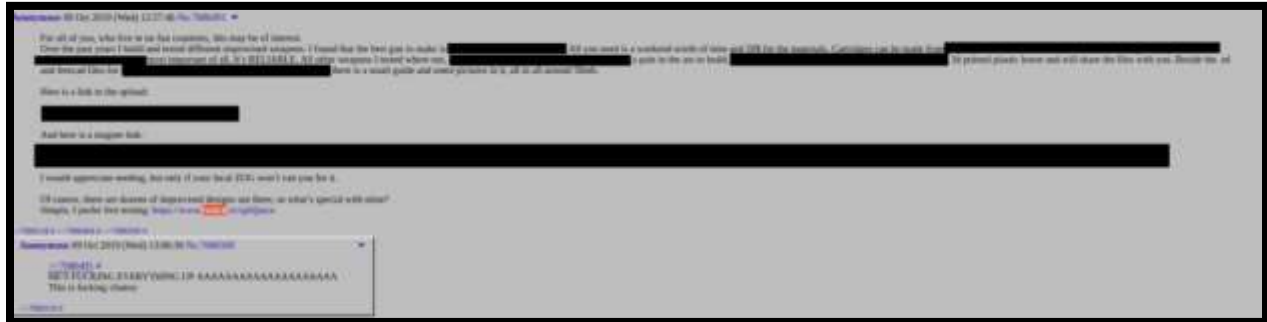


Figure 1 The original post

As shown, this was mostly about the improvised guns, though even here there is an antisemitic reference to ZOG and Jewish conspiracy theories.

Once copy of the files was uploaded to the surface web, the other copy was uploaded to the Dark Net. This is the fourth attack from the far right in the chans that follows this approach of a post to an image board with a manifesto and at least an attempt to live stream. The previous attacks were in [Christchurch](#) (New Zealand), [Poway](#) (USA), and [El Paso](#) (USA). This is the first time with this style of attack that we have seen the Dark Web used as an original upload location for the manifesto.

## 2.3 The Manifesto

The archive file that was uploaded contained three separate PDF files in addition to the .stl and freecad files for printing parts of the weapons. The first was created on October 1, 2019 and is named in Japanese characters which spell out manifesto. The second with a filename of "DoKumentation" was created on October 2, 2019 and is described as "A short pre-action report". The third was created on October 6, 2019 and provides the live streaming details.

### 2.3.1 マニフェスト

The Japanese characters spell the Japanese word "Manifesuto" which in English is "manifest". The addition of two more characters would convert it to the noun manifesto (マニフェスト, 檄文).

The document opens with a title "Techno-Barbarism" displayed in the custom font [Moderne Fraktur](#), an [Old English style](#) of font created by another German in 1999. It is likely a reference to the tabletop game Warhammer 40,000 in which "Techno-barbarians is the name given to the warriors who battled over the ruins of Terra during the Age of Strife".

The subtitle describes the document as a "spiritual guide for discontent White Men" designed for the near future, four years from now. The message is short and in multiple different large sizes of font. First it calls on white men to "Dedomesticate yourself" then it directs them (in huge 60 point font) to "KILL ALL JEWS!". On the next page, almost as an afterthought, it adds to also kill Muslims, Christians, Communists, people of colour and traitors. It uses derogatory language for each group.

The inclusion of Christians is unusual but discussion on /pol/ from around 2017 showed some people promoting the idea that Christianity and White nationalism were mutually exclusive. The argument presented was that (1) Christ was Jewish [QED], (2) the loyalty of Christians is suspect as their loyalty would first be to Jesus and only after to their "race", and further, they would accept non-whites so long as they converted.

Some White nationalist groups have co-opted Norse mythology. We see this in one of the documents Balliet uploaded where he speaks of Valhalla, the place where worthy warriors go after they die in Norse mythology. In Melbourne, the far-right group "[Soldiers of Odin Australia](#)", an offshoot of a Finnish group, is an example of this connection. The groups are named after [Odin](#) a principle god, and specifically a war god, in Norse mythology.

Many white nationalist groups, however, consider themselves Christian. The [Christian Identity movement](#) is an example of this, as is the [Ku Klux Klan \(KKK\)](#). Much of the far right has adopted Christian crusader imagery in their promotion of hate against the Muslim community.

The third page is almost entirely blank, except for the comment "thanks for reading" in regular sized font at the bottom of the page. Following the incitement to violent extremism the document ends with what looks like an advertisement with a large image, an offer and some fine print with conditions. The offer reads "Become a Techno-Barbarian TODAY and get a FREE\* Cat-Girl". The fine print reads "\*Disclaimer: You need to kill at least one jew to qualify. Alternatives include Fox-Girls and normal Waifus. She will always be loyal, so treat her good." The image features a Catgirl in a box labelled "Strategic Cat-girl Supplies" in Moderne Fraktur font (as used at the start of the document). The original image, which has been widely shared online over many years, instead has a parody of an Amazon logo with the word "Anyzon" in black above the curved orange arrow.

The image is of Yukino Yukinoshita but turned into a cat girl. The character is from the Japanese light novel series (and later anime television series) "Yahari Ore no Seishun Rabukome wa Machigatteiru" (literally: "My Youth Romantic Comedy Is Wrong, As I Expected") which was judged the best Japanese light novel by online polls in 2014, 2015 and 2016. In the series [Yukino Yukinoshita](#) is a 16/17 year old student who was the founding president of the [Service Club](#), a student club for volunteers to help those in need. One of her quotes is "People fail because they don't understand the hard work necessary to be successful". Somewhat ironic given Balliet's attack was generally seen as a dismal failure by those he was trying to incite.

As mentioned, Yukino Yukinoshita is in this instance turned into a Catgirl. [Catgirls](#), also known as Neko or Nekomimi (literally "cat-ears" in Japanese), are characters in anime and manga who are girls with cat characteristics, often just the ears, but they may have other characteristics such as the eyes and tail of a cat. They are [popular on 4chan](#) and more broadly within parts of online culture. In some parts of online culture, particularly around the Chans (4chan / 8chan and others) the use of Catgirls can involve an element of gender based hate. This at one point led to the ban of and [significant debate](#) about the [appropriateness of Catgirls](#) on Reddit's socialism community, /r/socialism. When gendered based hate is in play, the misogyny reduces women to "pets" designed for the largely male audience to own and use.

The "advertisement" as a whole follows the misogynistic use of catgirls. In this instance not only is girl with cat like features presented as a pet, she is offered as a free giveaway. The message she will "always be loyal" and should be "treated good" further promotes the idea of a pet.

### 2.3.2 Read This First

The file with the filename of “READ THIS FIRST” provided a short message “Thank you for all the good time anon” and a link which was labelled as the livestream.

The live streaming account name was “spilljuice”. According to [the dictionary](#), an archaic meaning of "spill" includes "kill" or "destroy". "Juice" is a pun on "Jews" popularised by the second ["Hipster Hitler" cartoon](#) from August 28th, 2010 which was spread in various forms online. The image of Hitler in the "I love juice" shirt is often used in isolation as a meme.





Figure 2 The second Hipster Hitler cartoon

The document goes on to sarcastically thank Mark Mann, described as an 8chan Board Owner, for making a donation of 0.1 bitcoin (around AU\$1,220). The attacker states he was at the time intending to target Muslims and had promised the board owner he would not name him. After naming him the message continues by accusing him of being a "filthy jew" and says that he probably does not exist anyway and is likely from the CIA and trying to radicalise people and set them up. He concludes with further antisemitic stereotype.

Mark Mann is a Jewish employee of the internet service provider NT Technology, a company owned by Jim Watkins who also owns 8chan.<sup>75</sup> The reference has been described as “almost certainly a cruel joke” but one which demonstrates the Halle attacker was “deeply familiar” with 8chan.<sup>76</sup>

### 2.3.3 DoKumentation

The file named "DoKumentation" opens with the title “a short pre-action report”. It is 11 pages long, the first 8 and 3/4 are a description of weapons, filming equipment and body armour. The next page and a quarter describe his objectives and plan. The last page is a list of “achievements” in the style of a video game.

#### 2.3.3.1 *The equipment*

The first section details the weapons under sections named “on man”, “car guns” and “fallback weapons”. The weapons include six different guns, a sword, a knife and a range of explosives.

Except for the Smith-Carbine rifle (a gun patented in 1857 and used in the American civil war), the guns are improvised, that is, self-made, as is the ammunition. Balliet knew the weapons, particularly the guns, were very poor quality. He describes the range of most of his guns and the worst had a range of just 5 metres while the best had a range of 25 metres. To put this in perspective, the average 14 to 18 year old boy can [throw a ball](#) about 58 meters. The two people he killed were both killed at close range. He also described a range of other shortcomings in his weapons. One gun, made with a 3D printer, was likely to heat up and melt from repeated use. Another was highly likely to jam and would require significant time and tools to fix.

---

<sup>75</sup> Robert Evans & Frederick Brennan 2019, “The State of California Could Have Stopped 8Chan: It Didn’t”, *Bellingcat* (4 November), at <https://www.bellingcat.com/news/2019/11/04/the-state-of-california-could-have-stopped-8chan-it-didnt/>, accessed 12 December 2019.

<sup>76</sup> Ibid.

### Luty SMG 9mm Parabellum



The explosives are described as fragmentation grenades, pipe bombs, nail bombs, smoke grenade, breaching charge, anti-material charge and detonation caps. As stated earlier, thankfully neither the guns nor the explosives were able to destroy the wooden door which prevented him gaining access to his primary target, the synagogue and the people praying within.

This part of this manifesto document appears designed to facilitate actions by others. Descriptions vary with some more focused on how the ammunition will be stored / held, while others give detailed specifications of the materials, sizes, chemical ratios and so on, . for the guns and their ammunition. For the 3D printed gun, he writes that "Building instruction and .stl files are in the full upload." A 3D printer was also used for the stock of two guns and cartridges for one.

#### *2.3.3.2 The Plan*

This section, taking up a page, ends with "Tldr:" (short for "too long didn't read") and a 2.5 line summary which highlights how Balliet wants to "Go in and kill everything" but expects he will have to improvise, things will go wrong, and he will end up in a situation where he will "Drive away. Kill some more." Which is exactly what happened.

The summary ends "Repeat until all jews are dead or you prove the existence of Waifus in Valhalla, whatever comes first. Jej." This short ending has compresses the key ideas. (1) an antisemitic call not

only to kills Jews, but seek the complete annihilation of Jews. Something reminiscent of Hitler's final solution. (2) a reference to Waifus,<sup>77</sup> a term from anime for the woman a character is fond of, (3) the reference to Valhalla refers to Norse mythology and is co-opted by far-right groups as part of white supremacy, (4) "Jej" is an ironically mistyped variation of "Kek", both being 4chan / 8chan versions of "lol". Its use is a deliberate effort to link back to the chans.

The inclusion of a summary and an explicit expectation that people would not read a page about his plan (while there is no such summary of the previous and much longer discussion of weapons) again highlights where Balliet's interest lies, and it is not in deep ideological discussions.

Some features from the detailed explanation of the plan:

- There is another instance of "jej" when he jokes that "For some reason (jej) the security measures are quite high" on the synagogue.
- He refers to Jews as "rats", a well worn antisemitic trope, saying he may try "lure the rats out".
- He also again refers repeatedly to Jews as "kikes", another antisemitic slur.
- He also uses the antisemitic trope of "ZOG" ("Zionist Occupied Government") claiming Jews are responsible for governments increasing Muslim immigration. This is a common far right conspiracy theory, and it goes back to older conspiracy theories of Jewish power more generally such as those found in the forgery [The Protocols of the Elders of Zion](#).
- He states that he chose to attack on Yom Kippur "because even 'non-religious' jews are often visiting the synagogue on this date".
- He also states this synagogue was chosen as it was the closest place where a significant number of Jews could be found that was close to him.
- He originally considered attacking a mosque but decided the Jews were the greater enemy.
- The section ends with a chilling line that promoting and encourages "White men" to kill Jews, with the intention of exterminating them.

#### 2.3.3.3 *Achievements*

The final page of this part of the manifesto is a list of "achievements". There are goals as might appear in a game in order to receive a reward or achievement badge. In this case, however, the goals all related to the planned terrorist attack. There were 26 different achievements listed.

#### **Technical steps to carrying out the attack**

- Upload the PDF
- Successfully livestream the attack

#### **Murder particular targets**

- Murder a Jew
- Murder 6 Jews
- Murder a Jewish woman
- Murder a Jewish child
- Murder a Jew using a grenade

---

<sup>77</sup> Waifu, at <https://www.dictionary.com/e/fictional-characters/waifu/>, accessed 12 December 2019.

- Murder both a Jew and Muslim
- Murder 3 people of colour in a specified time period
- Murder a “traitor”
- Murder a police officer (literally “Kill a ZOG-bot”)
- Murder a communist
- Murder a Christian

#### Murder someone using a particular weapon

- Murder someone with a particular homemade gun x 4 different named guns
- Murder someone with a sword
- Murder someone with a knife
- Murder someone using the “secret weapon”
- Murder someone with a particular type of explosive x 2 different types

#### Serious harm

- Stab a Muslim

#### Property destruction

- Burn down a synagogue
- Burn down a mosque

#### Accidental harm

- Cause self-harm as a result of the homemade explosives

Each goal was given a title as well as a description. The names are a range of puns and racist memes. The goal to kill 6 Jews, for example, was labelled “Anudda Shoa” a reference to the Holocaust and the 6 million Jews who were murdered by the Nazis. The goal of killing a Jewish woman is titled “Gender Equality”, an ironic title given the rejection of feminism in particular and equality in general by the attacker and this subculture.

## 2.4 Technology the Attacker Used

The post announcing the attack was originally made on the meguca.org imageboard. An archive file was created with 7-Zip, a free and open-source file archiver, which contained the three pdf files making up the manifesto as well as .stl and freecad files for 3D printing parts of the weapons. The archive file was uploaded to anonfile.com and the Dark Web by the attacker and the link to the archive was included in the original post. The live streaming was carried out via twitch.tv, a stream service for gamers which is owned by Amazon. The weapons and munitions were homemade and used technology in the form of a 3D printer for some of the components. These technologies will now be examined in further detail.

### 2.4.1 The Announcement: Meguca.org

Meguca.org is an image board loosely affiliated with 4chan's anime board.<sup>78</sup> The name is based on a meme mocking the anime Puella Magi Madoka Magica.<sup>79</sup> Its homepage declared, "[M]eguca.org has not received any gag orders and there's no Patriot Act here. Sucks to live in a third world police state like the US".<sup>80</sup> Its source code repository describes it as an "anonymous realtime imageboard focused on high performance, free speech and transparent moderation".<sup>81</sup> A few days after the attack (at least from the 11th of October) the site went down.

In a series of posts in April 2017 the admin of /pol/ on Meguca discusses the site and the /pol/ boards rules.<sup>82</sup> The global rules across all boards only banned illegal content and spamming. The /pol/ board added rules against "disruption" – anything off topic or spammy, "degeneracy" - used in a similar sense to that of the Nazis themselves to refer to anything their ideology disagreed with, for example *Degenerate Art*,<sup>83</sup> "cancer" - anything which can "kill" the thread/discussion,<sup>84</sup> and "namefaggotry" - posted that are not made as "anonymous".<sup>85</sup> It described itself as "EXPLICITLY a natsoc board, anti-degenerate, anti-semitic, pro-white". The board admin considered 8chan compromised and said "admitting you're from 4chan is a bannable offense".

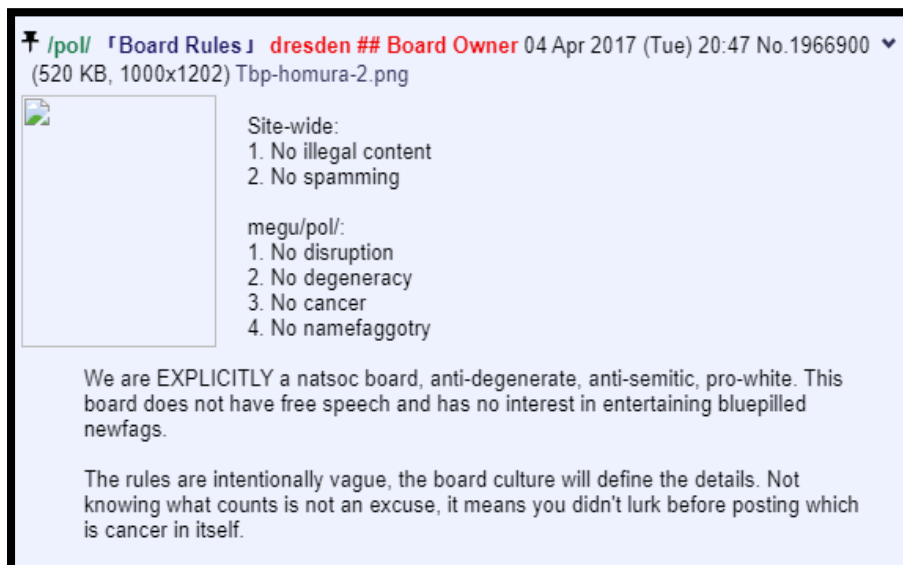


Figure 3 Introduction to the rules of /pol/ on Meguca

<sup>78</sup> Ryan Broderick, 2019. "Far-Right Halle Shooter Allegedly Posted A Manifesto With Xbox-Like "Achievements", *BuzzFeed News* (11 October), at <https://www.buzzfeednews.com/article/ryanhatesthis/halle-germany-shooter-meguca-anime-manifesto>, accessed 12 December 2019.

<sup>79</sup> Ibid.

<sup>80</sup> Ibid.

<sup>81</sup> Bakape, 2019. "Meguca", *Github*, at <https://github.com/bakape/meguca>, accessed 12 December 2019.

<sup>82</sup> "Meguca", 2017. *Github*, at <https://web.archive.org/web/20170713104204/https://meguca.org/pol/1966900>, accessed 12 December 2019.

<sup>83</sup> *Degenerate Art*, at <https://www.tate.org.uk/art/art-terms/d/degenerate-art>, accessed 12 December 2019.

<sup>84</sup> Adrien Chen, 2011. "Here's What 5 Million Posts on 4chan Look Like", *Gawker* (12 July), at <https://gawker.com/5820505/heres-what-5-million-posts-on-4chan-look-like>, accessed 12 December 2019.

<sup>85</sup> 'Namefag', *Urban Dictionary*, at <https://www.urbandictionary.com/define.php?term=namefag>, accessed 12 December 2019.

The admin stated users should “always maintain your opsec” (operational security) and banned “Any links posted to any non-anonymous social communities... for any reason other than raiding”. Raids, that is mass attacks, on other online sites were therefore, explicitly encouraged. Rather than arranging to meet in person via the board members were told to “Organize local” highlighting a desire for people to act beyond the online forum. In a post about “transparency” the admin says that “Meguca's servers are in Paris, DNS is cloud flare” and that the Admin is a “Lat” (Latvian). The idea of it being hosted in France seems particularly strange given that country’s strong laws against antisemitism and Holocaust denial.<sup>86</sup> In another post they say that “IPs are stored for 7 days”.

Just as 8chan was seen as more extreme than 4chan, Meguca set itself up, and its /pol/ board in particular, to be more extreme than 8chan and explicitly neo-Nazi. On this board there was no effort to even pretend the racism and neo-Nazism was satirical or in jest and there was no interest in attracting and converting new users. This was a community designed for extremism.

**RECOMMENDATION 1:** Where an image board is hosted in a country and the site, or a board within it, actively promotes hate speech which is unlawful in that country, the hosting provider once it is aware of this, should take action to terminate the hosting.

**RECOMMENDATION 2:** Where a domain name is registered in a country, and the owner actively uses the site at that domain for the purpose of promoting hate speech which is unlawful in that country, the domain name should be terminated by the domain name registrar.

#### 2.4.2 The first Document Hosting Service: anonfile.com

The anonfile.com service is an anonymous file hosting service. Users can upload files of up to 20 GB to the service and are then provided with a unique URL that allows the files to be downloaded.<sup>87</sup> The URL can then be shared with others to download the contents. There are no limits on the number of downloads, the bandwidth that can be used, or the length of time the file can be online.<sup>88</sup>

The service has a short statement on its *terms of use* with just 5 points.<sup>89</sup> They are (in full):

##### § General

It is strictly forbidden to spread viruses, trojans, corrupt and/or illegal material via AnonFile. Always check with your local laws before submitting content.

##### § Availability

AnonFile cannot guarantee full availability of the service, however, we do our best to keep the service as stable as possible. AnonFile disclaim all responsibility for loss of income due to downtime and/or data loss

##### § Logging Downloads

<sup>86</sup> Valery Engel, 2012. *White Papers of Hate 2012*. Berlin, Germany: Book Club Knigovek, pp. 266-268. Online at <https://tandis.odihr.pl/bitstream/20.500.12389/21854/1/07980.pdf>, accessed 12 December 2019.

<sup>87</sup> ‘Home’, AnonFile, at <https://anonfile.com>, accessed 12 December 2019.

<sup>88</sup> ‘FAQ’, AnonFile, at <https://anonfile.com/faq>, accessed 12 December 2019.

<sup>89</sup> ‘Terms’, AnonFile, at <https://anonfile.com/terms>, accessed 12 December 2019.



We are strong advocates of privacy & do not log downloads.

#### § Administrative measures

AnonFile administrators has the right to remove and/or permanently ban file content they find inappropriate.

#### § Changes

This user agreement is subject to change at any time, please review this agreement before you decide to use the service. You are technically bound to accept this agreement by accessing/using the service.

The terms of service claim they are “strong advocates of privacy” and for this reason “do not log downloads”. This makes the service particularly attractive for those engaging in illegal activity including terrorism. With this deliberate attempt to avoid keeping records, when law enforcement is authorised to access the system and investigate it, there would likely be little available evidence to assist them.

The terms of service do forbid the use of the service “to spread viruses, trojans, corrupt and/or illegal material”. Terrorism is not specifically mentioned but would come under “illegal material”. The ordering of the prohibitions suggests the platform views sharing means of technically disrupting other systems as a far greater wrong than spreading illegal material.

A link to report abuse is visible in the footer of each page. The footer reads: “Login - Register - Terms of Use - API - FAQ - Feedback - REPORT ABUSE”. The prominence given to reporting abuse is high which is positive. Far less positive is the abuse reporting process itself.

Despite the terms of service stating that the platform “are strong advocates of privacy”, as shown in Figure 4, the reporting page states “You must provide genuine information regarding who you are, who you represent and which file(s) this report concerns. Note: We strongly believe in transparency toward our users. Therefore, [sic] by filing a report you also agree on it being attached for public viewing along with the takedown message in order to inform our users.”<sup>90</sup> This denies users the ability to report content anonymously.

The arguments in favour of anonymous reporting of potential abuse are far stronger than arguments in favour of allowing anonymous hosting of files. This setup facilitates the spread of illegal content while inhibiting reporting of abuse.

---

<sup>90</sup> ‘Abuse’, AnonFile, at <https://anonfile.com/abuse>, accessed 12 December 2019.



# Report Abuse

If you believe some of our users has violated our Terms of Service or your intellectual property rights, please file a report in the form below.

You must provide genuine information regarding who you are, who you represent and which file(s) this report concerns.

**Note:** We strongly believe in transparency toward our users. Therefor, by filing a report you also agree on it being attached for public viewing along with the takedown message in order to inform our users.

\* English only.

\* All Fields Required.

Reason for reporting:

Name:

E-mail:

Link to report:

Abuse Report Description:



Type the above characters:

Figure 4 Abuse reporting form on anonfile.com

**RECOMMENDATION 3:** All services that allow users to upload or post content should have clearly visible mechanisms for reporting to the service provider any content that violates the terms of such services.

**RECOMMENDATION 4:** All services that allow users to upload or post content should allow content to be reported anonymously to the service provider and by anyone who can see the content. If content is visible without having an account, then it should be reportable without having an account.

**RECOMMENDATION 5:** To assist with lawful counter terrorism investigations, all services that allow users to upload or post content should maintain logs for at least 24 hours. Where a user reports content, log details related to the original uploader / poster of that content should be maintained for a further period of at least 7 days.

## 2.4.3 The second Document Hosting Service: The Dark Web

The attacker also uploaded the archive file with their manifesto documents and CAD files to the Dark Web. This is the first attack of this kind where the manifesto has been released on the Dark Web right from the start by the attacker, rather than being transferred to the Dark Web after it became harder to share through traditional websites and online services.

The Dark Web is a part of the Internet that can only be reached using specialised software such as The Onion Router (aka Tor). Content on the Dark Web is not indexed and the software used to access it has been designed to ensure the anonymity of both the server hosting content and the user who is requesting access to it.<sup>91</sup> That includes ensuring the basic use of the service is anonymous, so a user requesting content does not know where the server is, and the server does not know who is requesting content from it. The servers operating in this way are known as *Tor hidden services* and they can be recognised by their address which ends in a “.onion” extension.<sup>92</sup> The system was created to facilitate anonymous access to an uncensored Internet as a form of opposition to an increasing threat of Internet surveillance.<sup>93</sup>

While designed to hide the location of the servers, which also makes it impossible to know what legal jurisdiction they are in, poor configuration can open vulnerabilities which can make it possible to unmask the server and trace its IP address.<sup>94</sup> Unmasking efforts in the past have included forcing servers to access a particular address, allowing the owner of that address to look up the Tor hidden service’s IP address in their logs.<sup>95</sup> Another approach has been to examine security certificates that have been misconfigured and appear on the surface web, but listing Tor hidden service address.<sup>96</sup> There have also been scanners like PunkSPIDER which have scanned the Dark Web for vulnerabilities.<sup>97</sup> A range of other attacks designed to compromise anonymity in the Dark Web have also been reported by researchers and as with all areas of cybersecurity it is a cycles of finding and patching vulnerabilities. At times knowledge of certain vulnerabilities are kept secret so they can be exploited by law enforcement and other government agencies.

A shift to the Dark Web as the initial hosting point for extremist material will further complicate the removal of content, but will also cut down the accessibility and spread of the content. For the content to spread it will still be necessary to share an address hosting the content and these addresses can themselves be targeted for removal by governments and online platforms.

**RECOMMENDATION 6:** Laws and policies designed to prevent the spread of extremist material need to be flexible enough to cover content consisting of a link which directly or indirectly will lead to the material.

---

<sup>91</sup> Joseph Cox, 2015. “This Researcher Is Hunting Down IP Addresses of Dark Web Sites”, *VICE* (23 June), at [https://www.vice.com/en\\_us/article/9ak7xa/this-researcher-is-hunting-down-ip-addresses-of-dark-web-sites](https://www.vice.com/en_us/article/9ak7xa/this-researcher-is-hunting-down-ip-addresses-of-dark-web-sites), accessed 12 December 2019.

<sup>92</sup> Ziyahan Abeniz, 2018. “Exposing the Public IPs of Tor Services Through SSL Certificates”, *Netsparker* (27 November), at <https://www.netsparker.com/blog/web-security/exposing-public-ips-tor-services-through-ssl-certificates/>, accessed 12 December 2019.

<sup>93</sup> ‘History’, *Tor Project*, at <https://www.torproject.org/about/history/>, accessed 12 December 2019.

<sup>94</sup> Joseph Cox, 2015. “This Researcher Is Hunting Down IP Addresses of Dark Web Sites”, *VICE* (23 June), at [https://www.vice.com/en\\_us/article/9ak7xa/this-researcher-is-hunting-down-ip-addresses-of-dark-web-sites](https://www.vice.com/en_us/article/9ak7xa/this-researcher-is-hunting-down-ip-addresses-of-dark-web-sites), accessed 12 December 2019.

<sup>95</sup> Ibid.

<sup>96</sup> Ziyahan Abeniz, 2018. “Exposing the Public IPs of Tor Services Through SSL Certificates”, *Netsparker* (27 November), at <https://www.netsparker.com/blog/web-security/exposing-public-ips-tor-services-through-ssl-certificates/>, accessed 12 December 2019.

<sup>97</sup> Thomas Brewster, 2015. “Hackers Scan All Tor Hidden Services To Find Weaknesses In The ‘Dark Web’”, *Forbes* (1 June), at <https://www.forbes.com/sites/thomasbrewster/2015/06/01/dark-web-vulnerability-scan/#26ddd30c6d23>, accessed 12 December 2019.

#### 2.4.4 The Live Streaming and Video Hosting Service: Twitch

In this attack Twitch (Twitch.tv), a live streaming service owned by Amazon, was used to provide the broadcast. Twitch describes itself as "the world's leading live streaming platform for gamers". It was created as a gamer focused spin off of the live streaming service Justin.tv, which was shutdown in August 2014 when the company decided to focus on Twitch. Though still mostly used for broadcasting game play, with categories dedicated to different games and other themes, there is increasing popularity in the non-game "Just Chatting" and "IRL" categories. Prior to this attack the biggest problem Twitch had was preventing adult content which is against its community standards.<sup>98</sup>

The attack was livestreamed on Twitch at <https://www.twitch.tv/spilljuice> for 35 minutes starting at 12:00 pm Central European Time (CET).<sup>99</sup> Three people watched the attack in this livestream.<sup>100</sup> There is a setting in Twitch which can cause a video to be automatically generated and posted when a livestreaming session ends. This setting was turned on in the attacker's account. The resulting video was seen by 333 people over the next 4 hours and 45 minutes since the livestream ended. The spread of the video greatly increased between 5:20 pm CET and 5:50 pm CET with 2200 additional visitors.<sup>101</sup> At 5:50 pm CET the video was removed and the "spilljuice" channel were suspended.<sup>102</sup>

The Twitch service has an extensive reporting function which allows livestreams, videos, clips, private messages, live chat, profile content, usernames, channel points and rewards as well as failure to moderate others to all be reported. It also provides a general option for anything else not covered.

In the case of livestreaming and videos the second stage of reporting offers a range of categories such as "Threats, harm, or endangerment of someone" and "hate speech, harassment, or abuse".

While generally well paired, the urgency required in a livestream of real-world violence is significantly higher than that

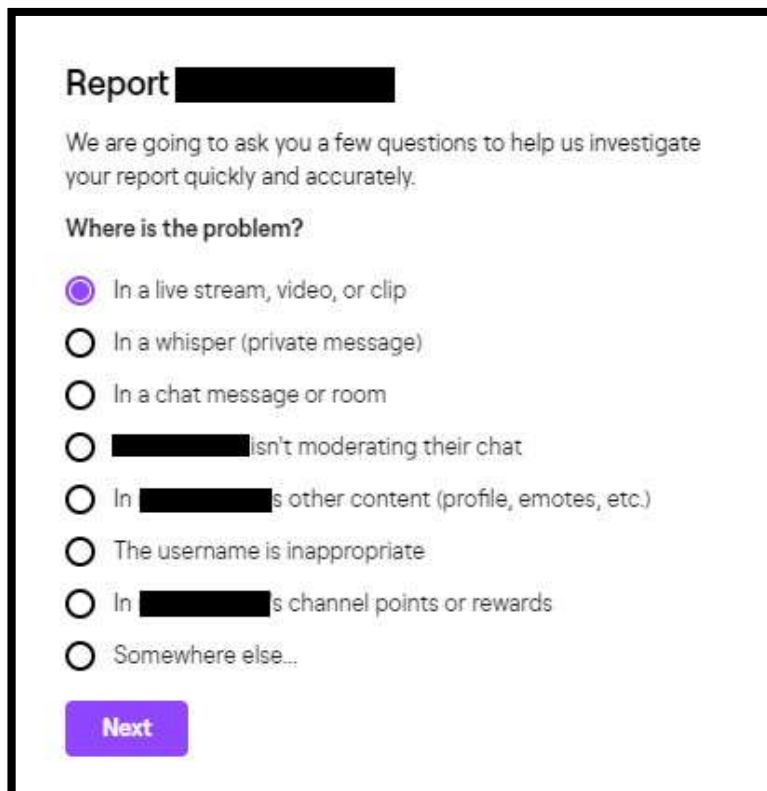


Figure 5 Step one in reporting on Twitch

<sup>98</sup> Eric Switzer, 2019. "Twitch Banned These Korean Supermodels, But They'll Be Back", *The Gamer* (20 August), <https://www.thegamer.com/twitch-banned-korean-supermodels-theyll-be-back>, accessed 12 December 2019.

<sup>99</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1182036266344271873>, accessed 12 December 2019.

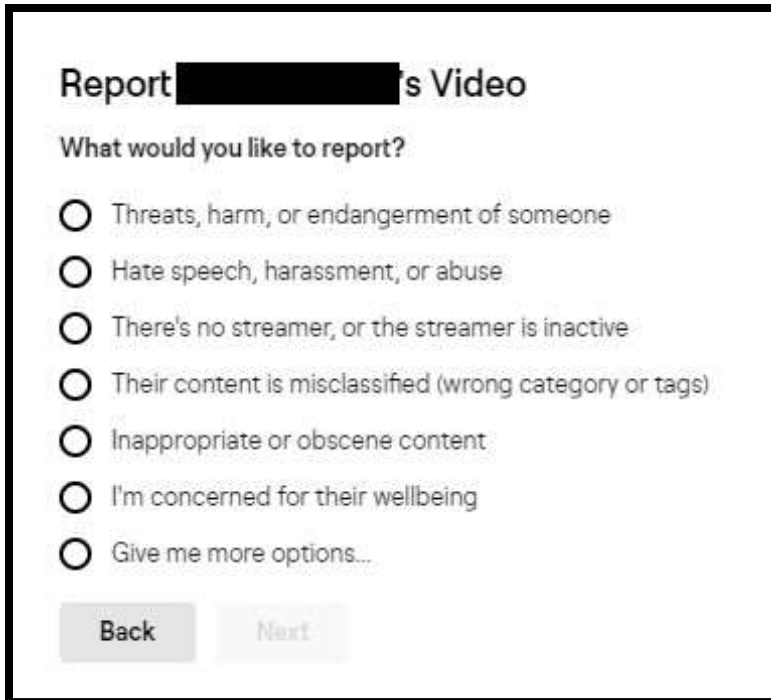
<sup>100</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1185200174953455620>, accessed 12 December 2019.

<sup>101</sup> Ibid.

<sup>102</sup> Ibid.

required in the case of threats. Endangerment covers a wide range of problematic behaviour from encouraging someone to commit suicide through to suggestions which carry a risk of relatively minor injury.

Overall the Twitch reporting system is extensive, mature and fit for purpose. Depending on the volume of reports in the “threats, harm, or endangerment of someone” category and the average speed at which Twitch can respond to them, there may be a need to introduce a new category for “Real world violence, extremism or crime”. This would allow faster responses in the case of unfolding real world harm.



Report [redacted]'s Video

What would you like to report?

- ☐ Threats, harm, or endangerment of someone
- ☐ Hate speech, harassment, or abuse
- ☐ There's no streamer, or the streamer is inactive
- ☐ Their content is misclassified (wrong category or tags)
- ☐ Inappropriate or obscene content
- ☐ I'm concerned for their wellbeing
- ☐ Give me more options...

Back Next

A further reporting step allows users to provide further details including links to videos if they wish.

**RECOMMENDATION 7:** Livestreaming and video hosting sites should provide reporting options that allow the rapid identification, and a priority response, to reports of actual violence, extremism or unfolding crime.

**RECOMMENDATION 8:** Platforms should publish their target response time for reviewing and responding to reports of content flagged by users as potential violent extremist content or whichever broader category the platform chooses which includes violent extremist content. Platforms should also publish their average response time to reports in this category on a regular, e.g. monthly, basis.

### 3 Antisemitism in the Halle Attack

The term “antisemitism” refers to the hatred of Jews, but its long history and many differing forms can at times make it difficult to identify or understand.

The term itself was coined by German Journalist Wilhelm Marr, who between 1879 and 1880 published two popular pamphlets which referred to “Jews” and “Jewishness” as “Semitismus”, and “Antisemitismus” as opposition to the Jewish people.<sup>103</sup> Marr himself was an antisemite, founding the *Antisemiten-Lega* or “League of Antisemites”, and based his beliefs on pseudoscientific theories of race

---

<sup>103</sup> Wilhelm Marr, *Der Sieg des Judenthums über das Germanenthum. Vom nicht confessionellen Standpunkt aus betrachtet*, 1879; Wilhelm Marr, *Der Weg zum Siege des Germanenthums über das Judenthum*, 1880.

that predated Nazi racial science.<sup>104</sup> While the term “Semitic” is used in linguistics for a broad group of languages,<sup>105</sup> the term antisemitic has always been exclusively about hatred of Jews.<sup>106</sup> The spelling without a hyphen, antisemitism and rather than anti-Semitism, is preferred by many scholars to avoid confusion or obfuscation.<sup>107</sup>

While Marr was concerned with the race of Jews, anti-Jewish hatred well-predated him, and was often based on religious grounds during the Middle Ages. In Christian Europe, Jews were known as “Christ-Killers” for their alleged role in the death of Jesus Christ,<sup>108</sup> and even subject of fantastical accusations such as ‘blood libel’, which accused Jews of using the blood of Christian children in rituals.<sup>109</sup>

In order to aid the understanding of antisemitism, the International Holocaust Remembrance Alliance (IHRA), an international inter-governmental organisation, adopted the *Working Definition of Antisemitism* on 26 May 2016.<sup>110</sup> The adoption was a unanimously decision by the then 31 member countries.<sup>111</sup> Australia was an observer to the IHRA at the time and joined the organisation as a full member in June 2019.<sup>112</sup> Before discussing the specific manifestations of antisemitism in the Halle attack, we will introduce the *Working Definition of Antisemitism* in more detail.

### 3.1 The IHRA Working Definition of Antisemitism

Since it was adopted in May 2016, the IHRA Working Definition of Antisemitism has received broad international support. A resolution of the European Parliament calls on member states and European institutions to adopt the definition,<sup>113</sup> and the definition has been formally adopted in Austria, Belgium, Bulgaria, Canada, the Czech Republic, France, Germany, Greece (by the Ministry of Education), Hungary, Israel, Lithuania, the Republic of Moldova, the Republic of North Macedonia, Romania, Scotland, Slovakia, Sweden, United Kingdom and the Netherlands. In the United States an almost identical definition is used by the State Department.

---

<sup>104</sup> ‘Wilhelm Marr’, *Jewish Virtual Library*, at <https://www.jewishvirtuallibrary.org/wilhelm-marr>, accessed 12 December 2019.

<sup>105</sup> Patrick R. Bennett, 1998. *Comparative Semitic Linguistics: A Manual*. Winona Lake, Indiana: Eisenbrauns.

<sup>106</sup> International Holocaust Remembrance Alliance, 2018. “Spelling of Antisemitism”, at <https://www.holocaustremembrance.com/spelling-antisemitism>, accessed 12 December 2019.

<sup>107</sup> Ibid.

<sup>108</sup> Jeremy Cohen, 2007. *Christ Killers: The Jews and the Passion from the Bible to the Big Screen*. New York: Oxford University Press.

<sup>109</sup> Gavin I. Langmuir, 1996. *Toward a Definition of Antisemitism*, Los Angeles: University of California Press, p. 216.

<sup>110</sup> International Holocaust Remembrance Alliance, 2016. “Working Definition of Antisemitism 2016”, at <https://www.holocaustremembrance.com/node/196>, accessed 12 December 2019.

<sup>111</sup> International Holocaust Remembrance Alliance, 2016. “Working Definition of Antisemitism” (press release), at <https://www.holocaustremembrance.com/stories/working-definition-antisemitism>, accessed 12 December 2019.

<sup>112</sup> Marise Payne, 2019. “Australia joins International Holocaust Remembrance Alliance”, *Press Release from Australia’s Minister for Foreign Affairs* (5 June), at [https://foreignminister.gov.au/releases/Pages/2019/mp\\_mr\\_190605.aspx](https://foreignminister.gov.au/releases/Pages/2019/mp_mr_190605.aspx), accessed 12 December 2019.

<sup>113</sup> Roberta Metsola & Heinz K. Becker, 2017. *European Parliament Resolution on Combating Anti-Semitism (Resolution 2017/2692)*, The European Parliament. Online at [http://www.europarl.europa.eu/doceo/document/B-8-2017-0383\\_EN.html?redirect,%20accessed%2012%20December%202019](http://www.europarl.europa.eu/doceo/document/B-8-2017-0383_EN.html?redirect,%20accessed%2012%20December%202019), accessed 12 December 2019.

In Australia the definition is used in an annual report on antisemitic incidents compiled by the Executive Council of Australian Jewry.<sup>114</sup> It has also been adopted by the Australian National Union of Students and a range of Students' Unions.<sup>115</sup>

The core of the IHRA Working Definition explains:<sup>116</sup>

---

*Antisemitism is a certain perception of Jews, which may be expressed as hatred toward Jews. Rhetorical and physical manifestations of antisemitism are directed toward Jewish or non-Jewish individuals and/or their property, toward Jewish community institutions and religious facilities.*

---

It continues with several examples of different types of common manifestations of antisemitism, although makes it clear that antisemitism is not limited to these examples.<sup>117</sup> The examples provided are:<sup>118</sup>

- 
- *Calling for, aiding, or justifying the killing or harming of Jews in the name of a radical ideology or an extremist view of religion.*
  - *Making mendacious, dehumanizing, demonizing, or stereotypical allegations about Jews as such or the power of Jews as collective — such as, especially but not exclusively, the myth about a world Jewish conspiracy or of Jews controlling the media, economy, government or other societal institutions.*
  - *Accusing Jews as a people of being responsible for real or imagined wrongdoing committed by a single Jewish person or group, or even for acts committed by non-Jews.*
  - *Denying the fact, scope, mechanisms (e.g. gas chambers) or intentionality of the genocide of the Jewish people at the hands of National Socialist Germany and its supporters and accomplices during World War II (the Holocaust).*
  - *Accusing the Jews as a people, or Israel as a state, of inventing or exaggerating the Holocaust.*

---

<sup>114</sup> Julie Nathan, 2018. *Report on Antisemitism in Australia 2018*, Edgecliff, NSW: Executive Council of Australian Jewry, Online at <http://www.ecaj.org.au/wp-content/uploads/2018/11/ECAJ-Antisemitism-Report-2018.pdf>, accessed 12 December 2019.

<sup>115</sup> Gareth Milner, 2018. "First Week of University Tainted by Antisemitism and Discrimination", Australian Union of Jewish Students. Online at [http://www.aujs.com.au/o\\_week\\_antisemitism\\_statement](http://www.aujs.com.au/o_week_antisemitism_statement), accessed 12 December 2019.

<sup>116</sup> International Holocaust Remembrance Alliance, 2016. "Working Definition of Antisemitism" (press release), at <https://www.holocaustremembrance.com/stories/working-definition-antisemitism>, accessed 12 December 2019.

<sup>117</sup> Ibid.

<sup>118</sup> Ibid.



- *Accusing Jewish citizens of being more loyal to Israel, or to the alleged priorities of Jews worldwide, than to the interests of their own nations.*
- *Denying the Jewish people their right to self-determination, e.g., by claiming that the existence of a State of Israel is a racist endeavor.*
- *Applying double standards by requiring of it a behavior not expected or demanded of any other democratic nation.*
- *Using the symbols and images associated with classic antisemitism (e.g., claims of Jews killing Jesus or blood libel) to characterize Israel or Israelis.*
- *Drawing comparisons of contemporary Israeli policy to that of the Nazis.*
- *Holding Jews collectively responsible for actions of the state of Israel.*

---

The definition highlights that “criticism of Israel similar to that leveled against any other country cannot be regarded as antisemitic”, but that there are forms of antisemitism which manifest as a “targeting of the state of Israel, conceived as a Jewish collectivity”. The definition also highlights how “Antisemitism frequently charges Jews with conspiring to harm humanity, and it is often used to blame Jews for ‘why things go wrong.’”

Given the many forms antisemitism has taken throughout history, from racial to religious, political to personal, the IHRA’s Working Definition provides a helpful, accessible, and easy to understand aid to understanding the problem and classifying antisemitic manifestations. The fact it is based upon academic expertise and adopted in so many countries through democratic decision making further enhances its authority. The categories of common antisemitism outlined by the examples in the IHRA Working Definition will in this section of the report be applied to aspects of the Halle attack.

**RECOMMENDATION 9:** Those responding to antisemitic manifestations and incidents should make use of the International Holocaust Remembrance Alliance’s *Working Definition of Antisemitism*.

**RECOMMENDATION 10:** Australia should join with other IHRA member countries in formally adopting the International Holocaust Remembrance Alliance’s *Working Definition of Antisemitism* for domestic use.

### 3.2 Manifestations of Antisemitic in the Halle Attack

The antisemitic intent of the attack in Halle is clear and needs little explanation, however, a detailed consideration of the many antisemitic manifestations involved in the attack demonstrates the link between words and deeds, the link between hate speech and hate action. Understanding this link is important when it comes to recommendations and action to prevent further attacks. It may also have a bearing on the legal classification of certain expression as some expression may be considered part of the act of extremism rather than mere words.

#### 3.2.1 The objective, location and timing of the attack

The objectives of the attack, as listed in the *Dokumentation* part of the manifest, was to “Kill as many anti-Whites as possible, jews preferred”. Under the core of the IHRA definition the words themselves are a “rhetorical manifestation” of antisemitism and the attempted attack was a “physical

manifestation” of antisemitism, with both being directed against “individuals” “Jewish community institutions” and “religious facilities” as described in the core of the definition.

There is a further element of antisemitism in the objective. Jews are presented as the priority target within what the attacker called the “anti-whites”. This is the promotion of an antisemitic conspiracy theory about Jewish power and more specifically the conspiracy theory of “White Genocide” which says the Jews are behind a plot to “destroy the white race”.<sup>119</sup> The falls within the second of the examples in the IHRA Working Definition which speaks of “stereotypical allegations about Jews as such or the power of Jews as collective... especially but not exclusively, the myth about a world Jewish conspiracy”.

In “The Plan” part of the manifesto, a synagogue is listed as the first target and this target is chosen even after consideration is given to the high security and increased difficulty involved. The choice of target is justified in the manifesto over other potential targets, such as a “mosque or an antifa ‘culture center’” because “It’s the nearest location with a high population of Jews, simple as that”.

The timing was also designed to maximise the potential for harm to Jews. The manifesto states, “the best day of action should be Jom Kippur, because even ‘non-religious’ jews are often visiting the synagogue on this date”. “Jom Kippur” is the German language spelling of Yom Kippur,<sup>120</sup> and not an ironic misspelling like “jej”. Yom Kippur, also known as the Day of Atonement, is the holiest day in Judaism and often observed by more secular Jews who often do not observe other religious holidays,<sup>121</sup> as the manifesto noted.

The manifesto goes on to claim, “The only way to win is to cut of the head of the ZOG, which are the kikes”. This highlights how the choice of target was made with a deliberate and overriding aim of causing harm to “Jewish community institutes and religious facilities”, as per the core of the IHRA definition. It also repeats the second bullet point argument about “the power of Jews as a collective” and “the myth about a world Jewish conspiracy”, but this time goes further with a direct reference to “ZOG” (discussed in more detail shortly).

The final line of the plan section in the manifesto states, “if every White Man kills just one [jew], we win”. When this is taken alongside the objective to prove the viability of improvised weapons and to “increase the moral of other suppressed Whites”, it demonstrates an intent to directly inspire further killings of Jews in the name of a White nationalist ideolog. This is the first example of antisemitism in the Working Definition, “Calling for, aiding, or justifying the killing or harming of Jews in the name of a radical ideology”.

### 3.2.2 Racial slurs

A number of racial slurs are evident in the manifesto. They include “spilljuice”, “filthy jew”, “Kike”, and “Kikelett”. The use of slurs represents “rhetorical... manifestations of antisemitism... directed towards Jewish... individuals” as per the Working Definition and falls under the example of “Making mendacious,

---

<sup>119</sup> Julie Nathan 2018, “As the Pittsburgh synagogue massacre shows, fears of ‘White Genocide’ are incitement to murder”, *ABC Religion and Ethics* (29 October), at <https://www.abc.net.au/religion/white-genocide-is-incitement-to-murder/10442966>, accessed 12 December 2019.

<sup>120</sup> ‘Yom Kippur’, 2019. *bab.la*, at <https://en.bab.la/dictionary/english-german/yom-kippur>, accessed 12 December 2019.

<sup>121</sup> “Yom Kippur”, *Society for Humanistic Judaism*, at <https://shj.org/humanistic-jewish-life/about-the-holidays/yom-kippur/>, accessed 12 December 2019.



dehumanizing, demonizing, or stereotypical allegations about Jews” as the racial slurs are connected to these ideas.

As explained, “spilljuice” is a combination of an archaic word meaning “kill” or “destroy” with a pun of “Jews” popularised by the Hipster Hitler cartoon. The slur “filthy Jew” or “dirty Jew” in an antisemitic slur which suggest a physically and/or moral undesirability.<sup>122</sup> “Filthy Jew” was a theme in Nazi and Vichy propaganda.<sup>123</sup> Historically, it is linked to an antisemitic claim that Jewish blood was dirty and would contaminate wells and as recently as 1892 this idea led to Jews being quarantined during outbreaks of typhus and cholera and banned by law from German public swimming pools.<sup>124</sup>

The term “Kike” is a more recent antisemitic slur and one that emerged in the United States. It first appeared in print in 1919 in “The American Language: A Preliminary Inquiry into the Development of English in the United State” and is listed as one of the “common terms of disparagement” in American English,<sup>125</sup> and is described as a “characteristic Americanism”.<sup>126</sup> The term is thought to have originated with illiterate Jewish migrants on Ellis Island who refused to sign with a customary “x”, associating it with Christianity, and instead draw a circle, known as a *kikel* in Yiddish.<sup>127</sup> It is thought that the immigration inspectors began referring to anyone who signed with a circle as a “Kikel” or “Kike”.<sup>128</sup> In this context a “Kikelett” in the attacker’s achievement list refers to a “little Jew”, specifically a Jewish child. In a recent court filing the Anti-Defamation League explained that the word kike “has no singular definition but, rather, encapsulates and invokes the full range of anti-Semitic stereotypes, including beliefs that Jews are cheap, untrustworthy, conniving, powerful, rich, grasping, and malevolent toward non-Jews.”<sup>129</sup>

The variety of slurs used in the manifesto is an aspect of the antisemitic culture on /pol/. The results from the NCRI report on quantifying antisemitism online found that there was wide use of both classic antisemitic slurs and newly invented ones.<sup>130</sup>

### 3.2.3 The Greedy Jew trope

In the READ THIS FIRST document, the attacker spends most of the document complaining about an individual called Mark, who he calls a “filthy Jew” while noting a donation of 0.1 bitcoin he, the attacker,

---

<sup>122</sup> The top definition on urbandictionary.com for “Dirty Jew” claims there are Jews that lack a conscience or morals regarding business deals, which makes them “dirty”: ‘Dirty Jew’, *Urban Dictionary*, 2012., at <https://www.urbandictionary.com/define.php?term=Dirty%20Jew>, accessed 12 December 2019, accessed 12 December 2019.

<sup>123</sup> Margaret Anne Hutton, 2004. *Testimony from the Nazi Camps: French Women's Voices*. New York: Routledge, p. 313.

<sup>124</sup> Steven K. Baum, 2012. *Antisemitism Explained*. Maryland: University Press of America.

<sup>125</sup> Ibid, 115.

<sup>126</sup> Ibid, 155.

<sup>127</sup> Geoffrey Hughes, 2006. *Encyclopedia of Swearing: Social History of Oaths, Profanity, Foul Language, and Ethnic Slurs in the English Speaking World*. New York: M. E. Sharpe.

<sup>128</sup> This origin story is also relayed in the following novel: Mordecai Richler, 1991. *Solomon Gursky was Here*. London: Random House, p. 172.

<sup>129</sup> ADL, 2019. *Randy Ethan Halprin v. Lorie Davis*. Dallas, Texas: United States District Court, Online at <https://www.adl.org/media/13045/download>, accessed 12 December 2019.

<sup>130</sup> Joel Finklestein et al., 2018. *A Quantitative Approach to Understanding Online Antisemitism Part 2 : Temporal Analysis*. Network Contagion Research Institute. Online at <https://ncri.io/2018/09/06/a-quantitative-approach-to-understanding-online-antisemitism-part-2-temporal-analysis/>, accessed 12 December 2019.

received from this individual. The document asks, “why would a fucking jew give away money for free?”. This is a representation of the antisemitic stereotype that Jews are greedy, representing the second example of antisemitism provided in the IHRA definition.

This stereotype originated in the Middle Ages when Jews were forced out of many occupations and often into money-lending which Christians were forbidden by the church from engaging in. This gave rise to the stereotype of Jews being greedy or obsessed with money.<sup>131</sup> This antisemitic trope is used again in the achievements list in the manifesto where one achievement is titled “2 Kikes 1 Shekel”, Shekel referring to the currency used in both ancient Israel and the modern state of Israel. The word association also seems to imply that 2 Jews would fight over 1 shekel, reinforcing the stereotype.

This stereotype is contradicted by examples of Jewish philanthropy throughout the world. The Hebrew word *Tzedakah* means charity is a significant concept in Judaism.<sup>132</sup> Research into Jewish giving in America highlighted how the average Jewish household donated US\$2,526 per year to charity, significantly more than the average Protestant household at US\$1,749 or the average Catholic household at US\$1,142.<sup>133</sup> In addition to this is the charity from foundations. North American Jewish grant-making institutions contributed an estimated \$9 billion to charity each year with about 75% of it going to non-Jewish causes.<sup>134</sup> Then there are the mega-donors. The Forbes 400 in 2016 had at least 33 Jews on it and only about 11% of their giving went to Jewish causes.<sup>135</sup>

In Australia a number of the leading philanthropists in the country are Jewish and can be seen in the “Australian Philanthropy Top 350” list.<sup>136</sup> The list includes range of Jewish donors such as the Lowy Family, Besen Family, John Gandel and Pauline Gandel (Gandel Philanthropy), the Pratt Family (Pratt Foundation), Nora Goodridge (Goodridge Foundation), Smorgon Family, Hannah Cohen and family, Harry Triguboff, Bob Magid, David Gonski, Helen and Aron Kleinlehrer, and Penelope Seidler and the late Harry Seidler.<sup>137</sup> The list includes details of the recipients of the donations and while there are some Jewish causes lists, such as Jewish schools, most donations go to general causes in the fields such as higher education, the arts and medical research.

### 3.2.4 Holocaust denial

At the start of the attack in Halle the attacker states in his video that the Holocaust “didn’t happen”. Denying the Holocaust is the fourth example of antisemitism listed in the Working Definition, specifically “Denying the fact, scope, mechanisms (for example gas chambers) or intentionality of the genocide of the Jewish people at the hands of National Socialist Germany and its supporters and accomplices during World War II (the Holocaust).”

---

<sup>131</sup> Derek Jonathan Penslar, 2001. *Shylock's Children: Economics and Jewish Identity in Modern Europe*, Los Angeles: University of California Press, p. 16.

<sup>132</sup> Rabbi Hayim Halevy Donin, 1972. *To Be A Jew*. New York: Basic Books, p. 48.

<sup>133</sup> Hanna Shaul Bar Nissim, 2011. “American Jews and charitable giving: An enduring tradition”, *The Conversation* (11 December), at <https://theconversation.com/american-jews-and-charitable-giving-an-enduring-tradition-87993>, accessed 12 December 2019.

<sup>134</sup> Ibid.

<sup>135</sup> Ibid.

<sup>136</sup> Fundraising Research & Consulting, 2019. “Australian Philanthropy Top 350”, at <https://www.fundraisingresearch.com.au/top-donors.html>, accessed 12 December 2019.

<sup>137</sup> Ibid.

Holocaust denial was started by the Nazis themselves with organised disinformation campaigns even as the Holocaust was occurring.<sup>140</sup> Towards the end of the war Himmler ordered the destruction of records, the crematoria and evidence of the mass murders.<sup>141</sup> An order written in his own hand in April 1945, to prevent the spread of testimony, directs that no prisoner "fall into the hands of the enemies alive".<sup>142</sup> The denial continued after the Holocaust and occurred on both the political right and the political left.

Ein erschütterndes Dokument,  
dreissig Jahre später

14/9/45

Der Mensch braucht nicht in Angst  
zu leben, er darf zu leben.  
Der Mensch darf leben in der  
Friede der Erde, keine der Kette  
haben und glücklich sein in der Freiheit  
in der Welt zu leben.

- F. K. K.

*Figure 6 Order by Himmler stating that "Surrender is out of the question... No prisoner should fall into the hands of the enemies alive".*

144 Ibid.

In the manifesto's achievements list there is an example of Holocaust denial and trivialisation. The achievement "Anudda Shoa" for killing 6 Jews is a reference to the well-known death toll of approximately 6 million Jews killed in the Holocaust. The death toll of the Holocaust is often mocked by antisemites online, using phrases like "Muh Six Gorillion",<sup>145</sup> sometimes accompanied by the antisemitic meme of the Jew.<sup>146</sup> The achievement uses this theme, mockingly imitating a person saying "Another Shoah", with "Shoah" being a Hebrew name for the Holocaust.



Figure 7 Example of the "Muh 6 Gorillion Holocaust denial alongside a merchant meme

### 3.2.5 The ZOG Conspiracy Theory

As discussed previously, the acronym "ZOG", an abbreviation for "Zionist Occupied Government", is a common antisemitic trope in the Halle attack. It falls within the Working Definition's second example of conspiracy theories of "Jews controlling... government or other societal institutions". "Zionist" here simply means Jewish, though some use Israel and Jewish interchangeably seeing Israel as the manifestation of the Jewish collective. Where the allegation is made that it is Israel controlling world governments, under the Working Definition this could be seen as a form of antisemitic "targeting of the state of Israel, conceived as a Jewish collectivity", and not a "criticism of Israel similar to that leveled against any other country".

The term was popularised by an article in *The New York Times* on 27 December 1984 which concerned robberies carried out by a white supremacist group called The Order. These robberies were carried out to fund a war against the United States Government, which the order called "ZOG" or "Zionist Occupation Government".<sup>147</sup>

<sup>145</sup> 'Six Gorillion', ADL, at <https://www.adl.org/education/references/hate-symbols/six-gorillion>, accessed 12 December 2019.

<sup>146</sup> Andre Oboler, 2014. *The Antisemitic Meme of the Jew*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/the-antisemitic-meme-of-the-jew/>, accessed 12 December 2019.

<sup>147</sup> Brad Steiger & Sherry Steiger, 2013. *Conspiracies and Secret Societies: The Complete Dossier*. Mississippi: Visible Ink Press, p. 522.

In the attacker's achievements list ZOG appears again, this time when speaks about killing a "ZOG-bot", a term that has been used in conspiracy circles since at least 2008 to refer to police.<sup>148</sup> It is based on the idea the police are robots who will act as ordered by the Jews who the conspiracy theorists allege are controlling the government and its institutions. Given that the term "ZOG-bot" does not refer to Jews, this example demonstrates how, in the words of the Working Definition, a "rhetorical manifestation... directed towards... non-Jewish individuals" can still be a manifestation of antisemitism. In this case the term, while directed towards non-Jews, also promotes an antisemitic allegation about Jews.

In the post announcing the attack on meguca.org there is a line saying, "I would appreciate seeding, but only if your local ZOG won't van you for it." The reference to "van" in reference to the "party van" 4chan slang for police.<sup>149</sup> The use of van as a verb is a reference to being picked up by police and arrested. The idea the police would be acting under orders that come from Jews who are pulling the strings of government is explicit.

### 3.2.6 Redemptive Antisemitic Worldview

The beliefs expressed by the attacker converge to represent what can be described as a "redemptive" antisemitic worldview. The term "redemptive antisemitism" was coined by historian Saul Friedländer to describe antisemitic worldviews that could explain everything in the world and offer some kind of "redemption" for antisemites.<sup>150</sup> Redemptive antisemitic worldviews have existed in various forms throughout history, represented in the antisemitic text *The Protocols of the Elders of Zion*,<sup>151</sup> Nazi ideology, and the cultural Marxism conspiracy theory that claims the Jewish intellectualism masterminded a conspiracy to infiltrate and bring down Western cultural and social institutions.<sup>152</sup>

This worldview unites the various examples of antisemitism in the Halle attack. The Greedy Jew, Holocaust denial and ZOG conspiracy tropes converge into the idea of a worldwide Jewish conspiracy obsessed with gaining material wealth, through means such as falsifying the Holocaust, to fund their control over Western governments and their efforts to destroy the White race. This conspiracy theory, uniting all the Jews collectively into a target then provides a path to action and redemption for

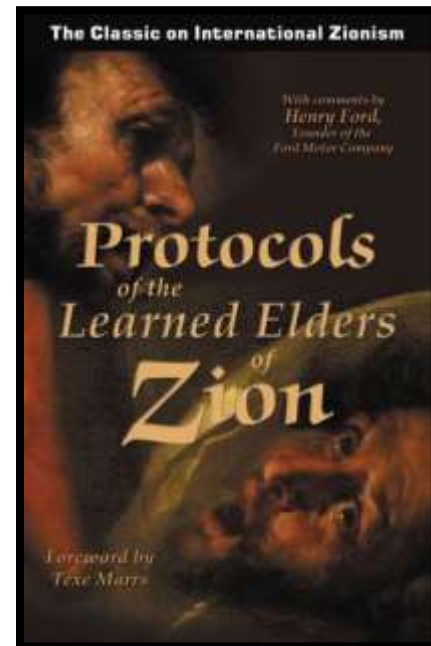


Figure 8 Modern example of the Protocols text.

<sup>148</sup> Dreglord, 2008. "Zogbot", Urban Dictionary, at <https://www.urbandictionary.com/define.php?term=Zogbot>, accessed 12 December 2019.

<sup>149</sup> Brad, 2009. "4chan", Urban Dictionary, at <https://knowyourmeme.com/memes/4chan-party-van>, accessed 12 December 2019.

<sup>150</sup> Saul Friedländer, 1997. *Nazi Germany and the Jews: Volume 1: The Years of Persecution, 1933-1939*. London: Orion Books, pp. 73-112.

<sup>151</sup> Currently available for purchase on Amazon and advertised with an explicitly antisemitic blurb, see: <https://www.amazon.co.uk/Protocols-Learned-Elders-Zion-Henry-ebook/dp/B004U7FK00>.

<sup>152</sup> Samuel Moyn, 2018. "The Alt-Right's Favourite Meme Is 100 Years Old", *The New York Times* (November 30), at <https://www.nytimes.com/2018/11/13/opinion/cultural-marxism-anti-semitism.html>, accessed 12 December 2019.

antisemites which the manifesto chillingly calls for when it say, “After all, if every White Man kills just one [Jew], we win.”

The redemptive antisemitic worldview also connects the other forms of discrimination displayed in the manifesto and attack. The achievements list includes goals for attacking Muslims, communists, “traitors” Christians, “ZOG-bots” and burning down a Mosque. However, antisemitism is the uniting factor and most significant form of discrimination in this worldview, as indicated by the decision to attack a synagogue rather than a “mosque or an antifa ‘culture center’, which are way less defended”.

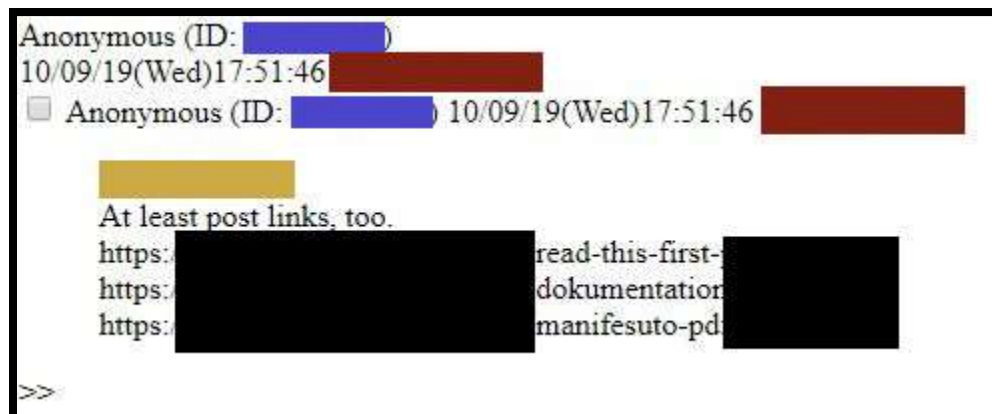
In the worldview of the attacker, the Jews are responsible for all the ills in society, and even though he discriminates to these other targets, he portrays them as “golems”, referring to anthropomorphic beings made from substances like clay in Jewish folklore.<sup>153</sup> However, this term is also synonymous in both Judaism and beyond for a mindless entity.<sup>154</sup> In this way, he alleges that all these other targets of discrimination are mindless enemies directed by the “Zionist Occupied Government”, and that to redeem the world, antisemites must “cut of the head of ZOG, which are the kikes”. This uniting factor is a unique quality to antisemitism, and represents the second and third examples of antisemitism in the Working Definition.

## 4 Responses to the Halle Attack

### 4.1 /pol/ and the Image Boards

#### 4.1.1 Use of /pol/ to Spread the Manifesto and Video

4chan's /pol/ board soon started a discussion on the attack. While not shared at the start of thread, it wasn't long before copies of the manifesto were being shared.



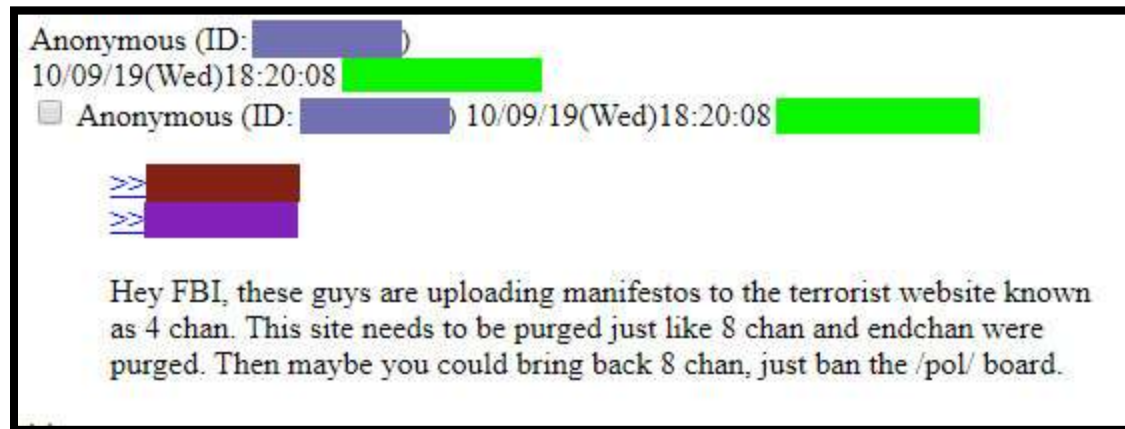
One posted responded suggesting 4chan should be shutdown and 8chan restored, but without /pol/. The poster writes, "Hey FBI, these guys are uploading manifestos to the terrorist website known as 4

<sup>153</sup> Moshe Idel, 1990. *Golem: Jewish Magical and Mystical Traditions on the Artificial Anthropoid*. New York: State University of New York Press.

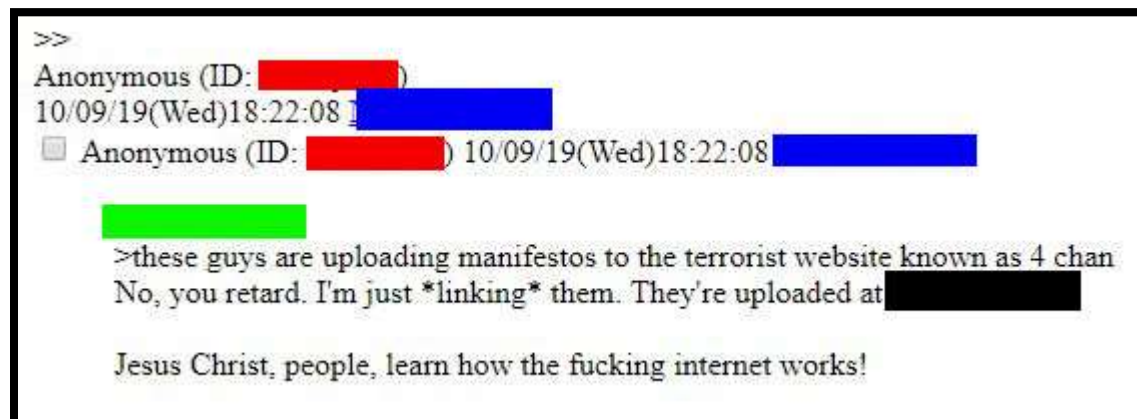
<sup>154</sup> Marilyn Cooper 2017, “Jewish Word | Golem: A Mutable Monster”, *moment* (17 July), at <https://momentmag.com/jewish-word-golem/>, accessed 12 December 2019.



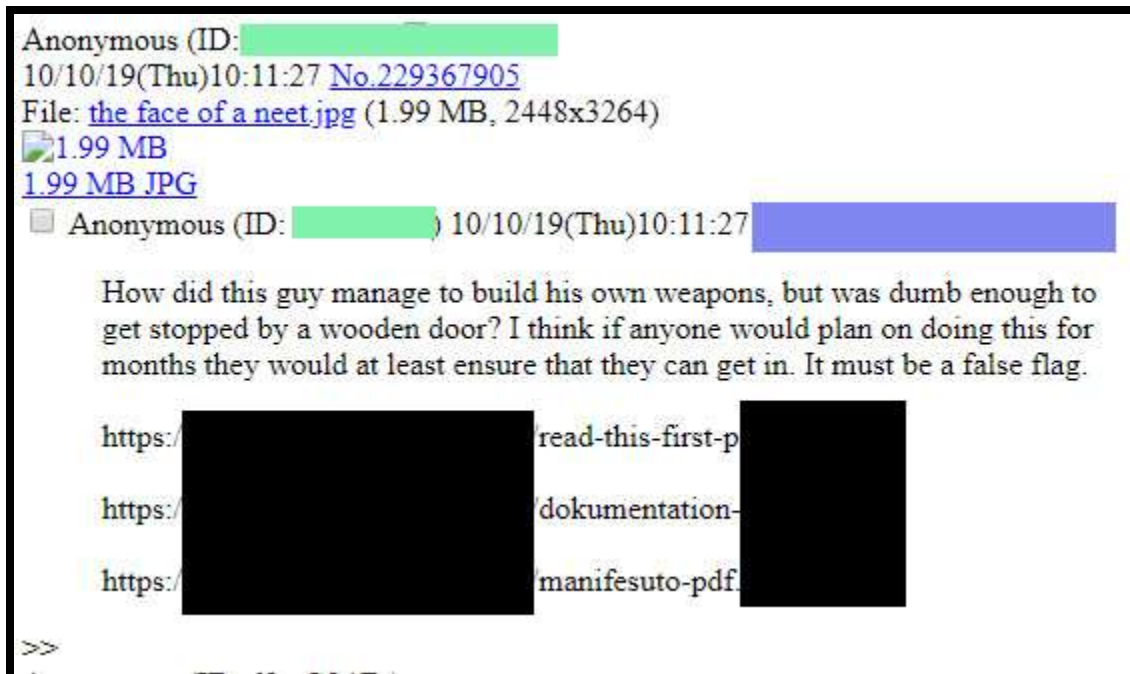
chan. This site needs to be purged just like 8 chan and endchan were purged. Then maybe you could bring back 8 chan, just ban the /pol/ board."



The response from the poster who shared links to the manifesto documents was to draw a distinction between posting links that promote terrorist material and uploading a copy of the material. Such a distinction is of little consequence when it comes to making terrorist material available. It makes the mistake of trying to apply ideas learned from copyright law (where a link would not be a copy) to other fields where the crime will usefully be facilitating the spread of the material.

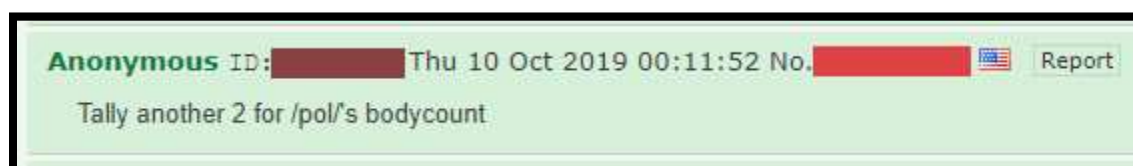


Multiple copies of the manifesto were uploaded to multiple threads over the next 48 hours and beyond.



Links to the video were also shared, the most common being to bitchute.com but it was not the only source.

The general sentiment on /pol/ was against Balliet, not because he was attempting a horrific crime, but because of what was seen as his ineptness at killing people. As one posted noted, however, "Tally another 2 for /pol/'s bodycount". While the first post was not on 4chan, and 8chan is currently down, these deaths are still a part of the /pol/ culture which has encouraged such violent extremism.



## 4.2 /pol/ Fake News and Trolling

On Wednesday night some on /pol/ on 4chan decided to use the tragic events to spread fake news and troll an unrelated person.

A threat with a link to a news article from the Washington Post was started with the added details that "Police report that a perpetrator of the attack on a synagogue in Halle has been arrested. The suspect is said to be Rainer W., known to the police, who had already been charged with incitement to hatred." The image used is of Rainer Winkler.



/pol/ - Politically Incorrect -
4chan
Index
NSFW
Ghost
Gallery
Stats

Search or insert post number



483x483 482x484 1570623882098.png  
View Same Google igdb SauceNAO Trace

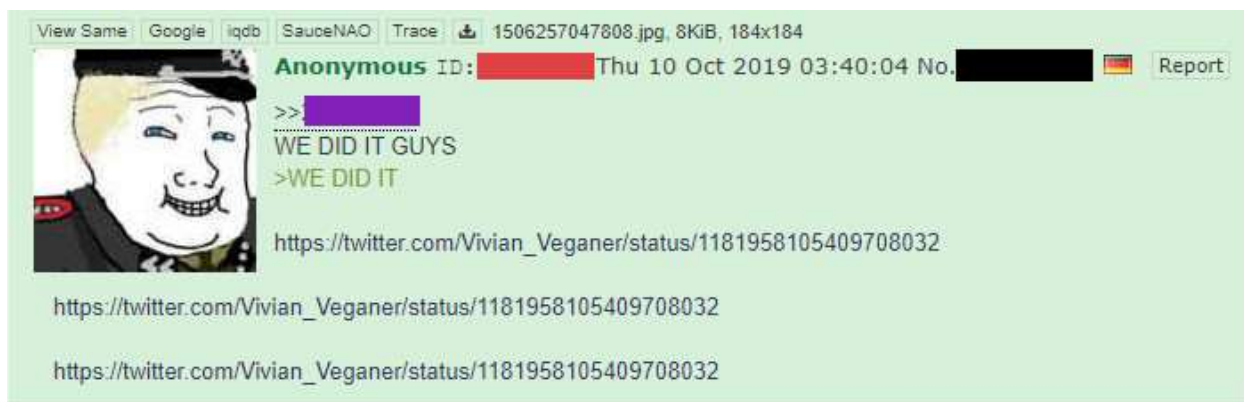
**TERRORIST IN GERMANY WAS FOUND** Anonymous ID: [REDACTED] Wed 09 Oct 2019 [163 / 35 / 103]  
23:26:44 No. [REDACTED] 80 View Reply Original Report  
Quoted By: [REDACTED]

Police report that a perpetrator of the attack on a synagogue in Haale has been arrested. The suspect is said to be Rainer W., known to the police, who had already been charged with incitement to hatred.  
[https://www.washingtonpost.com/world/shooting-near-synagogue-in-germany-leaves-at-least-two-people-dead-police-say/2019/10/09/08214514-ea89-11e9-9306-47cb0324fd44\\_story.html](https://www.washingtonpost.com/world/shooting-near-synagogue-in-germany-leaves-at-least-two-people-dead-police-say/2019/10/09/08214514-ea89-11e9-9306-47cb0324fd44_story.html)

Anonymous ID: [REDACTED] Wed 09 Oct 2019 23:29:07 No. [REDACTED] 80 Report  
Quoted By: >> [REDACTED]  
Typical nazi

Winkler, who goes by the handle Drachenlord (Dragon Lord) is a German streamer, YouTuber and heavy metal fan. His [YouTube Channel](#) has over 11 million subscribers. He has been the subject of serious trolling. A female troll pretended to be interested in him, then when he proposed in a live stream, shot him down. He responded to the trolling and abuse by publishing his address and daring people to come try it in person. The result was the creation of a pilgrimage for trolls to visit him in groups. Some shouted abuse, some smashed windows, some threw eggs. In [August 2018 a mass pilgrimage](#) was called in which 10,000 people said they would attend. Local police declared a multi-day ban on public assemblies. As many as 800 people, mostly adolescent, defied the ban. They came from as far away as Northern Germany, Austria and Switzerland. It took the reallocation of special security forces from a German football championship match to restore order.

In this instance oe24TV started using the image of Winkler in coverage about the attack. This was quick shared via Twitter and victory was claimed in the same 4chan thread.



This is not the first time /pol/ has tried to troll Winkler with fake news during a fatal attack. *Hope Not Hate* in the UK had reported how his images was also used during the Parkland shooting.

#### 4.3 Misidentification of Kohlchan

The International Centre for the Study of Radicalisation at Kings College (UK) originally claimed that Balliet shared the documents through Kohlchan, a German equivalent to 4chan. An update to the

articles notes, that the Centre later amended that claim and correctly pointed to the meguca.org imageboard as the source.

As of October 22, 2019 Kohlchan is still down with a notice stating that after analysis they have concluded this had nothing to do with them. They highlight how the incorrect information went viral through the mainstream media and also point to a news article which provides the correct information.

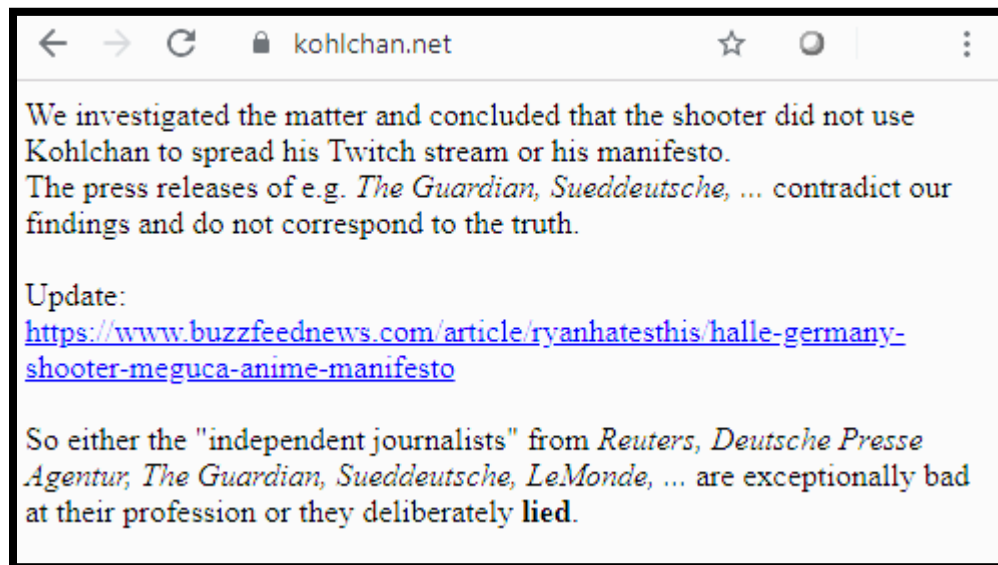


Figure 9 Kohlchan announcement

#### 4.4 Response from the Technology sector

Concerns with the way social media platforms moderate user content has been a high profile issue since 2008 when Facebook was first challenged over antisemitism,<sup>155</sup> and then specifically over Holocaust denial material.<sup>156</sup> After initial opposition, the complaints about Holocaust denial material eventually led to what is now the standard practice of geo-blocking content so that material prohibited by national laws in a country is not shown to users whose IP addresses indicate they are visiting from that country.<sup>157</sup>

Traditionally technology platforms have responded to incidents on their platforms individually and with little cooperation. Terms of service vary widely when it comes to prohibiting hate speech. Randi Zuckerberg, then Facebook's marketing director and spokesperson (and sister of founder Mark Zuckerberg) said it was "Facebook's policy to not remove groups that deny the Holocaust" back in

<sup>155</sup> Andre Oboler, 2008. *Online Antisemitism 2.0: "Social Antisemitism on the Social Web"*. JCPA: Post-Holocaust and Antisemitism Series (April 2008, No. 67). Jerusalem, Israel: Jerusalem Center for Public Affairs. Online at, at <http://jcpa.org/article/online-antisemitism-2-0-social-antisemitism-on-the-social-web/>, accessed 12 December 2019.

<sup>156</sup> Andre Oboler, 2008. *Facebook, Holocaust Denial, and Anti-Semitism 2.0*. JCPA: Post-Holocaust and Anti-Semitism. Jerusalem, Israel: Jerusalem Center for Public Affairs. Online at <http://jcpa.org/article/facebook-holocaust-denial-and-anti-semitism-2-0/>, accessed 12 December 2019.

<sup>157</sup> Ibid.

2009,<sup>158</sup> a position she has continued to promote in recent years, long after leaving Facebook.<sup>159</sup> YouTube had taken a similar stand but reversed its policy in June 2019 saying it would now remove videos that deny “well-documented violent events” such as the Holocaust and school shootings.<sup>160</sup>

Under increasing pressure from governments to do more to tackle extremism, technology companies have begun working closer in tackling terrorism since 2017. This pressure has significantly increased since the Christchurch attack in March 2019 and under the Christchurch Call which governments and technology companies have signed up to support. Halle marked the first time a more formal and systematic collective response was put into action. Data from that collective effort identified 36 visually-distinct videos across multiple platforms.<sup>161</sup> This section examines the response to the Halle incident by a range of technology platforms.

#### 4.4.1 Twitch

Twitch’s first public response to the Halle attack can be seen in series of tweets made at 1:30am Central European Time (CET) on October 9<sup>th</sup>, around 13.5 hours after the attack started. A further update with some corrections was provided in a series of tweets on October 17<sup>th</sup>. The times and dates in the images provided in this section reflect the local time in Melbourne, Australia, for each Tweet.

The [first tweet](#) expressed the company's shock and condolences for the victims. It was liked over 12,442 times and retweeted over 1,579 times.



Figure 10 Twitch’s first tweet after the attack

<sup>158</sup> Michael Arrington, 2009. “Facebook Employees Speak Their Mind On Holocaust Denial”, *TechCrunch* (16 June), at [www.techcrunch.com/2009/06/15/facebook-employees-speak-their-mind-on-holocaust-denial/](http://www.techcrunch.com/2009/06/15/facebook-employees-speak-their-mind-on-holocaust-denial/), accessed 12 December 2019.

<sup>159</sup> Laurie Segall, 2018. “Exclusive: Randi Zuckerberg responds to her brother's Holocaust comments”, *CNN Business* (19 July), at <https://money.cnn.com/2018/07/19/technology/randi-mark-zuckerberg-facebook-holocaust/index.html>, accessed 12 December 2019.

<sup>160</sup> Reuters, 2019. “YouTube Bans Holocaust Denial Videos in Policy Reversal”, *VOA News* (07 July), at <https://www.voanews.com/silicon-valley-technology/youtube-bans-holocaust-denial-videos-policy-reversal>, accessed 12 December 2019.

<sup>161</sup> GIFCT, 2019. *Update to GIFCT Statement on Halle Shooting*. Global Internet Forum to Counter Terrorism. Online at <https://gifct.org/press/gifct-statement-halle-shooting/>, accessed 12 December 2019.

The second tweet stated the company has a "zero-tolerance policy against hateful conduct, and any act of violence is taken extremely seriously".<sup>162</sup> They stated that they acted with urgency to remove the content and "will permanently suspend any accounts found to be posting or reposting content of this abhorrent act." That post received 4,594 likes and 398 retweets.

A later tweet from October 17<sup>th</sup> (CET) indicates that it was not until 5:50 pm CET, almost 6 hours after the live streaming of the attack started, that the video was in fact removed and the associated channel suspended.<sup>163</sup> From the information provided in the fourth Tweet from October 9<sup>th</sup>,<sup>164</sup> it appears the delay in removal may have been a result of the video not being reported by other users until around the time it was removed.

Without knowing exactly when the video was first reported to Twitch, and therefore at what point they became officially aware of the video on their platform, it is impossible to know how quick their response was and whether the claim that they "worked with urgency" is in fact accurate.

**RECOMMENDATION 11:** When a violent extremist attack is livestreamed the platform that was

used to stream the incident and / or host the initial video of the incident should provide transparency on exactly when the livestream and/or video was first reported to them and when exactly they acted to remove it.

**RECOMMENDATION 12:** Platforms should take all reasonable steps to facilitate and encourage the reporting of material depicting and promoting violent extremism, as well as all other reasonable steps to identify such material themselves. They should expeditiously remove such material once they become aware of it. Provided the above steps are taken, there should be a clear safe harbour, protecting platforms from liability for material they are unaware they are hosting.



Figure 11 Twitch's second tweet after the attack

<sup>162</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1182000480349605889>, accessed 12 December 2019.

<sup>163</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1185200174953455620>, accessed 12 December 2019.

<sup>164</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1182036268202381313>, accessed 12 December 2019.



The third gave the initial information suggesting around 5 people viewed the attack live and that the video lasted 35 minutes,<sup>165</sup> as mentioned this was later revised to 3 people having watched it live.<sup>166</sup>

The fourth tweet noted that a video was automatically saved from the livestream that in the 30 minutes before it was flagged and removed by Twitch staff 2200 people had seen it.<sup>167</sup> Further details on this were provided on October 17<sup>th</sup> highlighting that in addition to the 2200 who saw it in the half an hour before it was removed, a further 333 had seen the video prior to this.<sup>168</sup>

Twitch goes on to note that "This account was created about two months prior to streaming the shooting and had attempted to stream only once before."<sup>169</sup> Their investigation noted that the video was not appearing in any recommendations or directories, meaning that the viewers were not a result of internal promotion on Twitch but rather of external sharing of the link outside Twitch. They state, "our investigation suggests that people were coordinating and sharing the video via other online messaging services."<sup>170</sup>

Twitch noted that they shared the hash (a digital signature which can be used to identify digital content) of the video with an "industry consortium" that works to prevent such content being spread. Later posts on the 18th of October named the consortium as GifCT. Twitch is not directly a GifCT member, but its parent company Amazon is one of the members.



Figure 12 Twitch's third tweet after the attack



Figure 14 Remainder of the October 9 tweets from Twitch

<sup>165</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1182036266344271873>, accessed 12 December 2019.

<sup>166</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1185200174953455620>, accessed 12 December 2019.

<sup>167</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1182036268202381313>, accessed 12 December 2019.

<sup>168</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1185200176006230016>, accessed 12 December 2019.

<sup>169</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1182036269519368193>, accessed 12 December 2019.

<sup>170</sup> 'Twitch', *Twitter*, at <https://twitter.com/Twitch/status/1182036270710571009>, accessed 12 December 2019.

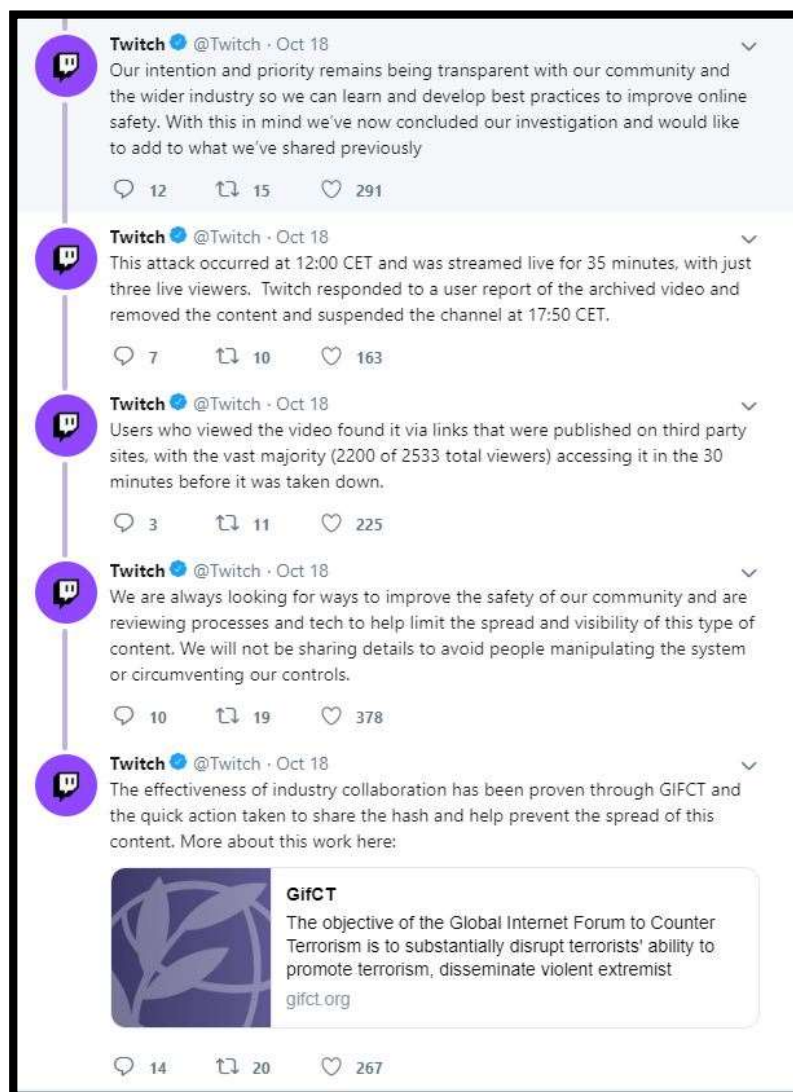


Figure 15 Twitch tweets from October 17 (CET)

#### 4.4.2 Telegram

Copies of the video were distributed through the encrypted messenger app Telegram.<sup>171</sup> Prof. Megan Squire first reported the spread of the video to Telegram, noting that in public channels she monitored there were two primary sources, one for the long video and the other for a short version.<sup>172</sup> These sources were in turn amplified by smaller public channels. Four of the small channels only shared the long video while five shared both the long and short videos. She estimated the total potential audience was around 15,625 accounts on those 9 channels at that time, though there may be some overlap with people being in more than one of these channels.

<sup>171</sup> Tom Cleary, 2019. "Stephan Balliet: 5 Fast Facts You Need to Know", *heavy*. (09 October), at <https://heavy.com/news/2019/10/stephan-balliet/>, accessed 12 December 2019.

<sup>172</sup> MeganSquire0, 2019. *Twitter*, at <https://twitter.com/MeganSquire0/status/1181980782417633280>, accessed 12 December 2019.

On December 14, 2019, Prof. Squire provided us with a screen capture showing that the long version of the video was still on Telegram and had been viewed around 99,700 times. The short version has been removed by original poster, which reset the counter to 1, but it remains available via those who had shared it.

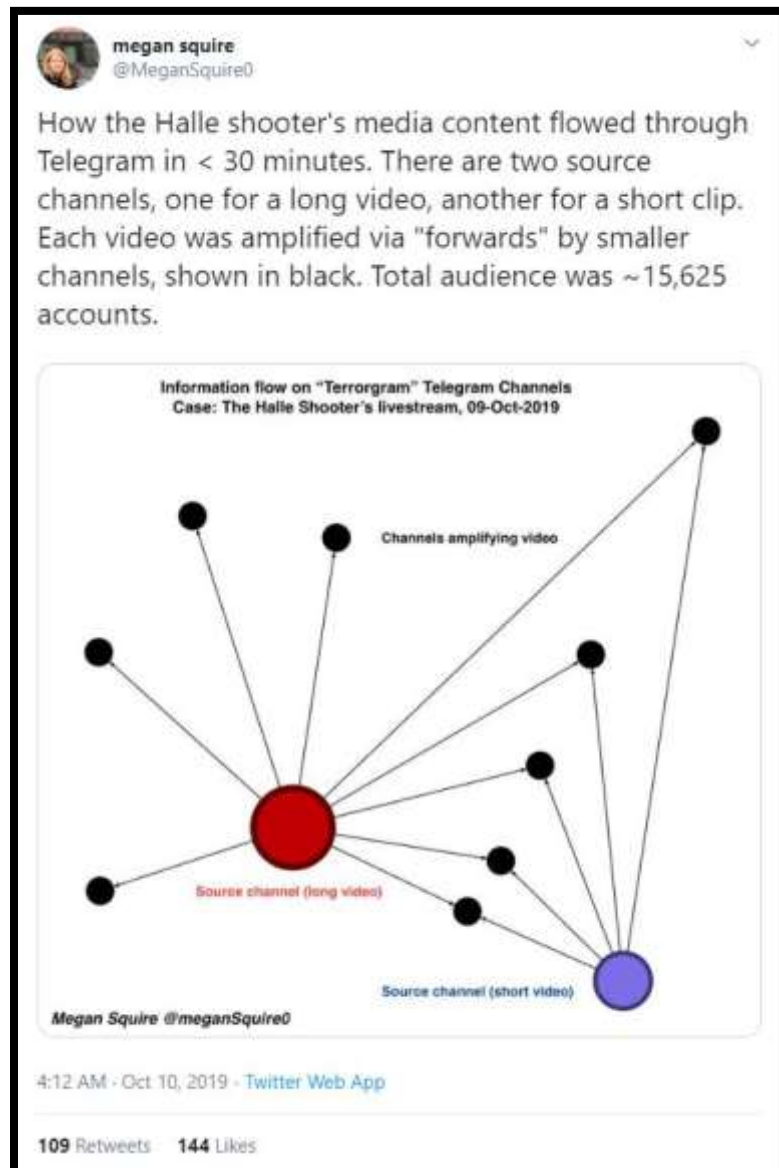


Figure 16 Prof. Megan Squire documents the spread to Telegram

Much of the discussion around Telegram and terrorism previously focused on government calls to compromise encryption, it is important to stress that this use of Telegram was in public groups which both researchers and law enforcement could monitor without the need to compromise encryption. The fact the video remains available via Telegram is concerning.



RECOMMENDATION 13: Telegram should join GIFCT and implement a system to remove videos from its platform which are registered in the GIFCT Hashing database.

#### 4.4.3 Google

Preliminary work we carried out after the attack identified copies of the three manifesto documents on a range of internet sites as well as two links allowing access to view the attacker's video. Some of the manifestos were found by monitoring /pol/ and other sites, but others were found through a Google search. We contacted our liaison at Google to discuss this and were urged to file an online report.

In completing the form we noted:<sup>173</sup>

---

*the Christchurch Call and Google's Commitment to "Prioritising moderation of terrorist and violent extremist content, however identified". In light of this commitment, we urge Google to voluntarily remove links to this content rather than allowing this material advocating terrorism to remain online [until] formal government take down action occurs. We note this content related to a GIFCT Content Incident Protocol incident.*

---

Google responded to our online submission three days after we made it. The response highlighted that, "Google aggregates and organizes information published on the web; we don't control the content found in the pages you've specified". They went on to note that "in accordance with Google's practices concerning content removal, the following URLs will be removed shortly from Google's search results for Australia". This only covered the links to the video, not the other links to copies of the manifesto. Google rejected one link, a blog post that included links to PDFs uploaded as blog content. One link Google correctly rejected as by the time they looked at it the content has been removed. The remaining links, including the links to the uploaded files at the blog, google requested further information on.

While Australia's Abhorrent Violent Material laws only require a hosting or content services to remove Abhorrent Violent Material, not links to that material, the *Broadcasting Services Act 1992* (Cth) goes further and has provisions relating to "link services" such as search engines.

Link services can be issued a take-down notice by the eSafety Commissioner to remove their links to prohibited content so long as the service has an "Australian connection".<sup>174</sup> The Act defined "Australian connection" for content services and in a note states that "a link is an example of content", meaning link services are content services for the purpose of deciding if they have an Australian connection. A service has an Australian connection if "any of the content provided by the content service is hosted in Australia".<sup>175</sup> It's been known since 2010 that some of Google's content was being served from within

---

<sup>173</sup> Report to Google 25 October 2019.

<sup>174</sup> *Broadcasting Services Act 1992* (Cth) Sch 7 Pt 3 Div 5.

<sup>175</sup> *Broadcasting Services Act 1992* (Cth) Sch 7 s 3.

Australia,<sup>176</sup> and since 2017 Google has also offered cloud services hosting in Sydney.<sup>177</sup> Google therefore has an Australian connection and can be subjected to take-down orders both for hosting prohibited content and for linking to it.

Google's distinction that they do not host the content they link to does not reduce their liability when they host links that point to prohibited content. We tried explaining this to Google and noted that the terrorist manifestos they were linking to would have to be classed as prohibited content if they were referred to the Classification Board.<sup>178</sup> In their response Google asked us to:<sup>179</sup>

---

*Please copy and paste, or clearly identify, the exact text or content you claim violates applicable law. Also, please explain the specific reasons why you believe the text or content violates or is illegal under applicable law. It would be helpful if you could cite the specific law(s) of your country you believe to be applicable to the content in question.*

---

In our reply we highlighted that three of the links were to copies of the same document (the "DoKumentation" part of the manifesto) hosted in different places. We explained that the document contained "Terrorist instruction material on page 9" and cited a passage saying "Most grenades are filled with a simplified formula of [redacted] from the book [redacted] made as followed: [redacted]". We gave the passage in full without the redactions. We then added "State objective of violence on page 9: '3. Kill as many anti-Whites as possible, jews preferred'" and "Incitement for others to copy this stated violence on page 10: 'The only way to win is to cut of the head of ZOG, which are the kikes. If I fail and die but kill a single jew, it was worth it. After all, if every White Man kills just one, we win.'"

The response from Google also included some standard boiler plate which is perhaps not the best advice to be giving people in relation to content promoting terrorism:<sup>180</sup>

---

*Even if we eliminated the page from our search results, it would still exist on the web. We encourage you to resolve any disputes directly with the owner of the website in question. Please visit <https://support.google.com/websearch/answer/9109> to learn how to contact a site's webmaster and request a change.*

---

More than two weeks after providing the information most of the links to the manifesto still appear in Google search results. The blog post is still there, but the links to content on it no longer appear in

---

<sup>176</sup> Brett Winterford, 2010. "Found: Google Australia's Secret Data Network", *ITnews* (5 March), at <https://www.itnews.com.au/news/found-google-australias-secret-data-network-168772>, accessed 12 December 2019.

<sup>177</sup> <https://www.cio.com.au/article/620891/google-opens-sydney-cloud-region/>, accessed 12 December 2019.

<sup>178</sup> This is required under s 9A of the *Classification (Publications, Films and Computer Games) Act 1995* (Cth).

<sup>179</sup> Response from Google 28 October 2019.

<sup>180</sup> *Ibid.*

Google. On further examination, the blog post itself now had three deadlinks. The documents that were uploaded to the blog show up with error messages. An examination of the hosting provider shows the blog was using Cloudflare's Content Delivery network. Given the recent statement by Cloudflare's CEO,<sup>181</sup> it appears likely it was action by Cloudflare to cease providing access to copies of these manifestos that has caused the files to vanish.

Google seeks to draw a distinction between hosting content and search saying the Christchurch Call does not apply to its search services. That position will be seen by many as a step backwards and we would urge all parts of Google to fully commit to combating terrorism. There should be no exceptions.

**RECOMMENDATION 14:** Google should commit to supporting the "Christchurch Call" across all parts of the business without exception. This includes preventing Google's search engine being used to access material promoting terrorism.

#### 4.4.4 GIFCT's Responsive Action

In July 2017 four of the largest technology companies, Facebook, Microsoft, Twitter and YouTube, decided to work together in their efforts to tackle terrorism.<sup>182</sup> The collective effort was called the Global Internet Forum to Counter Terrorism (GIFCT) and while others have been invited to join the project, membership is "limited to companies operating internet platforms and service".<sup>183</sup>

During this incident GIFCT for the first time activated its new Content Incident Protocol (CIP). A timeline of the action taken has been published to provide transparency and to help further improve the protocol.<sup>184</sup>

The first communications between the GifCT founding members (Facebook, Microsoft, Twitter and YouTube) occurred at 5am Pacific Time which is 2pm in Germany. That is two hours after the incident started and around 1.5 hours after it stopped being live streamed. At this stage the communications were triggered because of eye witness accounts that the attacker was wearing video equipment and which made it likely there was a livestream, but the platform in use was unknown.

Four and quarter hours later, more than 6 hours after the attack started, GifCT became aware of the video circulating on non-GifCT platforms. 54 minutes after this they formally declared it a Content Incident Protocol event and for the first time activated the agreed protocols. Those protocols involved:

---

#### 1. Alerting all members of the GIFCT that an active CIP was underway

---

<sup>181</sup> Matthew Prince, 2019. "Terminating Service for 8Chan", *Cloudflare Blog* (5 August), at <https://blog.cloudflare.com/terminating-service-for-8chan/>, accessed 12 December 2019.

<sup>182</sup> GIFCT, 2019. *Global Internet Forum to Counter Terrorism: Evolving an Institution*. Global Internet Forum to Counter Terrorism. Online at <https://gifct.org/about/>, accessed 12 December 2019.

<sup>183</sup> Ibid.

<sup>184</sup> GIFCT, 2019. *Update to GIFCT Statement on Halle Shooting*. Global Internet Forum to Counter Terrorism. Online at <https://gifct.org/press/gifct-statement-halle-shooting/>, accessed 12 December 2019.

- 2. Uploading hashes of the attacker's video, its derivatives, and other related content into the shared GIFCT hash database with a dedicated label to enable quick identification and ingestion by GIFCT member companies*
  - 3. Alerting the German government and Europol that an active CIP was underway*
  - 4. Continuing communications among GIFCT founding members to identify and address risks and needs during the active CIP*
  - 5. Establishing the timing of a Situational Awareness Interval when GIFCT would be able to share some detail of the CIP with impacted governments*
- 

The CIP event ended 22 hours later when the volume of attempts to upload the content to member platforms had significantly reduced. GifCT noted how in this instance only "36 visually-distinct videos" edits of the video emerged, far less than occurred with Christchurch.<sup>185</sup> In Christchurch there had been more than 800 distinct edits of the attacker's videos and Facebook alone had removed 1.5 million copies of it.

The GIFCT response is commendable, but being the first time there is room for further improvement. It is unclear how long Twitch knew about the content before GIFCT was notified. The provision of a 24/7 hotline for use by any technology company, whether or not they are member, and the promotion of this hotline within the sector may help to speed up responses in the future.

It also appears only the video was being tackled by GIFCT when the manifesto documents also deserve attention. Finding these documents is in many ways easier than finding different variants of the video. GIFCT should ensure manifesto material is included in its activities.

As content is more rapidly removed there will be a growing need for researchers from government, academia and civil society to be able to access terrorist material for research purposes. GIFCT is well placed to maintain an archive of such content and to accept, perhaps as associate members, researchers who after vetting could have access to that archive.

Finally, we note the work does not end when the incident ceases to be in the media. Based on information provided to us by Facebook, between 15 March to 30 September 2019 Facebook removed 4.4 million pieces of content related to the Christchurch attacks. 97% of the items were removed proactively, that is by automated systems without a user having to report them. There are now 800 known video derivatives of the Christchurch video according to Facebook. While subsequent attacks have been far less viral, the continued impact of this content, and continued efforts to share it are a cause for concern.

---

<sup>185</sup> GIFCT, 2019. *Update to GIFCT Statement on Halle Shooting*. Global Internet Forum to Counter Terrorism. Online at <https://gifct.org/press/gifct-statement-halle-shooting/>, accessed 12 December 2019.

**RECOMMENDATION 15:** Through the Global Internet Forum to Counter Terrorism (GIFCT), technology companies should provide a contact mechanism that is staffed 24/7 and available to assist any platform whose technology is abused to share manifestos or live streaming.

#### 4.4.5 The Tech Sectors Response in General

Tech Against Terrorism, a London based NGO, is an initiative launched by the United Nations Counter Terrorism Executive Directorate (UN CTED) in April 2017. They aim to support the global technology sector in responding to terrorism and have a particular focus on supporting smaller technology platform. They are a global forerunner in advocating for appropriate disclosures by platforms which have been exploited by terrorists. Following the Halle attack, Tech Against Terrorism provided analysis via e-mail and on their website of the technology sector's response to the incident.

The Tech Against Terrorism analysis was released on October 15<sup>th</sup>, 2019.<sup>186</sup> In their analysis, Tech Against Terrorism noted how many large and small platforms worked to prevent the spread of the content but state that the "response by smaller tech platforms and larger tech platforms to prevent virality are being undermined by both the mainstream media and fringe platforms." They also noted the use of both Twitter and Telegram to spread the video.

The analysis provided the best information available at the time it was released, though some of the information was later disproven. For example, the briefing claims the initial message was posted on Kohlchan, based on early reports from the International Centre for the Study of Radicalisation, when it was actually posted on Meguca.org (a fact the International Centre for the Study of Radicalisation later corrected). Similarly, the briefing claimed Twitch removed the content within 30 minutes, when in reality it took longer to 6 hours. This was a result of a tweet Twitch made which, while accurate, was also misleading. A tweet from Twitch some weeks later corrected the information (see section 4.4.1). We commend Tech Against Terrorism for their work collating information during the incident. We also note the need for greater cooperation between technology platforms and civil society to ensure accurate facts and analysis. There is also a need to update and correct information when it is later found to be inaccurate. Tech Against Terrorism have indicated they would like to be able to keep their online content updated as news evolves, but there are workload difficulties that occur, particular around the time of a major incident. Tech Against Terrorism is undertaking important work and greater support from donors for both their operations and communications work would be beneficial.

Another issue we noted is that the analysis, which was openly available through their website, listed a range of services where copies of the manifesto and videos could be accessed. While direct links to the content were avoided, naming the platforms still had the unfortunate effect of increasing the risk of the terrorist content spreading. In discussing this with Tech Against Terrorism they explained that the decision to go public occurred after a careful consideration and was a result of the platforms concerned (4chan, BitChute, and Kiwifarms) being repeat offenders who refused to remove manifestos and videos of terrorist content despite many requests for moderation. In making the decision they weighed up the need to prompt the platforms for action, with a consideration of the notoriety of the platforms and whether they would be introducing them to new users as means to access the content. Our own

---

<sup>186</sup> Tech Against Terrorism, 2019. *Analysis: What can we learn from the online response to the Halle terrorist attack?*. Online at <https://www.techagainstterrorism.org/2019/10/15/analysis-what-can-we-learn-from-the-online-response-to-the-halle-terrorist-attack/>, accessed 12 December 2019.

practice and recommendation for civil society organisations is usually to circulate such details confidentially to key stakeholders and avoid naming platforms until the content is no longer available there. There is a point where this is no longer viable, and we have ourselves followed Tech Against Terrorism's approach in naming Telegram as a platform that continues to host the video months after the attack. We would still, however, recommend not naming platforms currently hosting terrorist content, such as videos and manifestos, while an attack is in the media spotlight.

Tech Against Terrorism also mentioned the *Terrorist Content Analytics Platform (TCAP)* which they are developing with the support of Public Safety Canada to share data between platforms, academia, and data scientists. The system will also serve as an archive to help with the development of automated content classifiers. We welcome this development.

**RECOMMENDATION 16:** Access to the *Terrorist Content Analytics Platform* should be available to researchers after they are vetted to ensure they represent legitimate research efforts in government, academia or civil society.

**RECOMMENDATION 17:** The *Terrorist Content Analytics Platform* or a similar service should offer a tool for archiving and preserving online content for use by law enforcement and in legal proceedings. Adding content should be available to the public, but accessing archived content should be restricted to vetted people from government, academia and civil society.

**RECOMMENDATION 18:** Civil society organisations should redact or avoid naming hosting services that are making terrorist content available, but should confidentially report such content to key stakeholders in government, industry and civil society.

**RECOMMENDATION 19:** All companies that allow hosting of user generated content should have a process to receive reports from the public related to material promoting terrorism and this process should ensure rapid review.

## 4.5 Government Action

Germany has taken an international lead in tackling online hate speech over the last few years, and has proposed further law reform in response to the Halle attack. Australia has enacted world leading legislation to tackle the live streaming of abhorrent acts in response to the attack in Christchurch. In this section we examine how these countries responded to the online elements of the Halle attack. In making our recommendations here we have considered the doctrinal principles previously outlined in section 1.2.4.

### 4.5.1 Germany

Justice Minister Christine Lambrecht highlighted the connection between online incitement to hate and extremist violence saying, "What the disinhibition and unleashing of hatred in the net can lead to was shown again in the terrible attack on the Jewish community in Halle".<sup>187</sup>

---

<sup>187</sup> Kate Brady, 2019. "Germany announces plans to combat far-right extremism and online hate speech", *DW News* (30 October), at <https://www.dw.com/en/germany-announces-plans-to-combat-far-right-extremism-and-online-hate-speech/a-51049129>, accessed 12 December 2019.

Germany passed strong laws back in June 2017 requiring platforms to remove hate speech within 24 hours if its illegality was obvious and within 7 days when the determination was more difficult to make.<sup>188</sup> Failure would leave companies facing fines of up to €50 million.<sup>189</sup> While announcing the move in 2017 Justice Minister Heiko Maas said that "Death threats and insults, incitement to hate or (Holocaust denial) are not part of freedom of expression -- rather, they are attacks against other people's freedom" and "intended to intimidate and mute others".<sup>190</sup>

Following the Halle attack the Germany Government announced they would go further, creating new laws requiring platforms such as Facebook, YouTube and Twitter to report incidents of hate speech and the IP address of those who post them to government authorities.<sup>191</sup> A spokesperson for Germany's Data Protection Commission said it was "too early to say whether this is good or bad" but that, "there will certainly be questions to be asked regarding the ethics of private companies deeming what counts as a conspicuous post on social media."<sup>192</sup>

Companies make such judgements all the time when it comes to enforcing their own terms of service, the difference here is the involvement of the state and the possibility of a company's action leading to criminal sanctions. If a store has CCTV and someone commits a crime against the store, for example stealing, the store would have no difficulty in reporting the matter to police and handing over the CCTV footage. Similarly, if a customer was assaulted by another customer while in the store, the company would have no difficulty handing over CCTV footage to police. On the other hand, a customer swearing at another customer, even if captured on CCTV and potentially subject to a fine for disorderly conduct, would be unlikely to be reported. The question is simply where the line is drawn.

In Germany the line indicating hate speech is fairly clear, given platforms are already under an obligation to identify and remove such content. The question is what level of hate speech should be reported. Rather than a blanket report of every incident, a move which would overwhelm state resources and essentially treat major and minor offenses the same, we recommend that "a combination of sanctions, training, and educative efforts should be put in place".<sup>193</sup> As with all crime, the more serious incidents should be immediately reported to authorities. In the case of hate speech this involves threats of violence, incitement to hate and incitement to violence. In other cases, sanctions may start with penalties by a company, but once a company has exhausted its efforts at education and deterrence, the matter should escalate to one in which the power of the state intervenes.

**RECOMMENDATION 20:** Serious hate speech, that which makes threats of violence or incites either violence or hatred, should be immediately reported to authorities. Other forms of hate speech should be removed by the platform, but a log of the incident including the user's account and IP address should be recorded. Users should be informed when a platform takes action against them and should be

---

<sup>188</sup> AFP, 2017. "Germany imposes €50 million fines on social media firms that don't delete hate speech", *The Local.de* (30 June), at <https://www.thelocal.de/20170630/germany-imposes>, accessed 12 December 2019.

<sup>189</sup> Ibid.

<sup>190</sup> Ibid.

<sup>191</sup> Ibid.

<sup>192</sup> Ibid.

<sup>193</sup> Pompeu Casanovas Romeu and Andre Oboler, "Behavioural Compliance and Law Enforcement in Online Hate Speech". *TERECOM 2018 Technologies for Regulatory Compliance: Proceedings of the 2nd Workshop on Technologies for Regulatory Compliance co-located with the 31st International Conference on Legal Knowledge and Information Systems (JURIX 2018)*, pp. 125-134.



warned repeated breaches could lead to a report being made to authorities. Where platform sanctions prove ineffective at altering behaviour, the history of breaches and IP address of the user should be referred to authorities.

**RECOMMENDATION 21:** Once a user has been referred to authorities by a platform, a summary of any further hate speech incidents involving that user on that platform should be notified to authorities periodically (for example monthly) by the platform.

**RECOMMENDATION 22:** Once a user has been referred to authorities, the authorities should seek to convert the IP address into details of the account holder and add it to the record. Where the account holder is a company, the company should be notified with a request to identify the specific user.

**RECOMMENDATION 23:** Where a company cannot provide information on the person who committed a breach of the law against serious or repeated hate speech, assistance should be provided. Where a company will not provide information on the person who committed a breach of the law against serious or repeated hate speech, the company itself should be liable to corporate fines.

**RECOMMENDATION 24:** Users referred to authorities by platforms for repeated breaches that do not involve incitement to hate or violence should initially be issued a warning, potentially after a discussion with authorities in which their actions are discussed. Further breaches should lead to escalating fines. If fines fail to provide a deterrent more serious measures including imprisonment should be available.

**RECOMMENDATION 25:** Legal exemptions should be provided for researchers from government agencies and departments, academia and civil society engaged in testing the effectiveness of both platform and government agency responses. Such exemptions may require prior approval of the research by one or more authorised people or agencies who are independent of the enforcement system.

#### 4.5.2 Australia

In Australia the response for online safety and regulation of content such as that associated with the Halle attack rests with the Office of the eSafety Commissioner. This is a government agency created in 2015, initially for the purpose of providing online safety for children.<sup>194</sup> The remit has been expanded a number of times since then and the current purpose of the office is “to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences”.<sup>195</sup> The overarching goal is preventing harm through awareness-raising, education and best practice guidance.<sup>196</sup> The eSafety Commissioner has also been granted regulatory powers to prohibit material and order taken downs.

The eSafety Commissioner also has the power to issue a notice which affects the enforcement of new laws on Abhorrent Violent Material.<sup>197</sup> This is a category of prohibited content created in light of the

---

<sup>194</sup> Office of the eSafety Commissioner, 2019. ‘Who we are’, at <https://www.esafety.gov.au/about-us/who-we-are>, accessed 12 December 2019.

<sup>195</sup> eSafety Strategy 2019-2022, Office of the eSafety Commissioner, 1 <https://www.esafety.gov.au/sites/default/files/2019-10/eSafety%20Strategy%20Plan.pdf>, accessed 12 December 2019.

<sup>196</sup> eSafety Strategy 2019-2022, Office of the eSafety Commissioner, 2 <https://www.esafety.gov.au/sites/default/files/2019-10/eSafety%20Strategy%20Plan.pdf>, accessed 12 December 2019.

<sup>197</sup> Criminal Code Act 1995 (Cth) s 474.35.



Christchurch attack and includes sound, image and video, created by a person who is recording or livestreaming their conduct as they engage in a terrorist act, murder or other specified crimes.<sup>198</sup> The livestream and subsequent video of the Halle attack falls clearly within the definition of Abhorrent Violent Material and it is a criminal offence for content and hosting services to fail to expeditiously remove / cease hosting such content.<sup>199</sup> This law applies as long as the content can be accessed in Australia, regardless of whether it is actually hosted in Australia or not.<sup>200</sup> Failure to comply can result in a penalty of the greater of 50,000 penalty units (\$10.5 Million at present) or 10% of global profits for the month the failure occurred and the previous 11 months.<sup>201</sup> There is also the potential for jail time of up to 3 years or a fine of up to \$2.1 million for individuals.<sup>202</sup>

The Halle Attack began at 10 pm Australian Eastern Daylight Time. Early the next morning the Office of the eSafety Commissioner was in contact with Facebook, Twitter, Amazon and Google and worked with them to understand the situation in relation to the services offered to Internet users in Australia.<sup>203</sup> They also assessed a range of sites which were likely to be used to further distribute the material to gauge the risk of viral distribution.<sup>204</sup> The eSafety Commissioner became aware of three items of Abhorrent Violent Material and issues notices against each of the content services and their relating hosting services, a total of 6 Abhorrent Violent Material notices, which resulted in several items being removed.<sup>205</sup> In communications with OHPI the Office of the eSafety Commissioner expressed the view that the GIFCT Content Incident Protocol “appeared to work well to suppress the virality of the content”.<sup>206</sup>

The eSafety Commissioner also has power to refer content to the Classification Board.<sup>207</sup> The work of the Classification Board will be familiar to people in the form of film classifications such as G, PG, M or MA 15+.<sup>208</sup> The Classification Board has the power to classify Internet material, but in practice uses it very rarely. Where content that is to be classified relates to a terrorist act, there is a requirement that it be given the classification of “RC” (Refused Classification).<sup>209</sup> In explaining the “RC” classification the Classification Board explains:<sup>210</sup>

---

*Material that is Refused Classification is commonly referred to as being ‘banned’. Films, computer games and publications that are classified RC cannot be sold, hired, advertised or legally imported in Australia. Material that is classified RC contains*

---

<sup>198</sup> Criminal Code Act 1995 (Cth) s 474.31, s 474.32,

<sup>199</sup> Criminal Code Act 1995 (Cth) s 474.34,

<sup>200</sup> Criminal Code Act 1995 (Cth) s 474.34(2), (3).

<sup>201</sup> Criminal Code Act 1995 (Cth) s 474.34(10)

<sup>202</sup> Criminal Code Act 1995 (Cth) s 474.34(9)

<sup>203</sup> Communications between OHPI and the Office of the eSafety Commissioner, 30 October 2019.

<sup>204</sup> Ibid.

<sup>205</sup> Ibid.

<sup>206</sup> Ibid.

<sup>207</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 22(1)(g)

<sup>208</sup> <http://www.classification.gov.au/Guidelines/Pages/Guidelines.aspx>, accessed 12 December 2019.

<sup>209</sup> *Classification (Publications, Films and Computer Games) Act 1995* (Cth) s 9A

<sup>210</sup> <http://www.classification.gov.au/Guidelines/Pages/RC.aspx>, accessed 12 December 2019.

*content that is very high in impact and falls outside generally accepted community standards.*

---

Material with an RC classification is also “prohibited content” under Schedule 7 of the *Broadcasting Services Act 1992* (Cth).<sup>211</sup> Australian residents, bodies corporate carrying on activities in Australia, and Commonwealth, State and Territory Governments,<sup>212</sup> are able to make a complaint to the eSafety Commissioner about material that can be accessed in Australia which is prohibited content, or content that would be prohibited if it were classified.<sup>213</sup> The eSafety Commissioner can carry out an investigation in response to a complaint, or on her own initiative.<sup>214</sup> If the eSafety Commissioner carries out an investigation and prohibited content is found on a hosting service with an Australian connection, the eSafety Commissioner must issue a final take-down notice to have the content removed.<sup>215</sup>

While the classification and prohibited content approach overlaps with the Abhorrent Violent Material approach in the case of a video like that produced by the attackers in Christchurch or Halle, the two approach have some differences. The Abhorrent Violent Material approach creates a liability that occurs without the need for notice to be given, but it is far narrower as it only applied to material that records or livestreams the attack itself. The classification approach can also be used for video material which may be used to glorify the attack, but which was not created by the attacker or an associate of theirs and therefore fails the test for being Abhorrent Violent Material. The Abhorrent Violent Material provisions also only apply to online services, while the classification approach has broader reach and also prohibits the sale, hire, advertising or import of the material in other formats (for example, as data on a physical device).

Perhaps most significantly, the classification approach can also apply to manifestos produced and published in advance of an attack, but which are clearly a part of the terrorist act. This can be seen in New Zealand’s response to the Christchurch attack where the Government quickly classified the terrorist manifesto as “objectionable material”,<sup>216</sup> their equivalent of RC, and the New Zealand Department of Internal Affairs explained that, “this means that it is also illegal to hold a copy, share / distribute it under NZ Law”.<sup>217</sup>

Australia took the same approach in response to Christchurch. The Annual Report of the Australian Classification Board for 2018-2019 shows that only two requests for classification were made in relation to Internet content, both at the request of the eSafety Commissioner, and both were given a RC

---

<sup>211</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 20(1)(a)

<sup>212</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 41

<sup>213</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 37(1)

<sup>214</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 44.

<sup>215</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 47.

<sup>216</sup> Maggie Tait, 2019. “Christchurch attack publication ‘The Great Replacement’ classified objectionable”, *New Zealand Office of Film & Literature Classification* (23 March), at <https://www.classificationoffice.govt.nz/news/latest-news/christchurch-attacks-press-releases/#christchurch-attack-publication-the-great-replacement-classified-objectionable>, accessed 12 December 2019.

<sup>217</sup> DIA, 2019. *The Department’s response to the Christchurch terrorism attack video – Background information and FAQs*. New Zealand: Department of Internal Affairs. Online at <https://www.dia.govt.nz/Response-to-the-Christchurch-terrorism-attack-video>, accessed 12 December 2019.

classification.<sup>218</sup> The first item refused classification (Classification Number: 283834) matches the terrorist manifesto from the Christchurch attack. It is described by the Classification Board in the annual report as:<sup>219</sup>

---

*...a digital 87-page document, embedded within a PDF document... [which] described an ideological viewpoint, which was espoused to justify and encourage acts of terrorism against Muslim people. ...The Board was satisfied that the content promotes and incites in matters of crime or violence; and that it directly counsels, promotes, encourages and urges the doing of a terrorist act and directly praises the doing of a terrorist act in circumstances where there is substantial risk that such praise might have the effect of leading a person (regardless of his or her age or any mental impairment that the person might suffer) to engage in a terrorist act.*

---

The second item (Classification Number 283833) matches the description of the video of the Christchurch attack created as a result of the live streaming on Facebook. It is described in the annual report as:<sup>220</sup>

---

*...a short film – in the form of a recording of what appeared to be a live action video stream – that depicted the lead-up to and the shooting of a number of individuals inside a mosque and the events immediately following the shooting. ...The Board was satisfied that the content depicted, expressed or otherwise dealt with matters of crime, violence, cruelty and revolting or abhorrent phenomena in such a way that it offended against the standards of morality, decency and propriety generally accepted by reasonable adults; and that it directly counselled, promoted, encouraged and urged, and that it directly provided instruction on the doing of a terrorist attack, and directly praised the doing of a terrorist act in circumstances where there was a substantial risk that such praise might have the effect of leading a person (regardless of his or her age or any mental impairment that the person might suffer) to engage in a terrorist act.*

---

This classification approach has an additional declaratory benefit. By having the material classified as RC, and therefore prohibited content in Australia, a signal is sent to content providers. Some companies who are not bound by a country's laws will as a matter of their own corporate policies seek to prevent their services being used to share content that is illegal in a country to users in that country. If the declaration is not made, the company policies may not be triggered. Effective cooperation between

---

<sup>218</sup> Parliament of Australia, 2019. *Classification Board Annual Report 2018–19*, Canberra: Parliament House. Online at <https://www.classification.gov.au/about-us/research-and-publications/classification-board-and-classification-review-board-annual-reports-2018-19#toc-heading-4>, accessed 12 December 2019.

<sup>219</sup> Ibid.

<sup>220</sup> Ibid.

government and industry requires content to be classified, even when the government lacks jurisdiction to take action.

In the case of Halle communications with the Office of the eSafety Commissioner stated that the video was handled as Abhorrent Violent Material, but was not referred for classification as there were no reports of the content being hosted in Australia.<sup>221</sup> It was also noted that under the Abhorrent Violent Material laws notices to remove content could be issued, including to overseas sites, without seeking classification.

The law related to prohibited content covers not just the content itself, but also links to it. If in the course of an investigation the eSafety Commissioner is satisfied that an “end-users in Australia can access content using a link provided by a links service” and “the content is potential prohibited content” (that is content which is likely to be classified RC if referred to the Classifications Board) and “the links service has an Australian connection”, then “the Commissioner must” issue an “interim link-deletion notice” and “apply to the Classification Board” for the content to be classified.<sup>222</sup> As noted previously, Google appears to be a Link Service with an Australian Connection and also appears not to be removing links to the manifestos which are “potential prohibited content”. This suggests there may be a legal requirement for the content to be referred for classification and for Google to be directed to remove links to the content.

There is an alternative interpretation which suggest an “Australian Connection” does not exist unless the primary hosting location of the content, and not just servers to help with redistribution, are in Australia. If the intent of Parliament is to cast as wide a net as possible the term “Australian Connection” could be more clearly defined both in general and specifically for link services. There is a strong public policy argument that services which profit from advertising targeted at Australians, and which alter their content based on the fact a user is in Australia, should be subject to Australian laws on prohibited content. Complying with Australian law is a reasonable requirement for platforms targeting their product at the Australian market and profiting from doing so.

Based on a search of the classification board's RC decisions, since the Christchurch related classifications there have been no referrals of internet material to the Classifications Board. This mean the terrorist manifestos in Poway, El Paso and Halle have not as yet been refused classification in Australia.

During the course of this research the website of the Classification Board was updated and the online tool for reviewing classifications no longer allows users to easily request a list of all classification in a given date period by classification. This decreases government transparency. The classification of the Christchurch material was also obfuscated with the material listed as "ESAFETY CONTENT" 001 and 002. The manifesto was in fact listed as a film, not a document, in the record of the decision and made no reference to Christchurch. Neither did the video. There are ground not to provide, for example, the titles of Internet materials, but some reasonable description to aid those checking the record is needed if the Rule of Law is to be upheld. The public can't be expected to avoid e.g. importing prohibited content if the declaration that it has been refused classification has been obfuscated. A descriptive title such

---

<sup>221</sup> Communications between OHPI and the Office of the eSafety Commissioner, 30 October 2019.

<sup>222</sup> *Broadcasting Services Act 1992* (Cth) Schedule 7, s 62(2)

"Christchurch attacker's manifesto" and "video of live stream of Christchurch attack" would give sufficient clarity.

**RECOMMENDATION 26:** The eSafety Commissioner should refer all unclassified Abhorrent Violent Material for classification by the Classification Board. This should become a standard part of the process when new Abhorrent Violent Material is identified.

**RECOMMENDATION 27:** The eSafety Commissioner should refer to the Classification Board for classification the manifesto documents from the terrorist attacks in Halle, Poway and El Paso as was done in the case of Christchurch.

**RECOMMENDATION 28:** The eSafety Commissioner should announce when terrorist related material that has a risk of going viral has been given an RC rating and should advice the public to report any online copies to the eSafety Commissioner and not to share it.<sup>223</sup>

**RECOMMENDATION 29:** In Australia consideration should be given to creating a civil penalty regime for sharing material classified RC that promotes terrorism. Suitable exemptions should apply for those acting reasonably and in good faith for the purpose of journalism, scientific research or law enforcement.

**RECOMMENDATION 30:** The Classification Board should restore the previous tool that allowed more detailed interrogation of Classification Board decisions, specifically, it should allow all decisions in a given period for a particular classification to be listed.

**RECOMMENDATION 31:** The Classification Board should ensure either the title or a useful description is provided for material which is given an RC classification. This is necessary as the public can't comply with a ban if the banned content cannot be identified.

#### 4.6 Civil Society Action: Online Hate Prevention Institute

In addition to this in-depth report the Online Hate Prevention Institute completed a confidential report on November 24<sup>th</sup>, 2019, which we shared with government and impacted technology companies. In that report we identified a range of sites hosting material related to the Halle attack. All of the material was accessible from Australia. It included a copy of the video, still available at this time, and multiple copies of the manifesto documents. It also highlighted how search results were aiding access to this material.

After discussion with one of our contacts at Google we were asked to complete a removal request form. We did so and Google responded 3 days later. As discussed in the Google section, this resulted in the removal of links to two copies of the video and a request for further information in relation to links to the copies of the manifesto, which we provided. More than two weeks later we believe this ticket is still open and we have not heard back.

We have also been in contact with the Office of the eSafety Commissioner and have urged them to refer the manifestos to the Classifications Board. Should the content be classified RC, which is the only possible outcome if it is referred, it will make it much easier for Google to remove the search results.

---

<sup>223</sup> Office of the eSafety Commissioner, 'Report Abuse', at <https://www.esafety.gov.au/report>, accessed 12 December 2019.

This report, prior to being released publicly, is being shared with many of the impacted technology companies as well as other experts and stakeholders. Our aim as an organisation is always to lend our unique expertise and be a critical stakeholder working with governments, industry and civil society to reduce the risk of harm from online hate and extremism. We thank all of those who have engaged with us in this process.

## 5 A Culture Leading to Violent Extremism: The Image Boards and /pol/

Image boards are online discussion forums with a particular focus on the use of images. They are an early Internet technology and at the time added a significant new capability for Internet users, the ability to easily share and discuss images online. Another feature of these forums was the anonymity of their users. This was a benefit to these forums given the illegal nature of much of the content that was being discussed and shared. The image board concept originated in Japan but spread around the world.

In recent years there has been a shift in the image board culture as people set their sights beyond the online world. This has given rise to Anonymous first as a hacktivist group, then a larger political movement. It has also given rise to the Alt-Right, a social and political movement that seeks to alter the values of society and which stands in direct opposition to modern values of equality and human rights. Most worryingly, it has given rise to a sub-culture which incites and revels in violent extremism. It has created a global culture where hate and extremism can grow and fester.

The section begins with an introduction to the Japanese origins of the image boards. We then move into a discussion of 4chan, 8chan and the culture of /pol/.

### 5.1 Image Board Origins

Ayashii World (Japanese: Ayashii Warudo - あやしいワールド, Literally: Strange World) is the predecessor of the image boards and the first to introduce the anonymous discussion board culture.<sup>224</sup> It is also credited with introducing verbal memes, ascii art, and the first visual meme of online culture - the giko-neko ASCII art cat with a speech bubble whose message could be altered.<sup>225</sup>

Masayuki Shiba first operated Ayashii World in 1995 (between approximately August and December) through a dial-in Bulletin Board Service run by Nifty-Serve, then Japan's largest internet service

---

<sup>224</sup> Brad, 2016. "4chan - A Timeline History of Chan Imageboards", *Know Your Meme*, at <https://knowyourmeme.com/photos/1123439-4chan>, accessed 12 December 2019.; IsharaYar, 2013. "A Small History of Ayashii World", *AyashiWorldHistory*. Blogspot. Online at <http://ayashiworldhistory.blogspot.com/2013/02/a-small-history-of-ayashii-world-1.html>, accessed 12 December 2019.; *Complete History of 4chan*, at [http://tanasinn.info/wiki/Complete\\_History\\_of\\_4chan](http://tanasinn.info/wiki/Complete_History_of_4chan), accessed 12 December 2019.; *2ch Chronicle*, at [https://en.wikibooks.org/wiki/2ch\\_Chronicle](https://en.wikibooks.org/wiki/2ch_Chronicle), accessed 12 December 2019.

<sup>225</sup> Ndee 'Jkid' Okeh, 2017. "The Protochannel and the First Channel -- Ayashii World and Amezou World -- The Grandparents of the Western Imageboard Culture", at <http://yotsubasociety.org/ayashii-and-amezou/>, accessed 12 December 2019.

provider.<sup>226</sup> It operated on the “home party” service which allowed only an ID, title, name, and a post with a length of up to 20 lines of text to be displayed.<sup>227</sup>

This first version of Ayashii World focused on the computer game Kasumigaseki (霞ヶ関). Released by an anonymous computer programmer in August 1995,<sup>228</sup> the game was based on the Sarin gas terrorist attack on the Tokyo subway that March, an attack which killed 12 people and injured 5,000.<sup>229</sup> Players completed for a high score in the game by selecting the locations to place 5 Sarin gas canisters with the aim of harming as many people as possible; 10 points were awarded per death and 1 point per injury.<sup>230</sup>

After closing for a time, then a brief revival as a “home party”, in August 1996 the board moved to the Internet using a free BBS service from a company called Digital Eden.<sup>231</sup> In the BBS system the one internet provider both hosted the content and provided their paying customers with access to it, meaning there was no anonymity. In the new Internet based system the connectivity and the online service were separated. Further, identification became optional and “the contributors usually did not indicate their names in the name field, so that the community became an anonymous forum”.<sup>232</sup> Ayashii World discussed images, including illegal content such as child exploitation material, but the service itself was technically incapable of hosting images and instead in their posts users would provide links to images which were hosted elsewhere.<sup>233</sup> Ayashii hosted a number of boards, among them *gesu* (Literally: “scum”), which was used to plan attacks against other sites in a similar manner to /b/ which later emerged on 4chan.<sup>234</sup>

The first true image board, Licentious Notice Board (aka LNB), was created in August 1997.<sup>235</sup> It allowed images to be displayed in posts. LNB was initially online at

---

<sup>226</sup> Ndee ‘Jkid’ Okeh, 2013. “A small history of Ayashii World”, at <http://ayashiiworldhistory.blogspot.com/2013/02/a-small-history-of-ayashii-world-1.html>, accessed 12 December 2019.

<sup>227</sup> Ibid.

<sup>228</sup> Ibid; Chicago Tribune, 1995. “Programmer Shocks Internet with Subway Nerve Gas Game”, *Chicago Tribune* (26 October), at <https://www.chicagotribune.com/news/ct-xpm-1995-10-26-9510270293-story.html>, accessed 12 December 2019.

<sup>229</sup> History.com Editors, 2019. “Tokyo subways are attacked with sarin gas”, at <https://www.history.com/this-day-in-history/tokyo-subways-are-attacked-with-sarin-gas>, accessed 12 December 2019.

<sup>230</sup> Ibid.

<sup>231</sup> IsharaYar, 2013. “A Small History of Ayashii World”, *AyashiWorldHistory*. Blogspot. Online at <http://ayashiiworldhistory.blogspot.com/2013/02/a-small-history-of-ayashii-world-1.html>, accessed 12 December 2019.

<sup>232</sup> Muneo Kaigo and Isao Watanabe, 2007. “Ethos in Chaos? Reaction to Video Files Depicting Socially Harmful Images in the Channel 2 Japanese Internet Forum”, *Journal of Computer-Mediated Communication*, volume 12, number 4, pp. 1248-1268, p. 1251.

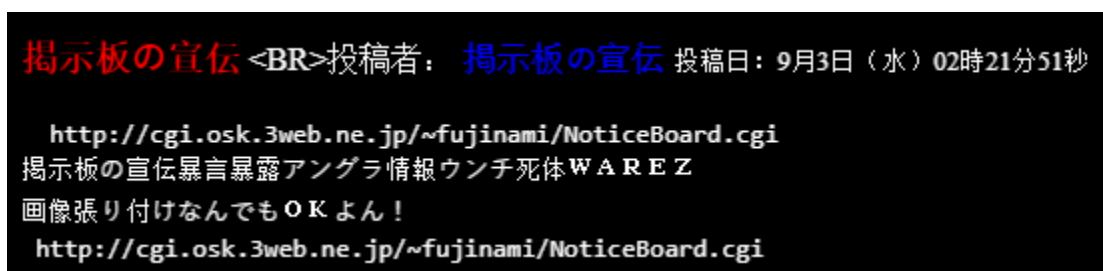
<sup>233</sup> IsharaYar, 2013. “A Small History of Ayashii World”, *AyashiWorldHistory*. Blogspot. Online at <http://ayashiiworldhistory.blogspot.com/2013/02/a-small-history-of-ayashii-world-1.html>, accessed 12 December 2019.

<sup>234</sup> Ndee ‘Jkid’ Okeh, 2017. “The Protochannel and the First Channel -- Ayashii World and Amezou World – The Grandparents of the Western Imageboard Culture”, at <http://yotsubasociety.org/ayashii-and-amezou/>, accessed 12 December 2019.

<sup>235</sup> Ibid.



<http://cgi.osk.3web.ne.jp/~fujinami/NoticeBoard.cgi>,<sup>236</sup> and posts promoting it on other forums presented it as a place where anything, including illegal content, could be posted (as shown in Figure 17 and Figure 19 which are translated in Figure 18 and Figure 20).<sup>237</sup> By 1998 a wide range of forums were running the imageboard.cgi script and displaying images rather than linking to them became the norm.<sup>238</sup>



掲示板の宣伝 <BR>投稿者: 掲示板の宣伝 投稿日: 9月3日 (水) 02時21分51秒

<http://cgi.osk.3web.ne.jp/~fujinami/NoticeBoard.cgi>  
 掲示板の宣伝暴言暴露アングラ情報ウンチ死体 W A R E Z  
 画像張り付けなんでも O K よん!  
<http://cgi.osk.3web.ne.jp/~fujinami/NoticeBoard.cgi>

Figure 17 Original Japanese post promoting LNB on September 3, 1997



**Bulletin Board Promotion** <BR> Poster: **Bulletin Board Advertisement** Posting Date: Wednesday, September 3 02:21:51

<http://cgi.osk.3web.ne.jp/~fujinami/NoticeBoard.cgi>  
 Bulletin board advertised rant exposure underground information uncle corpse WAREZ  
 Anything can be pasted!  
<http://cgi.osk.3web.ne.jp/~fujinami/NoticeBoard.cgi>

Figure 18 Google translate of a promotion post for LNB on September 3, 1997

<sup>236</sup> Licentious Notice Board Archive, at

[https://web.archive.org/web/20070907213600/http://history.amebbs.com/1997/1997\\_0805\\_n002main-ame.html](https://web.archive.org/web/20070907213600/http://history.amebbs.com/1997/1997_0805_n002main-ame.html), accessed 12 December 2019.

<sup>237</sup> 管理しない掲示板 (過去ログ9, at <https://museum.scenecritique.com/lib/tamon/uralog9.html>, accessed 12 December 2019.; 管理しない掲示板 (過去ログ10), at <https://museum.scenecritique.com/lib/tamon/uralog10.html>, accessed 12 December 2019.

<sup>238</sup> “るぼら,”教科書には載らないニッポンのインターネットの歴史教科書 単行本” (2010) (Barubora, “Japan's Internet History Not Appearing in Textbooks”, (2010)) quoted and translated in: IsharaYar, 2013. “A Small History of Ayashii World”, *AyashiWorldHistory*. Blogspot. Online at <http://ayashiiworldhistory.blogspot.com/2013/02/a-small-history-of-ayashii-world-1.html>, accessed 12 December 2019.





Figure 19 Original Japanese post promoting LNB on September 11, 1997

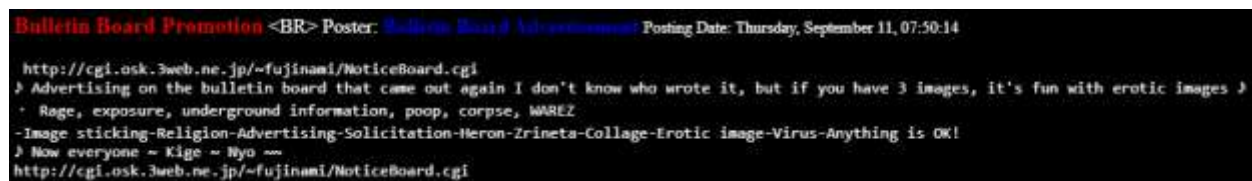


Figure 20 Google translate of a post promoting LNB on September 11, 1997

Ayashii World closed on 3 September 1998 in response to ongoing antagonism and the users divided among a range of other boards.<sup>239</sup> Amezu, created by Amezu-shi to host a collection of links pointing to these other boards, soon developed in its own forum.<sup>240</sup> It also introduced the style of conversation threading known as “floating threads” which is still used in image boards today.<sup>241</sup> In this style new threads appeared at the top of the list of topics, and within a thread new posts would appear at the bottom.<sup>242</sup> Amezu also introduced threads being bumped up the list of threads when they received a reply, unless users “sage” them to prevent this. It is described as the First Channel.<sup>243</sup>

<sup>239</sup> Ibid.

<sup>240</sup> Muneo Kaigo and Isao Watanabe, 2007. “Ethos in Chaos? Reaction to Video Files Depicting Socially Harmful Images in the Channel 2 Japanese Internet Forum”, *Journal of Computer-Mediated Communication*, volume 12, number 4, pp. 1248-1268, p. 1251.

<sup>241</sup> Ndee ‘Jkid’ Okeh, 2017. “The Protochannel and the First Channel -- Ayashii World and Amezu World – The Grandparents of the Western Imageboard Culture”, at <http://yotsubasociety.org/ayashii-and-amezu/>, accessed 12 December 2019.

<sup>242</sup> Muneo Kaigo and Isao Watanabe, 2007. “Ethos in Chaos? Reaction to Video Files Depicting Socially Harmful Images in the Channel 2 Japanese Internet Forum”, *Journal of Computer-Mediated Communication*, volume 12, number 4, pp. 1248-1268, p. 1251.

<sup>243</sup> *Complete History of 4chan*, at [http://tanasinn.info/wiki/Complete\\_History\\_of\\_4chan](http://tanasinn.info/wiki/Complete_History_of_4chan), accessed 12 December 2019.

In 1999 trolls engaged in a significant campaign of vandalism against Ameizou,<sup>244</sup> spamming it in a manner that cluttered the discussion threads making it unreadable.<sup>245</sup> Violent threats were also made against the owner,<sup>246</sup> and there were rumours they originated with the Yakuza, the Japanese crime syndicate.<sup>247</sup> Ameizou-shi responded by closing the Ameizou forum and calling on others to use his code and establish new image boards.<sup>248</sup>

Hiroyuki Nishimura, a user of Ameizou and at the time a student at the University of Central Arkansas, responded to the challenge.<sup>249</sup> On the 30 May 1999 using the code provided by Ameizou he launched the image board Ni-Channeru (Literally: 2 Channel, or Channel 2) which drew in a significant part of the former Ameizou audience.<sup>250</sup> It is named after the television station Channel 2 in the Kanto region of Japan, one of seven stations broadcast via VHF in the region, but is also a play on words as it was the second board for many after Ameizou.<sup>251</sup>

2channel soon “became not only the largest Japanese-language anonymous forum; but the definition of the Japanese Internet”.<sup>252</sup> One thing that set 2Channel apart is that despite still being a Japanese image board, it was hosted in the United States and was therefore beyond Japan’s stricter regulation of online content.<sup>253</sup> Post on 2channel included “racism and outright hatred toward society” through to criminal activity which ranges from leaked information on college entrance examinations to advertisements for murder.<sup>254</sup> Another use was to view “illegal or morally questionable violent content” given strict Japanese censorship of such content when it involves real people.<sup>255</sup>

A particular insight into 2channel can be seen in research into the forums response to the 27 October 2004 beheading of Japanese national Shosei Koda in Iraq by al-Qaida. 2channel users shared images and

---

<sup>244</sup> Ibid.

<sup>245</sup> Ndee ‘Jkid’ Okeh, 2017. “The Protochannel and the First Channel -- Ayashii World and Ameizou World – The Grandparents of the Western Imageboard Culture”, at <http://yotsubasociety.org/ayashii-and-ameizou/>, accessed 12 December 2019.

<sup>246</sup> Ibid

<sup>247</sup> IsharaYar, 2013. “A Small History of Ayashii World”, *AyashiWorldHistory*. Blogspot. Online at <http://ayashiworldhistory.blogspot.com/2013/02/a-small-history-of-ayashii-world-1.html>, accessed 12 December 2019.

<sup>248</sup> Ndee ‘Jkid’ Okeh, 2017. “The Protochannel and the First Channel -- Ayashii World and Ameizou World – The Grandparents of the Western Imageboard Culture”, at <http://yotsubasociety.org/ayashii-and-ameizou/>, accessed 12 December 2019.

<sup>249</sup> Ndee ‘Jkid’ Okeh, “2ch History”, at <https://github.com/bibanon/bibanon/wiki/2ch-History>, accessed 12 December 2019.

<sup>250</sup> *Complete History of 4chan*, at [http://tanasinn.info/wiki/Complete\\_History\\_of\\_4chan](http://tanasinn.info/wiki/Complete_History_of_4chan), accessed 12 December 2019.; Muneo Kaigo and Isao Watanabe, 2007. “Ethos in Chaos? Reaction to Video Files Depicting Socially Harmful Images in the Channel 2 Japanese Internet Forum”, *Journal of Computer-Mediated Communication*, volume 12, number 4, pp. 1248-1268, p. 1251.

<sup>251</sup> Ndee ‘Jkid’ Okeh, “2ch History”, at <https://github.com/bibanon/bibanon/wiki/2ch-History>, accessed 12 December 2019.

<sup>252</sup> *2ch Chronicle*, at [https://en.wikibooks.org/wiki/2ch\\_Chronicle](https://en.wikibooks.org/wiki/2ch_Chronicle), accessed 12 December 2019.

<sup>253</sup> Ibid.

<sup>254</sup> Muneo Kaigo and Isao Watanabe, 2007. “Ethos in Chaos? Reaction to Video Files Depicting Socially Harmful Images in the Channel 2 Japanese Internet Forum”, *Journal of Computer-Mediated Communication*, volume 12, number 4, pp. 1248-1268, p. 1254.

<sup>255</sup> Ibid 1255.

video of the beheading, spread of fake news about the incident, promoted clickbait posts with links they falsely claiming led to the video, and trolled new users to 2channel looking for the material and those who were tricked into revealing their IP address.<sup>256</sup> Empirical data over 5 threads and multiple days shown a high level of: anticipation of seeing the video, “banter” about Koda, neutral opinions and comments, information provision, and verification of information.<sup>257</sup> At the end of monitoring period, once the video and news of Koda’s death was verified, there was a high degree of anxiety/ fear about the execution video, mourning over his death and discussions about terrorism, war and politics, as well as an extremely high level of traffic to download the video.<sup>258</sup> Debate in the forum led to further discussion about the sharing of the execution video itself and moderation by the user community to limit or stop the spread of the video. The authors of the study noted how “postings expressing remorse and attempting moderation swelled in frequency and ultimately predominated” while anti-social postings decreased in face of the large number of posts promoting moderation.<sup>259</sup> The results show that even in an anonymous Internet forum, positive social norms can be established and have social impact but in the absence of that social pressure anti-social behaviour can dominate.

By August 2001 traffic to 2channel had grown so large the site was struggling to cope.<sup>260</sup> Two different approaches were taken, one by a sub-community of coders who sought to increase the efficiency of the code which ultimately reduced the load associated with some scripts by 90%, and the other by those who sought to create a second image board to spread the load.<sup>261</sup> The original 2channel continued to operate, now alongside a new forum.<sup>262</sup>

The new forum, also created by Hiroyuki Nishimura, was called Futaba channel (Literally: two leaves channel). It was established at 2chan.net and featured a graphic of a small plant with 2 leaves as its logo. For the first time in the channel boards, it also integrated the use of images.<sup>263</sup> It was Futaba which first created the board /b/ for posting random content.<sup>264</sup>

These Japanese boards all contributed to the creation of both the technology and the online culture that exists today. The desire to engage in anonymous discussion free of the need for cultural or political correctness is part of the DNA of the original Japanese boards and remains part of the culture across image boards in all languages today. The Japanese online sub-culture moved into the English-speaking world and indeed became a global sub-culture with the creation of 4chan and a range of successor image boards. These boards developed their own culture while maintaining an appreciation for the Japanese online sub-culture from which they had grown. The use of anonymity on the image boards to

---

<sup>256</sup> Ibid 1259-1260.

<sup>257</sup> Ibid 1261.

<sup>258</sup> Ibid.

<sup>259</sup> Ibid. 1262

<sup>260</sup> Ndee ‘Jkid’ Okeh, “2ch History”, at <https://github.com/bibanon/bibanon/wiki/2ch-History>, accessed 12 December 2019.

<sup>261</sup> Ibid.

<sup>262</sup> In October 2017 2channel was rebranded 5chan and moved to 5chan.net. [see: *2ch Chronicle*, at [https://en.wikibooks.org/wiki/2ch\\_Chronicle](https://en.wikibooks.org/wiki/2ch_Chronicle), accessed 12 December 2019].

<sup>263</sup> *Complete History of 4chan*, at [http://tanasinn.info/wiki/Complete\\_History\\_of\\_4chan](http://tanasinn.info/wiki/Complete_History_of_4chan), accessed 12 December 2019.; Muneo Kaigo and Isao Watanabe, 2007. “Ethos in Chaos? Reaction to Video Files Depicting Socially Harmful Images in the Channel 2 Japanese Internet Forum”, *Journal of Computer-Mediated Communication*, volume 12, number 4, pp. 1248-1268, p. 1251.

<sup>264</sup> Ibid.

allow not only politically incorrect speech, but to enable illegal activity and the sharing material related to violent extremism has continued and spread with the image boards themselves.

## 5.2 The Rise of 4chan

There were English language forums in the United States, but most required registration and email verification, lacking the anonymity of the Japanese boards.<sup>265</sup> They also lacked the “floating threads” which had been so successful on the Japanese boards. The features of the Japanese image boards were brought to the English language Internet audience with the creation of 4chan in 2003.

Founded by 15-year-old Christopher Poole in 2003, 4chan is an English language image board based on the code from the Japanese 2chan site. Its early growth was due to an exodus of users to 4chan from the forum ‘somethingawful.com’. Although originally intended for English-speaking fans of anime and other aspects of Japanese culture, 4chan’s scope rapidly expanded to encompass a wide range of topics.

By 2010 4chan was the 800th most popular Internet site globally according to Alexa and attracted around 8.2 million unique visitors a month.<sup>266</sup> By October 2016 it had climbed to the 573<sup>rd</sup> most popular site and was attracting 27 million unique monthly visitors.<sup>267</sup> Today the site has 27.7 million users,<sup>268</sup> but has dropped to the 219,478 position in Alexa.<sup>269</sup> According to statistics presented for potential advertisers, the site’s average audience predominantly male (about 70%) and in the age range of 18-34.<sup>270</sup> Australia makes up 5% of 4chan’s audience and is the 4<sup>th</sup> largest source of visitors to the site by country after the USA (47%), UK (8%) and Canada (6%).<sup>271</sup> Adjusted for population, of then 10 countries with the most visitors to 4chan Australian engagement (5.50%) is exceeded only by that of Sweden (5.54%) and significantly higher than the United States (3.98%).

4chan provided the foundation for a great deal of popular culture which spread across the Internet and occasionally offline, while at the same time maintaining a “culture of abuse”. Among the positive contributions of 4chan to popular culture are the modern concept of a meme,<sup>272</sup> LOLcats,<sup>273</sup> and the Anonymous movement.<sup>274</sup> Negative contributions to online culture coming from 4chan include encouraging suicides,<sup>275</sup> coordinating extreme harassment,<sup>276</sup> and initially hosting the misogyny that led

---

<sup>265</sup> Muneo Kaigo and Isao Watanabe, 2007. “Ethos in Chaos? Reaction to Video Files Depicting Socially Harmful Images in the Channel 2 Japanese Internet Forum”, *Journal of Computer-Mediated Communication*, volume 12, number 4, pp. 1248-1268, p. 1251.

<sup>266</sup> Josh Horwitz, 2016. “Hate speech factory 4chan is dying, and Twitter and Reddit should be paying attention”, *Quartz* (4 October), at <https://qz.com/799632/hate-speech-factory-4chan-is-dying-and-twitter-twtr-and-reddit-should-be-paying-attention/>, accessed 12 December 2019.

<sup>267</sup> Ibid.

<sup>268</sup> ‘Advertise’, 4chan, at <http://www.4chan.org/advertise>, accessed 12 December 2019.

<sup>269</sup> *Alexa Analytics*, ‘4chan.org’, at <https://www.alexa.com/siteinfo/4chan.org>, accessed 12 December 2019.

<sup>270</sup> Ibid.

<sup>271</sup> Ibid.

<sup>272</sup> <https://www.youtube.com/watch?v=dQw4w9WgXcQ>, accessed 12 December 2019.

<sup>273</sup> *Know Your Meme*, ‘Lolcats’, <https://knowyourmeme.com/memes/lolcats>, accessed 12 December 2019.

<sup>274</sup> INFOSEC, 2011. “A History of Anonymous”, (24 October), at <https://resources.infosecinstitute.com/a-history-of-anonymous/>, accessed 12 December 2019.

<sup>275</sup> Jay Hathaway, 2013. “4chan user sets himself on fire in livestreamed suicide attempt”, *The Daily Dot* (12 November), accessed 12 December 2019.

<sup>276</sup> Adrian Chen, 2010. “The Art of Trolling: Inside a 4chan Smear Campaign”, *Gawker* (17 July), at <https://gawker.com/5589721/the-art-of-trolling-inside-a-4chan-smear-campaign>, accessed 12 December 2019.

to Gamergate.<sup>277</sup> 4chan has received sporadic bursts of high-profile media attention, usually for its negative impact.

4chan has always cultivated a “too toxic to endure” culture steeped in sarcasm and irony that users claim is intentionally designed to confuse and shock new visitors. This culture was deployed as a tool for excluding certain social groups from participation and establishing subcultural boundaries and signposting group identity. One of the boards within 4chan, however, took this to a new level. The /pol/ board was regularly presented as a “containment zone”, a place within the 4chan community to quarantine behavior that was too toxic even for the rest of 4chan.

### 5.3 /pol/ the “Politically Incorrect” Board and its Evolving Antisemitism

The “politically incorrect” forum known for short as /pol/ can be found on 4chan, 8chan, and a range of other boards. The promotion of Nazism, racism, and xenophobia in general are popular themes on the board, and traditionally would continue only until someone started to take it seriously, before the mob would then turn on them. In recent years, however, that has changed.

/pol/-users are responsible for a range of actions that gained widespread media attention. They turned Microsoft’s self-learning Twitter bot into a Hitler loving racist.<sup>278</sup> They manipulated the media into believing there was a boycott of Star Wars on the grounds of the cast being too racially diverse and not ‘white enough’.<sup>279</sup> They spent years trolling cartoonist Ben Garrison, turning his political cartoons into pro-Nazi and antisemitic propaganda, and were involved in the efforts to turn an antisemitic image into a part of everyday Internet culture.<sup>280</sup> They are responsible for the spread of extremist slogans such as “Gas the kikes. Race war now” to a range of other platforms.<sup>281</sup>

While it used to be hard to know what was serious and what was a result of /pol/lacks (users of /pol/) trolling each other, the extreme views which started as a parody became an earnest belief within the /pol/ community. This normalisation of neo-Nazism on /pol/ was in part the results of a campaign by neo-Nazis from Stormfront who sought to convert the /pol/lacks to their ideology.<sup>282</sup> The rise of the alt-right also had a significant impact and /pol/ has become ground zero for a movement of “red-pilling”.

---

<sup>277</sup> Emily Todd VanDerWerff, 2014. “#Gamergate: Here's why everybody in the video game world is fighting”, Vox (13 October), at <https://www.vox.com/2014/9/6/6111065/gamergate-explained-everybody-fighting>, accessed 12 December 2019.

<sup>278</sup> Abby Ohlheiser, 2016. “Trolls turned Tay, Microsoft’s fun millennial AI bot, into a genocidal maniac”, *The Washington Post* (26 March), at <https://www.washingtonpost.com/news/the-intersect/wp/2016/03/24/the-internet-turned-tay-microsofts-fun-millennial-ai-bot-into-a-genocidal-maniac/>, accessed 12 December 2019.; Ethan Chiel, 2016. “Who turned Microsoft's chatbot racist? Surprise, it was 4chan and 8chan”, *Splinter* (24 March), <https://splinternews.com/who-turned-microsofts-chatbot-racist-surprise-it-was-1793855848>, accessed 12 December 2019.

<sup>279</sup> Fruzsina Eordogh, 2015. “How Trolls Fooled the Media with #BoycottStarWars”, *MOTHERBOARD: Tech by VICE* (21 October), at [https://motherboard.vice.com/en\\_us/article/vv74ay/how-trolls-fooled-the-media-with-boycottstarwars](https://motherboard.vice.com/en_us/article/vv74ay/how-trolls-fooled-the-media-with-boycottstarwars), accessed 12 December 2019.

<sup>280</sup> Andre Oboler, 2014. *The Antisemitic Meme of the Jew*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/the-antisemitic-meme-of-the-jew/>, accessed 12 December 2019.

<sup>281</sup> Janet Reitman, 2018. “All-American Nazis”, *Rolling Stone Magazine* (2 May), at <https://www.rollingstone.com/politics/politics-news/all-american-nazis-628023/>, accessed 12 December 2019.

<sup>282</sup> Janet Reitman, 2018. “All-American Nazis”, *Rolling Stone Magazine* (2 May), at <https://www.rollingstone.com/politics/politics-news/all-american-nazis-628023/>, accessed 12 December 2019.

The red-pill metaphor is a reference to a plot device featured in the 1999 film, *The Matrix*.<sup>283</sup> In the film the rebel leader Morpheus offers the main character, Neo, the choice of taking a red pill which will break him out of the artificial reality in which he is living and allow him to see the world as it is. Neo is also offered the choice of taking the blue pill, which will allow him to continue living in the false but comfortable reality that has been constructed for him. The term is frequently used across alt-right platforms as a means of distinguishing between a perceived informed minority (the red-pilled), and an ignorant majority (the blue-pilled). *Rolling Stone* Magazine explains how Andrew Oneschuk, who shot his two roommates at close range, had been convinced “through an intricate online world, that everything they’d ever learned was, essentially, a lie”.<sup>284</sup> Starting on /pol/ but spreading through the Alt-Right more generally, the idea of being red-pilled or “woke”<sup>285</sup> is to reject the messages and values taught by society. The views that replace this are based on conspiracy theories, racism, misogyny and the promotion of white supremacy.

Antisemitism has always been present on 4chan and was a part of /pol/ since /pol/’s inception in 2011 [see Figure 5].<sup>286</sup> After all, what could be more politically incorrect than claiming to support Nazism? This initial promotion of antisemitism was an attempt to cause shock and use the anonymity of the online forum to defy the norms of offline society. There was no particular malice towards Jews, instead the focus was on jokes and pranks expressed ironically to troll others.



Figure 21: The unofficial board logo/symbol for /pol/ underscores the recurring theme of Nazism on /pol/ boards.

An example of how Holocaust denial was originally promoted as a joke on 4chan was the “Dub the Dew” raid in 2012 where 4chan users manipulated an online poll used to name the new Mountain Dew

<sup>283</sup> Angela Nagle 2016, “The New Man of 4chan”, *The Baffler*, number 30, pp. 64-76, p. 66.

<sup>284</sup> Janet Reitman, 2018. “All-American Nazis”, *Rolling Stone Magazine* (2 May), at <https://www.rollingstone.com/politics/politics-news/all-american-nazis-628023/>, accessed 12 December 2019.

<sup>285</sup> Alice Marwick & Rebecca Lewis 2017, *Media Manipulation and Disinformation Online*. Data & Society Research Institute, Online at [http://www.chinhnghia.com/DataAndSociety\\_MediaManipulationAndDisinformationOnline.pdf](http://www.chinhnghia.com/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf), accessed 3 September 2018, p. 29.

<sup>286</sup> 4chan, at [https://commons.wikimedia.org/wiki/File:4chan\\_-\\_pol-\\_logo.png#filehistory](https://commons.wikimedia.org/wiki/File:4chan_-_pol-_logo.png#filehistory), accessed 12 December 2019.



drink.<sup>287</sup> Users were encouraged to “get all the Hitler and gushing granny names into the top 20”, resulting in the name “Hitler did nothing wrong” being voted to the #1 spot, with a variety of vulgar but not antisemitic names making up the rest of the top ten. The juxtaposition of a Holocaust denial name with other vulgar, but not antisemitic names indicates the top name was chosen to maximise the controversy of the incident, rather than to actually promote the idea of Holocaust denial.

Over time /pol/ has been taken over by neo-Nazis and its culture has changed from one that was ironically racist, with antisemitism being a part of that, to one where violence against Jews is not just advocated, but live streamed for the /pol/ community’s entertainment.

### 5.3.1 Antisemitic Alterations to Ben Garrison Cartoons

Another source of antisemitic material on /pol/ took the form of pro-Nazi and antisemitic cartoons created by as a result of users altering libertarian cartoons created by cartoonist Ben Garrison. Where the original cartoons aimed at targets like big government, the banks and drug companies, the altered versions shifted the target to Jews. Garrison has been described as the Internet’s most trolled cartoonist,<sup>288</sup> and was once described by the Alt-Right’s Milo Yiannopoulos as “probably the most trolled man in internet history”.<sup>289</sup>

The trolling of Ben Garrison started in 2011 and coincided with the decline of /b/’s position of cultural centrality on 4chan, and the creation of /pol/. Fake Ben Garrison cartoons were a part of the culture that emerged on /pol/ right from the start. Whenever a new cartoon was released by Garrison, 4chan-users would race each other to see who could alter the cartoon into something antisemitic. The collective investment in these endeavours by 4chan-users, as manifest in the countless threads dedicated to the cause, tapped into a kind of cultural crucible. On 4chan, only the most memorable productions will endure over time, because all ‘inferior’ productions are almost immediately displaced and deleted in the wake of the exceptionally fast pace in which content is posted and subsequently deleted on 4chan (cite). Consequently, whatever antisemitic material was produced first had to successfully endure this subcultural trial by fire, and would typically resonate with a wide audience, and could then be spread to multiple online forums and image hosting sites. The spread of the altered cartoons produced on 4chan was so extensive that they displaced the originals in online searches for Ben Garrison cartoons.<sup>290</sup>

---

<sup>287</sup> ‘Dub-the-dew’, *Know Your Meme*, at <https://knowyourmeme.com/memes/events/dub-the-dew>, accessed 12 December 2019.

<sup>288</sup> David Blumenstein, 2015. “The Internet’s Most Trolled Cartoonist”, *THENIB* (2 June), at <https://thenib.com/the-internet-s-most-trolled-cartoonist-91a92d9b7585>, accessed 12 December 2019.

<sup>289</sup> Milo Yiannopoulos, 2016. “Trolls will save the world”, *Breitbart* (20 August), at <https://www.breitbart.com/social-justice/2016/08/20/trolls-will-save-world/>, accessed 12 December 2019.

<sup>290</sup> Andre Oboler, 2014. *4Chan’s /pol/ and the Trouble with Dean*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/4chans-pol-and-the-trouble-with-dean/>, accessed 12 December 2019.



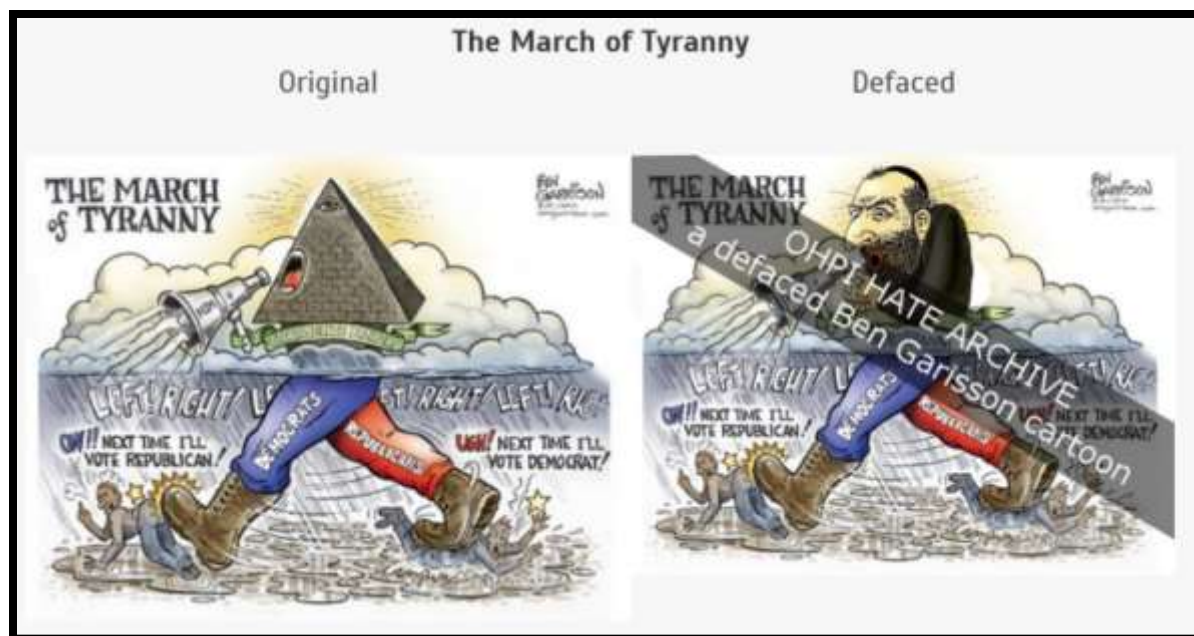


Figure 22 Original Ben Garrison cartoon [left] alongside a defaced version using the Antisemitic Meme of the Jew [right].

Garrison himself was also targeted, mostly by users on /pol/.<sup>291</sup> His image was photoshopped into a Nazi uniform and paired with fake biographical details. He was given the nickname “Zyklon Ben”, after the Zyklon B gas used to murder Jews at Auschwitz,<sup>292</sup> along a range of other names that sought to promote him as a hardcore Nazi. A page dedicated to this entirely fictional Ben Garrison was created at Encyclopedia Dramatica in April 2013.<sup>293</sup> Twitter references, showing the use in mainstream social media, can be found as early as June 21, 2013.<sup>294</sup> Despite the significant harm they caused him many on /pol/ genuinely liked the original versions of his cartoons and regularly said so. A comment posted to Garrison’s blog in November 2016 says “/pol/ here, we miss having you around, Ben... It is all in good fun that the edits are made... This may seem odd, but for the most part /pol/ has great respect for you. You produce great cartoons with ideas that challenge the establishment. Don’t be bothered by the edits, ‘Imitation is the sincerest form of flattery’ right? And come back and visit us again! Ave Zyklon Ben!”<sup>295</sup> The comment appears sincere, but also demonstrates a complete inability to understand why a person might object to being associated with Nazism. This can be seen in the idea altered copies of Ben’s work, with his name on it, which promote Nazism are seen as nothing more than fun. It can also be seen in the sign off, “Ave Zyklon Ben”, both respectful and entirely blind to harm of the “Zyklon Ben” invention on the real Ben Garrison.

<sup>291</sup> ‘Ben Garrison’, *Know Your Meme*, at <https://knowyourmeme.com/memes/people/ben-garrison>, accessed 12 December 2019.

<sup>292</sup> Emma Grey Ellis, 2017. “The Alt-Right Found Its Favorite Cartoonist—and Almost Ruined His Life at”, *WIRED* (19 June), at <https://www.wired.com/story/ben-garrison-alt-right-cartoonist/>, accessed 12 December 2019.

<sup>293</sup> ‘Ben Garrison’, *Know Your Meme*, at <https://knowyourmeme.com/memes/people/ben-garrison>, accessed 12 December 2019.

<sup>294</sup> Derailius, *Twitter*, at <https://twitter.com/derailius/status/348025007093456896>, accessed 12 December 2019.

<sup>295</sup> Ben Garrison, 2015. “Disclaimer: Don’t be Trolled”, *Grrrgraphics*, at <https://grrrgraphics.wordpress.com/grrrgraphics-disclaimer/>, accessed 12 December 2019.

Contemporaneous evidence shows the editing started at 4chan sometime between May and August 2011.<sup>296</sup> Encyclopedia Dramatica claims the first edits occurred on the 4chan.net's Nazi board “/n/”.<sup>297</sup> This information tallies with comments OHPI observed after releasing a report which covered Ben Garrison cartoons in 2014.<sup>298</sup> Garrison became aware of the altered cartoons and responded in May 2011 with a blog post in which stating that someone was editing his cartoons by “adding in offensive Jewish stereotypes” while leaving his name on the images.<sup>299</sup> He reassured any readers of his blog that his “target” was the “elite international banking system and the Federal Reserve. NOT Jews.”<sup>300</sup> Garrison himself later stated that his wife found the source of the altered cartoons on 4chan’s /b/.<sup>301</sup> While /b/ was not the first to alter a Garrison cartoon, it was a source of the continued trolling, partly in response to his blog post.

Further information on the trolling of Ben Garrison can be seen in OHPI 2014 report,<sup>302</sup> and has also been covered in subsequent briefings.<sup>303</sup>

### 5.3.2 The Antisemitism Meme of the Jew

One common theme of antisemitism is what we call the “Antisemitic Meme of the Jew” which /pol/ refers to as “The Happy Merchant” meme (see Figure 23).<sup>304</sup> It is a cartoon stereotype of a Jewish man with a black beard, long hooked nose, hunched back, crooked teeth and hands being wrung in glee. Our report into this meme covers its racist origins, including its creation by a white supremacist cartoonist and its use online in neo-Nazi circles, as well as its popularisation by 4chan and an attempt to integrate it into mainstream online culture through the *Know Your Meme* website.<sup>305</sup> New investigative research has

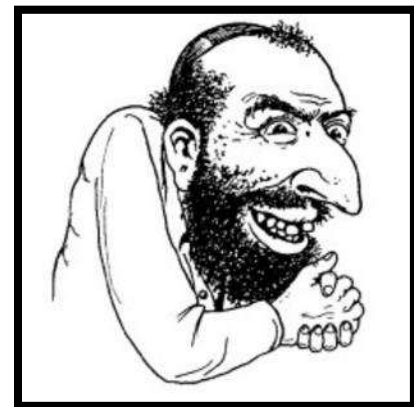


Figure 23 Antisemitic Meme of the Jew

<sup>296</sup> <https://web.archive.org/web/20141216074009/http://mpcdot.com/forums/topic/3026-ben-garrison-appreciation-thread/> - Original post 18 August 2011, accessed 12 December 2019.

<sup>297</sup> [https://encyclopedia.dramatica.rs/Ben\\_Garrison/JIDF\\_Version](https://encyclopedia.dramatica.rs/Ben_Garrison/JIDF_Version), accessed 12 December 2019.

<sup>298</sup> Andre Oboler, 2014. *The Antisemitic Meme of the Jew*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/the-antisemitic-meme-of-the-jew/>, accessed 12 December 2019.

<sup>299</sup> Ben Garrison, 2011. “GRRR-ALERT!”, *GrrGraphics* (22 May), <https://grrrgraphics.wordpress.com/2011/05/22/grrr-alert/>, accessed 12 December 2019.

<sup>300</sup> Ibid.

<sup>301</sup> Allum Bokhari, 2015. “Ben Garrison: How The Internet Made A Fake White Supremacist”, *Breitbart* (22 December), at <https://www.breitbart.com/tech/2015/12/22/ben-garrison-how-the-internet-made-a-fake-white-supremacist>, accessed 12 December 2019.

<sup>302</sup> Andre Oboler, 2014. *The Antisemitic Meme of the Jew*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/the-antisemitic-meme-of-the-jew/>, accessed 12 December 2019.

<sup>303</sup> Andre Oboler 2014. *Ben Garrison on Trolls*. Melbourne, Australia: Online Hate Prevention Institute. Online at <http://ohpi.org.au/ben-garrison-on-trolls/>, accessed 12 December 2019.

<sup>304</sup> Andre Oboler, 2014. *The Antisemitic Meme of the Jew*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/the-antisemitic-meme-of-the-jew/>, accessed 12 December 2019.

<sup>305</sup> Ibid.

revealed the author to be Nick Bogus and has shown that the cartoon has been circulating online since at least 2001.<sup>306</sup>

The meme is known for featured in antisemitic comics strips and being edited for a range of different contexts online. A recent report by the Network Contagion Research Institute covers how /pol/ creates large quantities of merchant memes and disseminates them into other social media spaces.<sup>307</sup>

The image was integrated into the first edited Ben Garrison cartoon, and many subsequent ones. It has also infected other popular memes. Recent research “demonstrates numerous instances of the Happy Merchant infecting well-known and popular memes” with the authors noting how this infection “could serve, for instance, to make antisemitism more accessible and common”.<sup>308</sup> Importantly this is not qualitative research, but a quantitative examination of the problem. An example of popular memes that have been infected with the antisemitic meme of the Jew and their spread through Twitter can be seen in Figure 24.

Through memes, and this one in particular in its many flavours, antisemitism is spread even by those who initially have very little antisemitic intent and see it as simply part of the online sub-culture. Over time, however, this exposure creates a normalisation and social acceptability of antisemitism which is known as the antisemitism 2.0 effect.<sup>309</sup>

---

<sup>306</sup> Joseph Bernstein, 2015. “The Surprisingly Mainstream History Of The Internet's Favorite Anti-Semitic Image”, *BuzzFeed* (5 February), at <https://www.buzzfeednews.com/article/josephbernstein/the-surprisingly-mainstream-history-of-the-internets-favorit>, accessed 12 December 2019.

<sup>307</sup> Savvas Zannettou, Joel Finkelstein, Barry Bradlyn & Jeremy Blackburn, 2018. “A Quantitative Approach to Understanding Online Antisemitism Part 3: Meme Analysis”, Network Contagion Research Institute: *arXiv e-prints*. Online at <https://ncri.io/2018/09/06/a-quantitative-approach-to-understanding-online-antisemitism-part-3-meme-analysis/>, accessed 12 December 2019.

<sup>308</sup> Savvas Zannettou, Joel Finkelstein, Barry Bradlyn & Jeremy Blackburn, 2018. “A Quantitative Approach to Understanding Online Antisemitism”, Network Contagion Research Institute: *arXiv e-prints*. Online at <https://arxiv.org/abs/1809.01644>, accessed 12 December 2019.

<sup>309</sup> Andre Oboler, 2008. “Online Antisemitism 2.0. ‘Social Antisemitism on the Social Web’”, *JCPA: Post-Holocaust and Antisemitism Series* (April 2008, No. 67), Online at <http://jcpa.org/article/online-antisemitism-2-0-social-antisemitism-on-the-social-web/>, accessed 12 December 2019.

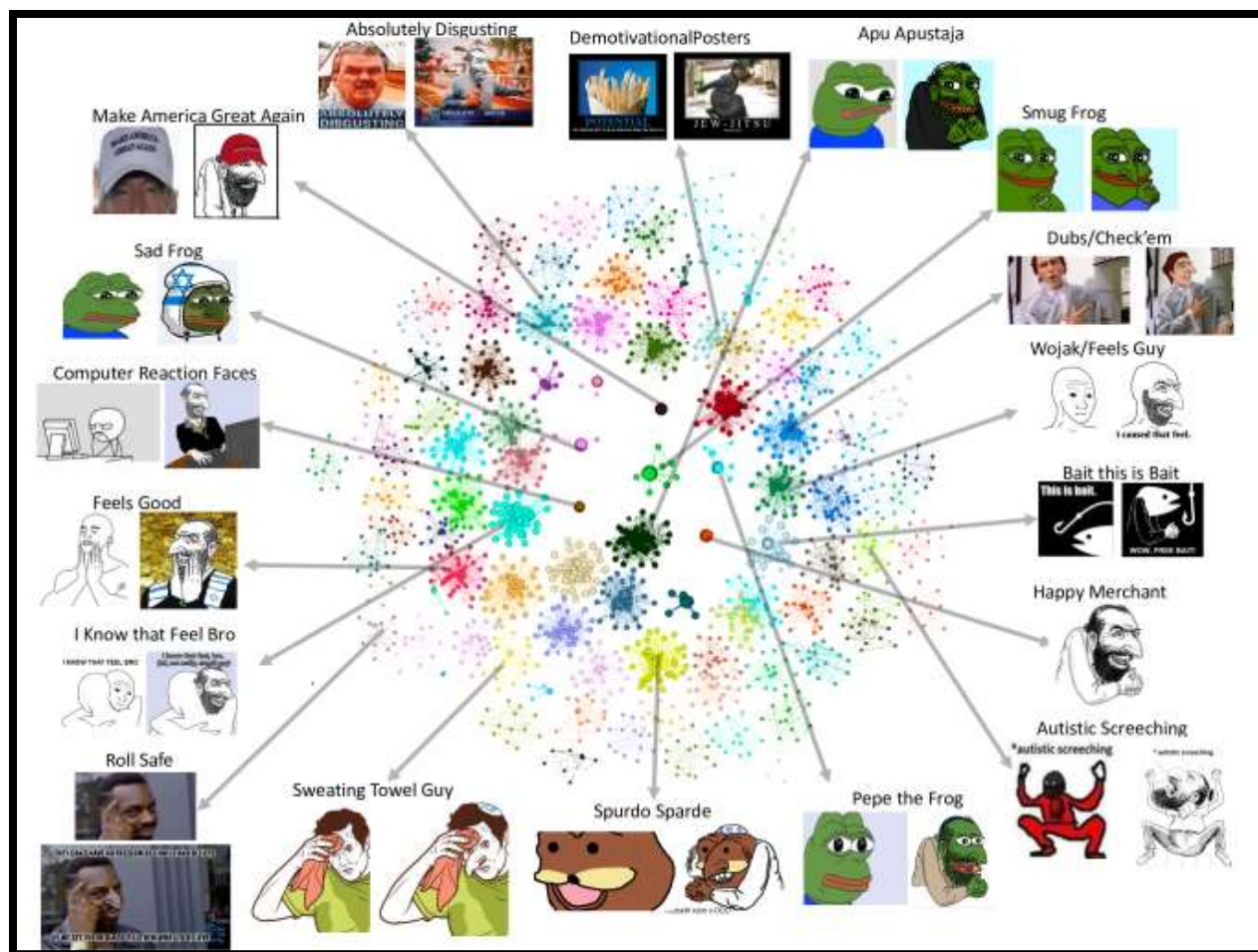


Figure 24 Penetration of the Antisemitic Meme of the Jew features into other meme templates<sup>310</sup>

### 5.3.3 A shift in /pol/'s antisemitism

There has been interest in /pol/ by neo-Nazis on Stormfront since at least July 2012.<sup>311</sup> At that time the “almost completely unmoderated” nature of /pol/ was already noted as a plus for spreading neo-Nazi ideology.<sup>312</sup> At this time there was push back on /pol/ to overt neo-Nazism.<sup>313</sup>

By January 2014, however, a long time stormfront user described /pol/ users as “strongly pro-WN [White Nationalism], pro-NS [National Socialism] or pro-libertarian” adding that “the whole culture of

<sup>310</sup> Image used with permission of the authors. Source: Savvas Zannettou, Joel Finkelstein, Barry Bradlyn, Jeremy Blackburn, 2019. “A Quantitative Approach to Understanding Online Antisemitism”, *14th International AAAI Conference on Web and Social Media*, Online <https://arxiv.org/abs/1809.01644>, accessed 12 December 2019.

<sup>311</sup> Post by returntrip, 17 July 2012 <https://www.stormfront.org/forum/t900887/>, accessed 12 December 2019.

<sup>312</sup> Ibid.

<sup>313</sup> Ibid.

the board is ragingly anti-jew”,<sup>314</sup> and that “there's a strong, almost overwhelming WN [White Nationalist] current on the /pol/ board”.<sup>315</sup>

Some long-time users of both 4chan and Stormfront at this time felt “4chan members don't genuinely believe in NS [National Socialism], separatism, or any WN [White Nationalism] ideology... most... Simply fancy the idea of acting ‘evil’ and ‘racist’”.<sup>316</sup> Others drew a distinction between /pol/ and 4chan more generally. One said 4chan was “a cesspool of corruption” (from a neo-Nazi perspective), but said “pol/ on the other hand, has many people on there that are racially aware” but that it wasn’t contributing to the neo-Nazi cause beyond leading people to Stormfront.<sup>317</sup> Others highlighted the difference between /b/ and /pol/ saying the former was “teenagers being racist for shock value” while the latter was “everything from promoting traditional values... to exposing Jews”.<sup>318</sup> Another explained that “/pol/ has only recently become a European Nationalist site” that it was “expanding at an unprecedented rate in influencing other sites on the internet”.<sup>319</sup> Another explained the influence of /pol/ explaining that, “/pol/ has made the notion of ridiculing Holocaust acceptable on the Internet with all the Ben 'Zyklon B' Garrison stuff and the like being funny as hell. You can now take more conservative stances without being bashed unreasonably, as well.”<sup>320</sup>

The infiltration by neo-Nazis from Stormfront did not go unnoticed. By February 2013 others on 4chan were already complaining about /pol/acks invading other boards and posting antisemitic and racist content that was completely off topic and simply disrupted other conversations. The post is about /pol/ but says refers to those from /pol/ not as /pol/acks, but as Stormniggers and Stormfags,<sup>321</sup> derogatory terms for Stormfront users.

---

<sup>314</sup> Ibid.

<sup>315</sup> Post by Blue Wolf, 24 January 2014, <https://www.stormfront.org/forum/t1019254-2/>, accessed 12 December 2019.

<sup>316</sup> Post by Cyan Sky, 24 January 2014, <https://www.stormfront.org/forum/t1019254/>, accessed 12 December 2019.

<sup>317</sup> Post by Remenersis, 5 February 2014, <https://www.stormfront.org/forum/t1019254-4/>, accessed 12 December 2019.

<sup>318</sup> Post by Blue Wolf, 24 January 2014, <https://www.stormfront.org/forum/t1019254/>, accessed 12 December 2019.

<sup>319</sup> Post by RedLightning, 23 August 2014, <https://www.stormfront.org/forum/t1019254-4/>, accessed 12 December 2019.

<sup>320</sup> Post by Posen, 23 August 2014 <https://www.stormfront.org/forum/t1019254-4/>, accessed 12 December 2019.

<sup>321</sup> ‘Stormfag’, *Urban Dictionary*, at <https://www.urbandictionary.com/define.php?term=stormfag>, accessed 12 December 2019.



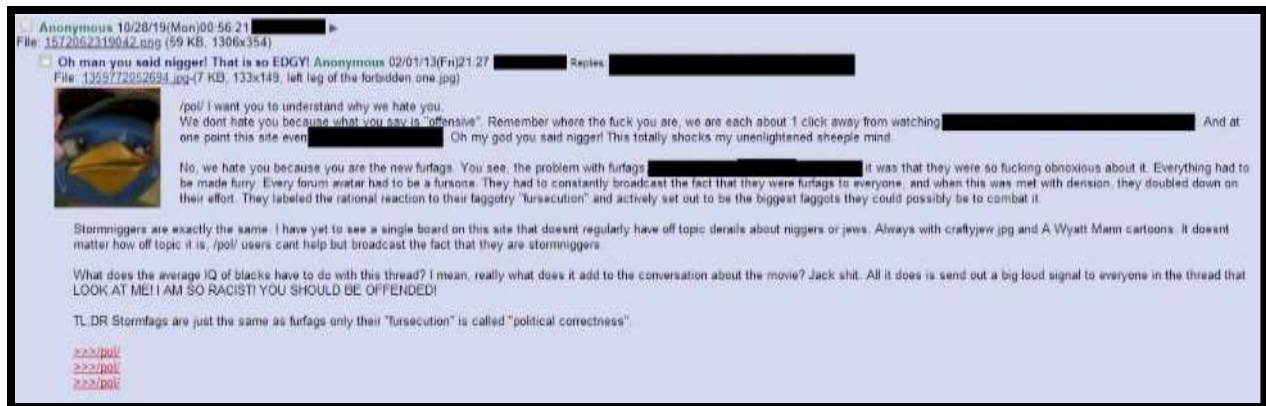


Figure 25 A 2013 post against /pol/ reposted in 2019

There were always Holocaust jokes, but as a result of the infiltration of neo-Nazis, Holocaust denial has become so regular on /pol/ a quick inspection immediately led to a post promoting a Holocaust denial documentary (see Figure 26). The post is titled "New Holocaust Documentary by Ryan Dawson" and provides a link to view the documentary. It is accompanied by a version of the Antisemitic Meme of the Jew.



Figure 26 The Antisemitic Meme of the Jew used in a post promoting a 2019 Holocaust denial documentary on /pol/

The infiltration led to a significant cultural change between /pol/ and the traditional form of more casual antisemitism on 4chan. As a user on 4chan's QA recently explained (see Figure 27), on /b/ when people complained about antisemitic jokes they receive abuse or more jokes, on /pol/ the response is instead "text walls about how the Holocaust didn't happen". The poster explains, it "stops being humor when you put more effort into defending it than the people opposing it".

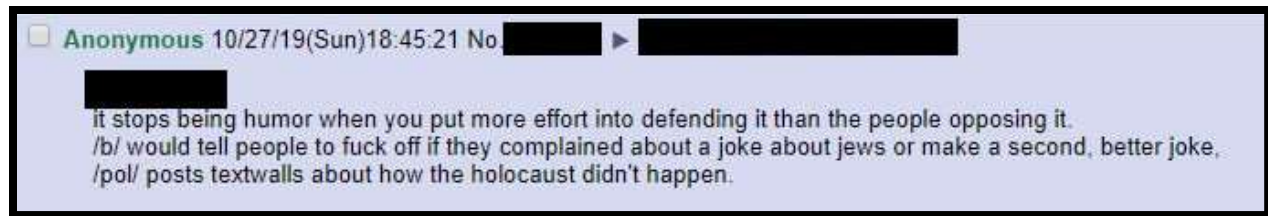


Figure 27 A QA poster on /pol/ going beyond humour

Even on QA, which usually sees very little infiltration from /pol/, a supporter of /pol/ quickly responded to this post by entered into a flame war and then a post saying their life would be “infinitely better when we can start killing you kikes in the streets”. Comments like this directed at violence demonstrate the toxic culture which as emerged within /pol/ and signal a significant shift from the antisemitism of earlier years.



Figure 28 A QA response from a /pol/ supporter

There have been some threads on /pol/ seeking to push back against the takeover by neo-Nazis, but they have been largely unsuccessful. A thread in April 2018 asked “/pol/, can we kick out all the stormniggers and unironic racists? It's getting a bit too autistic here” (Figure 29).<sup>322</sup> The poster later explained, “There's a difference between ironic racism and screeching "OY VEY GAS THE KIKES 1488" about everything” (see Figure 30).<sup>323</sup> Another user agreed saying it is felt a little too serious now, a third added “you realize that there is probably a reason it seems serious right?”.<sup>324</sup> Other responses accuse the poster of being a Jew, various posts share antisemitic and pro-Nazi material. An Australian poster ridiculed the idea of changing the culture on /pol/ and the original poster replied, quite unironically, “Stormfront thought they could, and they pulled it off” (see Figure 32). Part of the shift to greater extremism, however, is demonstrated in this thread by an image post which simply depicts a Jew (represented by the Antisemitic Meme of the Jew) being killed execution style (see Figure 31).

<sup>322</sup> 4plebs, at <https://archive.4plebs.org/pol/thread/167322687/>, accessed 12 December 2019.

<sup>323</sup> Ibid.

<sup>324</sup> Ibid.





Figure 29 /pol/ April 2018 asking to get rid of the neo-Nazis

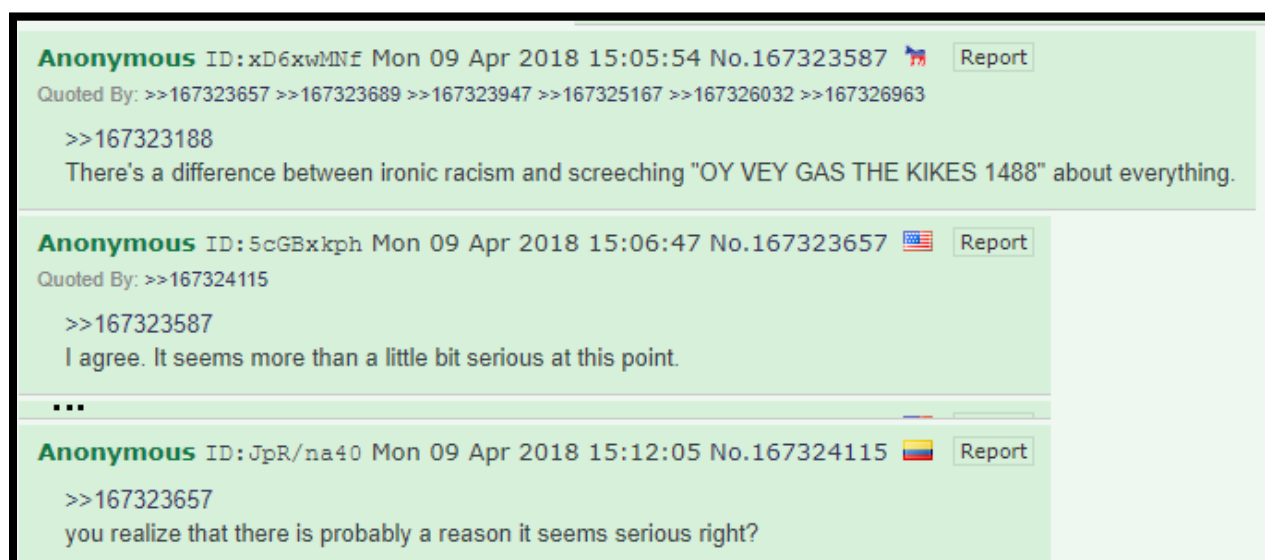


Figure 30 /pol/ post highlighting concern



Figure 31 /pol/ post executing a Jew

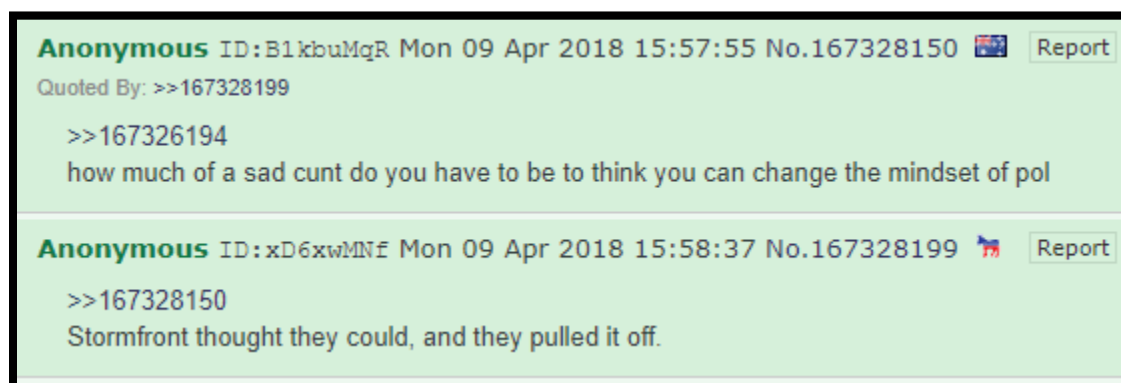



Figure 32 Stormfront changed the culture of /pol/

In another thread calling for the neo-Nazi's to be kicked off /pol/ in November 2018 (see Figure 33), the poster starts their message with a caricature of a post by a neo-Nazi.<sup>325</sup> Another user picks up one line in the impersonation that says "hurr durr I'm going to go out and shoot a bunch of kikes and niggers" and dismisses it saying "name one time this has happened" (see Figure 34). Since this post was made there have been 4 such incidents as documented in this report. 2019 has marked a significant shift in the nature of /pol/ and therefore in the way it needs to be treated.

<sup>325</sup> 4plebs, at <https://archive.4plebs.org/pol/thread/191950533/>, accessed 12 December 2019.

/pol/ - Politically Incorrect - 4chan Index - NSFW Ghost Gallery Stats

Search or insert post number



**Stormnigger Problem** Anonymous ID: ZS00Tdoc [50 / 22 / 40]  
 Sun 04 Nov 2018 11:01:32 No.191950533

View Reply Original Report

Quoted By: >>191950690 >>191950865 >>191951027 >>191951705  
 >>191952179 >>191952305 >>191952455 >>191952864  
 >>191953852 >>191953939 >>191956006 >>191956889  
 >>191957613 >>191957641 >>191960251

>be stormnigger  
 >"hurr durr I'm going to go out and shoot a bunch of kikes and niggers--I mean there's going to be a ((0099099(falseflag009))))00)set up by the ((999090((KIKES)))(()))00P) soon, watch the news!"  
 >\*shoots up synagogue/church\*

>"OH MY HITLER! I KNEW IT! STORMFRONT AND /POL/ ARE ALWAYS RIGHT! GAS THE KIKES RACEWAR NOW!"  
 >"Hello, /pol/ I am that ethnicity you have been brainwashed by other stormniggers to hate. I do this cartoonishly stereotypical thing every day and am actively seeking to personally kill you, every member of your family, your non-existent descendants and your family pet because you're the most bestest special race in the entire universe: White."  
 >"REEEEEEEEEEEEEEEEEEEEEEE! FUCKING [SLUR FOR ETHNIC GROUP] I'M GOING TO GO SHOOT UP A SYNAGOGUE/CHURCH/ BUILD EXPLOSIVES IN MY GARAGE TO KILL YOU!"  
 >Hey! Join my retarded faggot larp! IT'S NOT A FORCED MEME! IF YOU THINK IT'S STUPID AND GAY YOU'RE A FAGGOT (((990000((( KIKE)))099900OPPP))) ((((((9999000000008((SHILL)))009000pp090))  
 >"cough" unite the right 2.0 \*cough\* iotbw 2.0 \*cough\* #frightpower \*cough\*  
 >REEEEEEEEEEEEEEEEEEE! THESE DIDN'T FAIL! FUCK OFF KIKE!  
 It's time to kick the stormniggers out of /pol/.

4MiB, 400x300, hitlers legacy.gif  
 View Same Google iqdb SauceNAO Trace

Figure 33 Call to kick neo-Nazis off /pol/ in November 2018

**Anonymous** ID: Xyj863Yy Sun 04 Nov 2018 12:10:40 No.191957641 Report

Quoted By: >>191958515  
 >>191950533  
 >>"hurr durr I'm going to go out and shoot a bunch of kikes and niggers"

name one time this has happened

Figure 34 Dismissal of the idea of real violence

## 5.4 Gamergate and the Rise of 8chan

'Gamergate' is a catchall for a series of events that consisted mainly of the harassment of female video-game journalists, but also represents a watershed moment in a large-scale online cultural revanchist campaign against political correctness, identity politics and various other so-called 'liberal agendas'.<sup>326</sup>

<sup>326</sup> Nagle, Angela, 2017. *Kill All Normies: Online Culture Wars From 4chan and Tumblr to Trump and the alt-right*, New York: John Hunt Publishing. Online at <https://ebookcentral-proquest->

Gamergate represented a critical juncture that contributed significantly to the unification and galvanisation of previously disparate social groups that would eventually unite under the banner of the 'alt-right',<sup>327</sup> as discussed in the next section of this report.

Gamergate began in 2014 with the harassment of Zoe Quinn, a video game developer, after her ex-boyfriend wrote a blog post that, once amplified by Adam Baldwin's commentary on the matter via his considerable Twitter following, attracted mainstream public attention. It was claimed that Quinn had cheated on her boyfriend in order to advance her career in the videogame industry.<sup>328</sup> This precipitated a series of attacks on Quinn, including 'doxing', the dissemination of personal information online for malicious purposes (e.g., Quinn's home address, phone number, office address and phone number etc.), along with the theft of compromising photographs, the fabrication of compromising photographs, and countless death and rape threats.<sup>329</sup> This pattern of behaviour, more or less enhanced, was replicated and levelled against numerous prominent female figures in the videogame industry.<sup>330</sup> Accompanying the slew of increasingly severe harassment campaigns was a conspiratorial and enduring dialogue about 'journalistic ethics' that seriously considered the possibility of organised, systemic and endemic female manipulation of game reviewers.<sup>331</sup>

Initially 4chan was used as a key staging ground to launch many of these abusive, hateful endeavours that were carried out and clearly attributed by name to 'Gamergate'. The violent misogynistic harassment campaigns of gamergate eventually attracted so much attention from mainstream media and federal law-enforcement agencies that 4chan's administrators banned even *mentioning* Gamergate

---

[com.ez.library.latrobe.edu.au/lib/latrobe/detail.action?docID=4867966](http://com.ez.library.latrobe.edu.au/lib/latrobe/detail.action?docID=4867966), accessed 3 September 2018; Adrienne L. Massanari, 2015. *Participatory Culture, Community, and Play: Learning From Reddit*. New York: Peter Lang Publishing.; Adrienne L. Massanari, 2017. "#Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures", *New Media & Society*, volume 19, number 3, pp. 329-346.; Matthew N. Lyons, 2017. *Ctrl-Alt-Delete: The Origins and Ideology of the Alternative Right*, Political Research Associates, at <https://www.politicalresearch.org/2017/01/20/ctrl-alt-delete-report-on-the-alternative-right/>, accessed 3 September 2018.; Matthew Flisfender, 2018. "'Trump'—What Does the Name Signify? or, Protofascism and the Alt-Right: Three Contradictions of the Present Conjuncture", *Cultural Politics*, volume 14, number 1, pp. 1-19.

<sup>327</sup> Matthew N. Lyons, 2017. *Ctrl-Alt-Delete: The Origins and Ideology of the Alternative Right*, Political Research Associates, at <https://www.politicalresearch.org/2017/01/20/ctrl-alt-delete-report-on-the-alternative-right/>, accessed 3 September 2018, p. 8.; George Hawley, 2017. *Making Sense of the Alt-right*. New York: Columbia University Press, pp. 43-48.; David Neiwert, 2017. *Alt-America: The Rise of the Radical Right in the Age of Trump*, New York: Verso Books, pp. 213-215.

<sup>328</sup> Anastasia Powell & Nicola Henry, 2017. *Sexual Violence In a Digital Age*, London: Palgrave Macmillan, p. 169.

<sup>329</sup> Anastasia Powell & Nicola Henry, 2017. *Sexual Violence In a Digital Age*, London: Palgrave Macmillan, p. 169.

<sup>330</sup> Nagle, Angela, 2017. *Kill All Normies: Online Culture Wars From 4chan and Tumblr to Trump and the alt-right*, New York: John Hunt Publishing. Online at <https://ebookcentral-proquest-com.ez.library.latrobe.edu.au/lib/latrobe/detail.action?docID=4867966>, accessed 3 September 2018.

<sup>331</sup> Shira Chess & Adrienne Shaw, 2015. "A conspiracy of fishes, or, how we learned to stop worrying about #GamerGate and embrace hegemonic masculinity", *Journal of Broadcasting & Electronic Media*, volume 59, number 1, pp. 208-220.



(doing so is still grounds for a permanent ban from 4chan).<sup>332</sup> This resulted in the migration of 4chan-users to the then relatively new splinter-chan known as 8chan.<sup>333</sup>

8chan was created by Fredrick Brennan in October 2013,<sup>334</sup> in response to an increase in moderator activity on 4chan to crackdown on illegal content. It closely mirrors (and in many ways outright copies) 4chan, but is an independent site under different management and promotes itself as a “free-speech-friendly 4chan alternative”.<sup>335</sup> Faced with censorship on 4chan, those involved in Gamergate shifted on mass to 8chan where the misogynistic conspiracy theories were there spearheaded and endured prominently long after the 4chan ban. In fact, the banning of discussion of Gamergate on 4chan, fed 8chan’s exhortations of liberal censorship.<sup>336</sup> The fracture between the chans established some measure of animosity between the platforms, but this was somewhat bridged by the subcultural continuity provided by /pol/ as a dominant and consistent voice across the platforms. With its roots in the conspiracy, bigotry and hate of Gamergate, 8chan grew both larger and increasingly insular and hostile. Unable to cover the costs to keep it running, Brennan sold 8chan to US military veteran Jim Watkins in October 2014,<sup>337</sup> but continued to run the site until he quit in 2016.<sup>338</sup>

8chan became a dedicated forum for misogyny and discussions of perceived widespread misandry, but also expanded beyond the gendered politics of Gamergate to focus on violent extremism directed at a host of targets guided by the socio-political agendas of /pol/’s subculture that dominates the site. The culture in turn was able to become more extreme due to 8chan’s more extreme position on free speech.<sup>339</sup> From its creation until the time it was closed on 16 September 2019, the /pol/ board on 8chan hosted a total of 13,575,873 posts and would usually have between 2,500 and 3,000 unique visitors during a 72 hour period.<sup>340</sup>

---

<sup>332</sup> Nagle, Angela, 2017. *Kill All Normies: Online Culture Wars From 4chan and Tumblr to Trump and the alt-right*, New York: John Hunt Publishing. Online at <https://ebookcentral-proquest-com.ez.library.latrobe.edu.au/lib/latrobe/detail.action?docID=4867966>, accessed 3 September 2018, p. 170.

<sup>333</sup> David Neiwert, 2017. *Alt-America: The Rise of the Radical Right in the Age of Trump*, New York: Verso Books, pp. 235-236.

<sup>334</sup> Ethan Chiel, 2016. “Meet the man keeping 8chan, the world’s most vile website, alive”, *SPLINTER* (19 April), at <https://splinternews.com/meet-the-man-keeping-8chan-the-worlds-most-vile-websit-1793856249>, accessed 12 December 2019.

<sup>335</sup> Patrick Howell O’Neill, 2014. “8chan, the central hive of Gamergate, is also an active pedophile network”, *The Daily Dot* (17 November), at <https://www.dailydot.com/layer8/8chan-pedophiles-child-porn-gamergate/>, accessed 12 December 2019.

<sup>336</sup> Patrick D. Scolyer-Gray, 2019. “Interpreting ‘Artistic Works of Fiction and Falsehood’: A Sociological Analysis of The Production and Consumption of Knowledge on 4chan”, PhD thesis, La Trobe University, Bundoora.

<sup>337</sup> Ben Gilbert, 2019. “The bizarre life of 8chan owner Jim Watkins, the middle-age veteran who decamped to the Philippines and runs a pig farm”, *TECH INSIDER* (6 August), at <https://www.businessinsider.com.au/who-owns-8chan-jim-watkins-life-2019-8?r=US&IR=T>, accessed 12 December 2019.

<sup>338</sup> David Lipson, 2019. “Fred Brennan on the rise and fall of his website 8chan”, 7:30 Report on the ABC, 30 Sep 2019 Transcript: <https://www.abc.net.au/7.30/fred-brennan-on-the-rise-and-fall-of-his-website/11561968>, accessed 12 December 2019.

<sup>339</sup> Ethan Chiel, 2016. “Meet the man keeping 8chan, the world’s most vile website, alive”, *SPLINTER* (19 April), at <https://splinternews.com/meet-the-man-keeping-8chan-the-worlds-most-vile-websit-1793856249>, accessed 12 December 2019.

<sup>340</sup> *Congressional Supplemental Inquiries of 8chan, Submission to the Committee on Homeland Security*, 25 September 2019, p. 2, at <https://d5e10168-1d62-4e43-8269->

8chan is now widely known for hosting a far more radicalized iteration of /pol/-culture that has attracted considerable notoriety for its connections to various violent crimes and terrorism, including playing a large role in the Christchurch shootings and subsequent attacks in Poway and El Paso. By early 2019 Brennan had cut all ties with 8chan and after the mass shooting he went on a media blitz calling for the site he founded to be shutdown.<sup>341</sup>

## 5.5 Harnessing the Culture for Real Politics: The Rise of the Alt-Right

The culture of what became known as the Alt-Right in part grew out of the online culture in places like 4chan and 8chan, and in particular out of /pol/. This was not a grassroots political movement that emerged from the online culture, but rather a deliberate effort by political actors seeking to start a new movement to coopt the online culture, methods and community infrastructure to feed their growth.

The Alt-Right offered to take the political fantasies of some and trolling of others within the /pol/ subculture, and related right-wing online cultures on platforms like reddit, straight into real world politics. There is an overlap between the Alt-Right and these online sub-cultures, but the Alt-Right also including overt white nationalist and neo-Nazis who are not necessarily connected to this online subculture. While using online platforms as a source of material and recruitment, the Alt-Right doesn't support the sub-cultural ethos of anonymity, instead seeking to take their views mainstream so they can be spoken about openly.<sup>342</sup> They shifting their activities to personal accounts on mainstream platforms, and when they were kicked off those platforms, onto a collection of alternative platforms such as Gab and Voat.<sup>343</sup> Unlike the chans, the Alt-Right has leaders with public profiles and often a thirst for media attention.

### 5.5.1 Political origins

The term Alt-Right, or Alternative Right, is a term coined in 2008 in the title of a keynote address for the inaugural meeting of the H.L. Mencken Club.<sup>344</sup> The Club was created as a forum for an "intellectual right" which felt it was being "quarantined" by more traditional conservatives.<sup>345</sup> The leadership of the club included several notable academic racists.<sup>346</sup> Paleoconservative political philosopher Paul Gottfried was the founder of the club, white supremacist Richard Bertrand Spencer the master of ceremonies for

---

[5d58035f234e.filesusr.com/ugd/62f5a3\\_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true](https://5d58035f234e.filesusr.com/ugd/62f5a3_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true), accessed 12 December 2019.

<sup>341</sup> David Lipson, 2019. "Fred Brennan on the rise and fall of his website 8chan", 7:30 Report on the ABC, 30 Sep 2019. Transcript at, <https://www.abc.net.au/7.30/fred-brennan-on-the-rise-and-fall-of-his-website/11561968>, accessed 12 December 2019.

<sup>342</sup> Sean Illing, 2017. "A grad student spent 12 months undercover in Europe's alt-right movement", Vox (29 November), at <https://www.vox.com/policy-and-politics/2017/10/11/16424576/europe-alt-right-nationalism-racism-trump-brexite>, accessed 12 December 2019.

<sup>343</sup> Digital Forensic Research Lab, 2017. "alt-right and alt-social media", Medium (9 September), at <https://medium.com/dfriab/alt-right-and-alt-social-media-4fa23eb2fbd1>, accessed 12 December 2019.

<sup>344</sup> Helen Chernikoff, 2016. "Meet the Jewish 'Paleoconservative' Who Coined The Term 'Alternative Right'", Forward (29 August), at <http://forward.com/news/national/348372/meet-the-jewish-paleoconservative-who-coined-the-term-alternative-right/>, accessed 12 December 2019.

<sup>345</sup> Larry Keller, 2008. "Prominent Racists Attend Inaugural H.L. Mencken Club Gathering, Southern Poverty Law Center (26 November), at <https://www.splcenter.org/hatewatch/2008/11/26/prominent-racists-attend-inaugural-hl-mencken-club-gathering>, accessed 12 December 2019.

<sup>346</sup> Ibid.

the inaugural meeting and anti-immigration activist Peter Brimelow delivered the keynote address.<sup>347</sup> Spencer and Gottfried have been variously credited with coining the term “Alt-Right” at this meeting.

In 2010 Spencer founded the National Policy Institute and its online magazine “Alternative Right” with Paul Gottfried and Peter Brimelow as senior contributing editors.<sup>348</sup> His stated aim was “to forge a new intellectual right-wing that is independent and outside the ‘conservative’ establishment”.<sup>349</sup> This saw a generational shift not only in leadership but also in audience.

### 5.5.2 Harnessing the Online Subculture

The Alternative Right’s supporters were, according to Spencer, those who recognised the “uselessness of mainstream conservatism”, and were comprised of a younger demographic, often recent college graduates.<sup>350</sup> The Alternative Right continued to be linked to white supremacism,<sup>351</sup> but the audience now came from online sources, mainly online forums like 4chan and similar communities on Reddit and Twitter.<sup>352</sup> The /pol/ community was naturally aligned to the Alt-Right and the Alt-Right presented itself as the red-pilled true reality.

The Alt-Right, as it has been manifesting online, is a combination of the traditional far-right, those just in it “for the lulz” looking for amusement, those disillusioned with mainstream politics and those seeking to capitalize on their grasp of online culture. From the neo-Nazi elements, conspiracy theories of Jewish media control and media dishonesty are a staple of the Alt-Right and efforts targeting the media and particularly Jewish journalists led to a significant rise in antisemitism during the US election campaign.<sup>353</sup> While seeking to undermine the mainstream media, the Alt-Right have also been creating “parallel media institutions”,<sup>354</sup> promoting alternative news.<sup>355</sup>

### 5.5.3 Campaigning for Trump

/pol/ and the Alt-Right got behind Donald Trump in the 2016 election. A key symbol of this support became the use of Pepe the Frog. The Pepe cartoon character was created by Matt Furie in 2004 and became an exceptionally popular basis for a vast array of 4chan-memes, and eventually became a popular symbol used by prominent figures in the emergent ‘alt-right’ movement. By 2016, Pepe the Frog had acquired considerable notoriety.

---

<sup>347</sup> Ibid.

<sup>348</sup> Ibid.

<sup>349</sup> Ibid.

<sup>350</sup> ‘Alternative Right’, *Southern Poverty Law Center*, at <https://www.splcenter.org/fighting-hate/extremist-files/ideology/alternative-right>, accessed 12 December 2019.

<sup>351</sup> Ibid.

<sup>352</sup> Ibid.

<sup>353</sup> Lilly Maier, 2016. “Twitter Gives Online Hate Speech Its Biggest Platform — Why?”, *Forward* (18 October), at <http://forward.com/news/352133/twitter-gives-online-hate-speech-its-biggest-platform-why/>, accessed 12 December 2019.

<sup>354</sup> Charlie Warzel, 2017. “The Right Is Building A New Media ‘Upside Down’ To Tell Trump’s Story”, *BuzzFeed* (23 January), at <https://www.buzzfeed.com/charliewarzel/the-right-is-building-a-new-media-upside-down-to-tell-donald>, accessed 12 December 2019.

<sup>355</sup> Andrew Marantz, 2016. “What Happens When You’re Mistaken for America’s Leading Conspiracy Theorist”, *New Yorker* (19 December), at <http://www.newyorker.com/magazine/2016/12/19/what-happens-when-youre-mistaken-for-americas-leading-conspiracy-theorist>, accessed 12 December 2019.



The use of Pepe the Frog by /pol/, however, came first and while it had a multitude of subcultural meanings attached to it, some of them were blatantly antisemitic. Examples of Pepe dressed as a Nazi can be found as early as 2014 (see Figure 35).<sup>356</sup> The name of the uploader of this image to *Know Your Meme*, a user called “jewcrusher88” (“Jew Crusher” and 88 as a symbol for Heil Hitler), is notable and is an example of neo-Nazis seeking to infiltrate mainstream online culture – as we’re previously documented.<sup>357</sup> Nazi-related Pepe images also spread to platforms such as Twitter,<sup>358</sup> and Tumblr (Figure 36).<sup>359</sup>



Figure 35 This Pepe in a Nazi uniform can be seen as early as 2014

<sup>356</sup> jewcrusher88, 2014. “Feels Bad Man / Sad Frog”, *Know Your Meme* (23 August), at <https://knowyourmeme.com/photos/816541-feels-bad-man-sad-frog>, accessed 12 December 2019.

<sup>357</sup> Andre Oboler, 2014. *The Antisemitic Meme of the Jew*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/the-antisemitic-meme-of-the-jew/>, accessed 12 December 2019.

<sup>358</sup> @Xx\_Senpai\_xX, 2015. *Twitter* (11 July), at [https://twitter.com/Xx\\_Senpai\\_xX/status/620088820948598784](https://twitter.com/Xx_Senpai_xX/status/620088820948598784), accessed 12 December 2019.

<sup>359</sup> Premiumpepes, 2015. *Tumblr* (21 April), at <https://premiumpepes.tumblr.com/post/116983043126/super-rare-skinhead-pepe>, accessed 12 December 2019.



Figure 36 Skinhead Pepe on Tumblr in April 2015

The association between Trump and Pepe was started on /pol/ by a Malaysian artist called Maldraw on July 22, 2015.<sup>360</sup> The original image featured Pepe with Trump hair at the US Border with Mexico (see Figure 37). Nazi Pepe, however, continued to be a regular feature on /pol/ around September and early October 2015 as seen in Figure 38, Figure 39 and Figure 40.

<sup>360</sup> 2015. *4Plebs* (22 July), at <http://archive.4plebs.org/pol/thread/48390660#48392652>, accessed 12 December 2019.; 2016. *4Plebs* (15 September) <http://archive.4plebs.org/pol/thread/89025240/>, accessed 12 December 2019.; WarriorTang, 2016. "Nazi Pepe Controversy", *Know Your Meme* (27 September), at <https://knowyourmeme.com/memes/events/nazi-pepe-controversy>, accessed 12 December 2019.

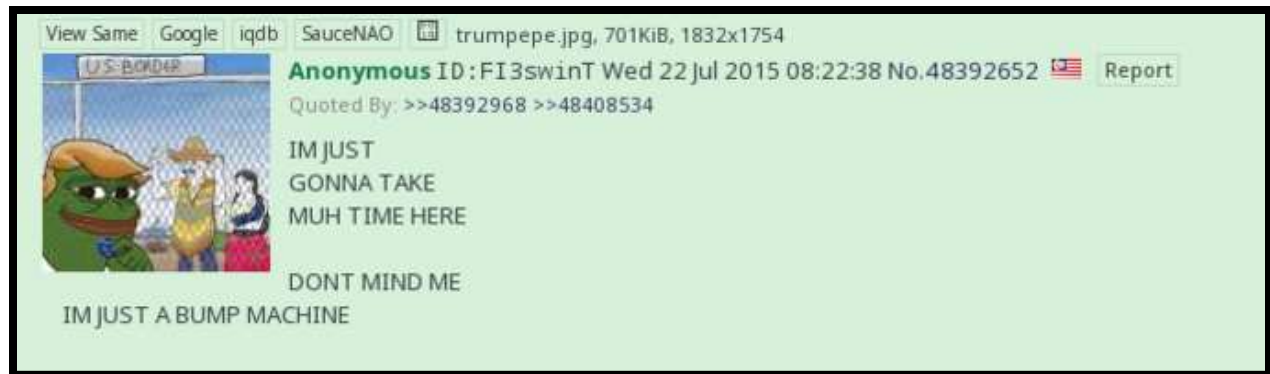


Figure 37 First appearance of Trump as Pepe

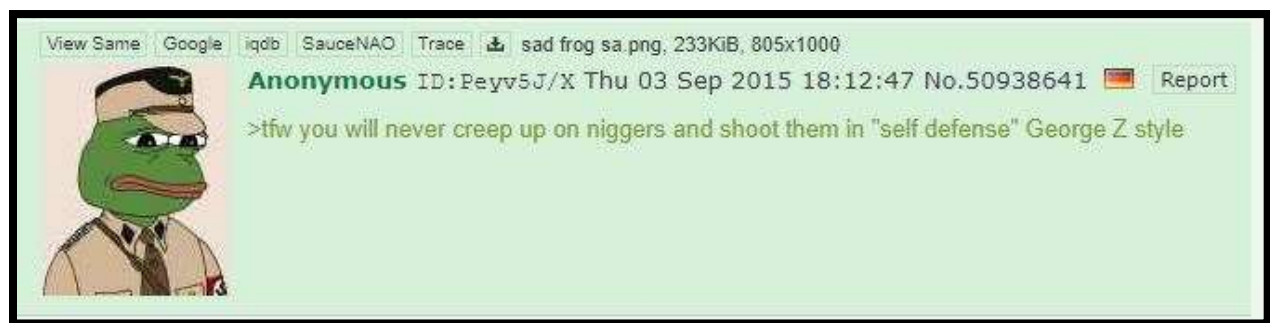


Figure 38 Pepe on /pol/ 3 September 2015



Figure 39 Pepe on /pol/ 5 October 2015



Figure 40 Pepe on /pol/ 5 October 2015

On the 13<sup>th</sup> of October 2015, Donald Trump re-tweeted a rendering of himself as Pepe the Frog along with the caption, “you can’t stump the trump” (Figure 41). This tweet created an indelible link between Trump and the emerging alt-right.<sup>361</sup> Some scholars have suggested that Trump may not have understood the meaning or implications of his tweet, symbolically or otherwise.<sup>362</sup> Regardless, from the perspective of many 4chan-users, Trump’s appropriation of Pepe signalled the gravity of 4chan’s cultural significance.



Figure 41 Candidate Trump retweeting an image of Pepe as President Trump

<sup>361</sup> Patrick D. Scolyer-Gray, 2019. “Interpreting ‘Artistic Works of Fiction and Falsehood’: A Sociological Analysis of The Production and Consumption of Knowledge on 4chan”, PhD thesis, La Trobe University, Bundoora, p. 238; Abby Ohlheiser, 2016. “Why Pepe the Frog’s Nazi phase doesn’t worry his creator”, *The Washington Post* (15 September), at <https://www.washingtonpost.com/news/the-intersect/wp/2016/09/14/why-pepe-the-frogs-nazi-phase-doesnt-worry-his-creator/>, accessed 12 December 2019.

<sup>362</sup> George Hawley, 2017. *Making Sense of the Alt-right*. New York: Columbia University Press, p. 121.

Although plausible that Trump was unaware of Pepe's symbolic significance, the same cannot be said for others, who rapidly identified the meme as well as its associations with /pol/ and the alt-right.

Hillary Clinton attempted to make use of Trump's ties to Pepe and on the 12<sup>th</sup> of September 2016 published a full-page explainer on Pepe the Frog on her Campaign website (see Figure 42). Tweeted only days after Clinton posted a Pepe the Frog explainer on her Campaign website, the visibility of celebrities like Cher tweeting about the symbolic associations between Pepe and Nazism, as well as the alt-right (Figure 43), shows how this knowledge had entered mainstream awareness.

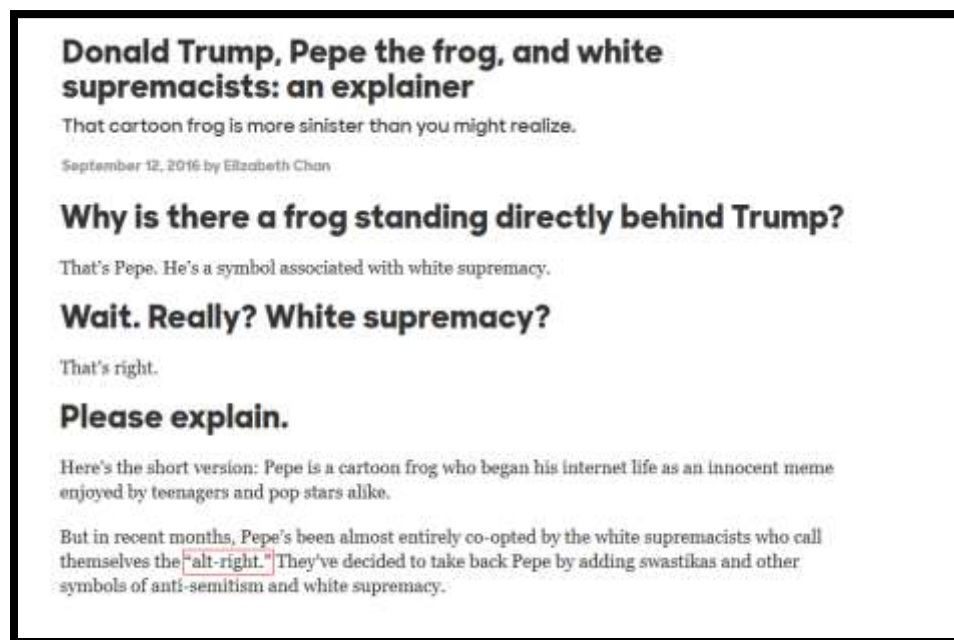


Figure 42 Clinton's pepe explainer from her website.



Figure 43 Cher tweeting on 16 September 2016 regarding the association between Pepe and neo-Nazism

The public response to Pepe was said to have “...delighted [4chan] denizens, who saw it as an example of ‘meme magic’ and a symbol of their significance”.<sup>363</sup> It also increased Trump’s interest in generating political capital by trolling mainstream politics. Trump implicitly endorsing politically incorrect trolling by using Pepe imagery as part of his more explicitly politically incorrect social media comments. This became part of a larger tactical effort creating a “spreadable spectacle” in which polarising views, popularist rhetoric and extreme opinion were spread through the use of disinformation, appropriation of online culture and the mainstream media’s willingness to perpetuate partisanship.<sup>364</sup> /pol/ were ecstatic at Trump’s eventual election win.<sup>365</sup>

Since the election, some close to both the Trump team and Spencer, like Charles C. Johnson, openly admit both to trolling and promoting conspiracy theories as a means of garnering votes.<sup>366</sup> Milo Yiannopoulos, technology editor for Breitbart News and a key protagonist in the cyber-harassment campaign targeting women in the video game industry (Gamergate), as well as an anti-Islam

<sup>363</sup> Alice Marwick and Rebecca Lewis, 2017. *Media Manipulation and Disinformation Online*. New York: Data & Society. Online at [https://datasociety.net/pubs/oh/DataAndSociety\\_MediaManipulationAndDisinformationOnline.pdf](https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf), accessed 18 December 2019. p. 22.

<sup>364</sup> Paul Mihailidis, Samantha Viotty, “Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in ‘Post-Fact’ Society” (2017) 61(4) *American Behavioral Scientist*.

<sup>365</sup> Abby Ohlheiser, 2016. “We actually elected a meme as president’: How 4chan celebrated Trump’s victory”, *The Washington Post* (10 November), at <https://www.washingtonpost.com/news/the-intersect/wp/2016/11/09/we-actually-elected-a-meme-as-president-how-4chan-celebrated-trumps-victory/>, accessed 12 December 2019.

<sup>366</sup> Ben Schreckinger, 2017. “The Alt-Right Comes to Washington”, *Politico* (January), at <http://www.politico.com/magazine/story/2017/01/alt-right-trump-washington-dc-power-milo-214629>, accessed 12 December 2019.



campaigner, was another key figure in the Alt-Right.<sup>367</sup> The far-right website *The Daily Stormer* had a site banner which said it was the “The World's Most Visited Alt-Right Website”.<sup>368</sup> Andrew Anglin who runs the site represents the neo-Nazi element in the Alt-Right and a link to the /pol/ base. He rejected a claim in the Washington Post that the Alt-Right’s “goal is often offensiveness for the sake of offensiveness in the way that many young white men embrace” responding, “No it isn’t. The goal is to ethnically cleanse White nations of non-Whites and establish an authoritarian government. Many people also believe that the Jews should be exterminated”.<sup>369</sup>

#### 5.5.4 Implosion

The Alt-Right was rapidly gaining steam until a National Policy Institute conference at the Ronald Reagan building in November 2016, just days after the election.<sup>370</sup> At the event, after media were asked to leave, Spencer was caught on film raising his arm and proclaiming, “Hail Trump, hail our people, hail victory!” as several attendees responded with Nazi salutes.<sup>371</sup> This open Nazism was the start of split in the Alt-Right,<sup>372</sup> and the emergency of what became known as the “New Right”,<sup>373</sup> or as Richard Spencer and the Alt-Right call them, the “Alt-Lite”.<sup>374</sup> These are people who had been part of the Alt Right but rejected the overt association with white nationalism and neo-Nazism. As Lucian Wintrich explained, the term alt-right had been “adopted by libertarians, anti-globalists, classical conservatives, and pretty much everyone else who was sick of what had become of establishment conservatism” but when “Richard

---

<sup>367</sup> ‘Alternative Right’, *Southern Poverty Law Center*, at <https://www.splcenter.org/fighting-hate/extremist-files/ideology/alternative-right>, accessed 12 December 2019.

<sup>368</sup> Amrita Khalid, 2016. “Donald Trump and the rise of the alt-right”, *Daily Dot* (1 September), at <http://www.dailydot.com/layer8/what-is-the-alt-right/>, accessed 12 December 2019.

<sup>369</sup> Keegan Hanks, 2016. “Whose Alt-Right Is It Anyway?”, *Southern Poverty Law Center* (25 August), at <https://www.splcenter.org/hatewatch/2016/08/25/whose-alt-right-it-anyway>, accessed 12 December 2019.

<sup>370</sup> Ben Schreckinger, 2017. “The Alt-Right Comes to Washington”, *Politico* (January), at <http://www.politico.com/magazine/story/2017/01/alt-right-trump-washington-dc-power-milo-214629>, accessed 12 December 2019.

<sup>371</sup> Daniel Lombroso and Yoni Appelbaum, 2016. “‘Hail Trump!': White Nationalists Salute the President-Elect”, *The Atlantic* (21 November), at <https://www.theatlantic.com/politics/archive/2016/11/richard-spencer-speech-npi/508379/>, accessed 12 December 2019.

<sup>372</sup> Ben Schreckinger, 2017. “The Alt-Right Comes to Washington”, *Politico* (January), at <http://www.politico.com/magazine/story/2017/01/alt-right-trump-washington-dc-power-milo-214629>, accessed 12 December 2019.; Andrew Marantz, 2017. “The Alt-Right Branding War Has Torn the Movement in Two”, *The New Yorker* (6 July), at <https://www.newyorker.com/news/news-desk/the-alt-right-branding-war-has-torn-the-movement-in-two>, accessed 12 December 2019.

<sup>373</sup> Justin Wm. Moyer and Perry Stein, 2017. “‘Alt-right’ and ‘alt-lite’? Conservatives plan dueling conservative rallies Sunday in D.C.”, *Washington Post* (23 June), at [https://www.washingtonpost.com/local/alt-right-and-alt-lite-conservatives-plan-dueling-conservative-rallies-sunday-in-dc/2017/06/22/242d8de2-56bd-11e7-9fb4-fa6b3df7bb8a\\_story.html](https://www.washingtonpost.com/local/alt-right-and-alt-lite-conservatives-plan-dueling-conservative-rallies-sunday-in-dc/2017/06/22/242d8de2-56bd-11e7-9fb4-fa6b3df7bb8a_story.html), accessed 12 December 2019.; Andrew Marantz, 2017. “The Alt-Right Branding War Has Torn the Movement in Two”, *The New Yorker* (6 July), at <https://www.newyorker.com/news/news-desk/the-alt-right-branding-war-has-torn-the-movement-in-two>, accessed 12 December 2019.

<sup>374</sup> Justin Wm. Moyer and Perry Stein, 2017. “‘Alt-right’ and ‘alt-lite’? Conservatives plan dueling conservative rallies Sunday in D.C.”, *Washington Post* (23 June), at [https://www.washingtonpost.com/local/alt-right-and-alt-lite-conservatives-plan-dueling-conservative-rallies-sunday-in-dc/2017/06/22/242d8de2-56bd-11e7-9fb4-fa6b3df7bb8a\\_story.html](https://www.washingtonpost.com/local/alt-right-and-alt-lite-conservatives-plan-dueling-conservative-rallies-sunday-in-dc/2017/06/22/242d8de2-56bd-11e7-9fb4-fa6b3df7bb8a_story.html), accessed 12 December 2019.



Spencer came along, throwing up Nazi salutes and claiming that he was the leader of the alt-right, he effectively made the term toxic” which caused others to “abandoned using it in droves”.<sup>375</sup>

The split became more evident in June 2017 with competing rallies in Washington DC. The “Freedom of Speech Rally” had been planned at the Lincoln Memorial, but after Richard Spencer was announced as a surprise speaker, two other speakers, Jack Posobiec and Laura Loomer, pulled out and refused to share a platform with him.<sup>376</sup> Posobiec instead organised the “Rally Against Political Violence” to occur at the same time in front of the White House.<sup>377</sup> The Alt-Lite, like the Alt-Right, embraces misogyny and xenophobia while opposing “the left” and “political correctness”.<sup>378</sup> Where the Alt-Right promotes the supremacy of White Nationalism, the Alt-Lite, according to Gavin McInnes, promotes “civic nationalism” and the superiority of “Western values”.<sup>379</sup>

The real implosion for the Alt-Right came with the *Unite the Right* rally in Charlottesville, Virginia, on the 11–12 of August 2017. The rally was organised by groups which included *The Daily Stormer* and the *National Policy Institute*.<sup>380</sup> The rally was intended to mark the shift of the Alt-Right from an online movement to political force in the national spotlight.<sup>381</sup> Hundreds of far-right activists attended along with a large counter protest.<sup>382</sup> Heather Heyer, a counter-demonstrator, was killed when a 22 year old a self-professed neo-Nazi drove his car into the crowd in what a judge described as “an act of terror”.<sup>383</sup> Hayer’s murder and the evidence of racism, hate and violence shocked America and led to a strong response with far-right protestors being identified, shunned by their families and in some cases fired

---

<sup>375</sup> Andrew Marantz, 2017. “The Alt-Right Branding War Has Torn the Movement in Two”, *The New Yorker* (6 July), at <https://www.newyorker.com/news/news-desk/the-alt-right-branding-war-has-torn-the-movement-in-two>, accessed 12 December 2019.

<sup>376</sup> Ibid.

<sup>377</sup> Ibid.

<sup>378</sup> ‘From Alt Right to Alt Lite: Naming the Hate’, *Anti-Defamation League*, at <https://www.adl.org/resources/backgrounders/from-alt-right-to-alt-lite-naming-the-hate>, accessed 12 December 2019.

<sup>379</sup> Andrew Marantz, 2017. “The Alt-Right Branding War Has Torn the Movement in Two”, *The New Yorker* (6 July), at <https://www.newyorker.com/news/news-desk/the-alt-right-branding-war-has-torn-the-movement-in-two>, accessed 12 December 2019.

<sup>380</sup> Dara Kerr, 2017. “White supremacist parties? Airbnb says not in my house”, *cnet* (9 August), at <https://www.cnet.com/news/airbnb-says-no-white-supremacist-parties-in-my-house/>, accessed 12 December 2019.

<sup>381</sup> Christa Case Bryant & Patrik Jonsson, 2018. “Jason Kessler and the ‘alt-right’ implosion after Charlottesville”, *The Christian Science Monitor* (9 August), at <https://www.csmonitor.com/USA/Politics/2018/0809/Jason-Kessler-and-the-alt-right-implosion-after-Charlottesville>, accessed 12 December 2019.

<sup>382</sup> Cameron McWhirter, 2018. “A Year After Charlottesville, the Alt-Right Movement Frays”, *Wall Street Journal* (8 August), at <https://www.wsj.com/articles/a-year-after-charlottesville-the-alt-right-movement-frays-1533720660>, accessed 12 December 2019.

<sup>383</sup> Gary Robertson, 2019. “Neo-Nazi gets second life sentence in murder of protester in Virginia”, *Reuters* (15 July), at <https://www.reuters.com/article/us-virginia-protests/neo-nazi-gets-second-life-sentence-in-murder-of-protester-in-virginia-idUSKCN1UA0TV>, accessed 12 December 2019.

from their jobs.<sup>384</sup> There was also a crackdown by social media companies making further organising more difficult.<sup>385</sup> The movement largely imploded.<sup>386</sup>

While there remains an overlap between people who would identify as Alt-Right or as neo-Nazis and some members of /pol/, the overlap is only partial. The Alt-Right took on a life of its own and shifted to other forums such as Gab, and while it struggles in the United States, evidence suggests it is growing in Europe.<sup>387</sup> The toxic culture on /pol/, meanwhile, is less coherent ideologically and more willing to encourage and celebrate violence for its own sake. The targeting of Christians in Halle in particular is inconsistent with the US style Alt-Right ideology. In /pol/ we see a culture in which the value of life is reduced and there is a presumption of a social acceptability to cause death for its own sake.

## 5.6 Terrorism on 8chan's /pol/

In 2019 /pol/ on 8chan was used three times to announce terrorist attacks and share the attacker's manifestos. In two of the attacks, links to livestreams on Facebook invited the /pol/ community to become an audience to the attack in real time. The attacks all had elements indicating a submergence in /pol/'s subculture. This raises questions about the responsibility of 8chan and /pol/ and whether the evidence of repeated serious harm is enough to justify action both in the United States and in other countries to prevent further harm. In this section the three attacks prior to Halle are discussed, but it should be remembered that the Halle attack also has references back to /pol/ on 8chan.

---

<sup>384</sup> Christa Case Bryant & Patrik Jonsson, 2018. "Jason Kessler and the 'alt-right' implosion after Charlottesville", *The Christian Science Monitor* (9 August), at <https://www.csmonitor.com/USA/Politics/2018/0809/Jason-Kessler-and-the-alt-right-implosion-after-Charlottesville>, accessed 12 December 2019.

<sup>385</sup> Cameron McWhirter, 2018. "A Year After Charlottesville, the Alt-Right Movement Frays", *Wall Street Journal* (8 August), at <https://www.wsj.com/articles/a-year-after-charlottesville-the-alt-right-movement-frays-1533720660>, accessed 12 December 2019.

<sup>386</sup> Christa Case Bryant & Patrik Jonsson, 2018. "Jason Kessler and the 'alt-right' implosion after Charlottesville", *The Christian Science Monitor* (9 August), at <https://www.csmonitor.com/USA/Politics/2018/0809/Jason-Kessler-and-the-alt-right-implosion-after-Charlottesville>, accessed 12 December 2019.; Cameron McWhirter, 2018. "A Year After Charlottesville, the Alt-Right Movement Frays", *Wall Street Journal* (8 August), at <https://www.wsj.com/articles/a-year-after-charlottesville-the-alt-right-movement-frays-1533720660>, accessed 12 December 2019.

<sup>387</sup> 2019. "How social media and tech fuel the far right, explained", *TRT World* (4 September), at <https://www.trtworld.com/magazine/how-social-media-and-tech-fuel-the-far-right-explained-29517>, accessed 12 December 2019.

### 5.6.1 Christchurch

On March 15<sup>th</sup> 2019, a terrorist attack in Christchurch, New Zealand, led to the death of 51 people. They were shot by a lone gunman who targeted two mosques during Friday prayers. The gunman, Brenton Harrison Tarrant, was an Australian citizen living in New Zealand.

The attack started with a post to /pol/ on 8chan (see Figure 44).<sup>388</sup> The post linked to a Facebook profile and said the poster would be live streaming an attack “against the invaders”. It said good bye in case he didn’t make it.

Given the high level of anonymity that usually exists, that combination of a link to a social media account, a threat of attack and a goodbye, should have triggered alarm bells for many, and should certainly have done so for any law enforcement officer who might have been monitoring the forums. However, since it was posted immediately before the attack, even if it were observed and action had been taken immediately, the exceptionally short notice limits the options afforded to any quick response counter-terrorism strategy.

The post provided links to a number of articles by Tarrant including his manifesto explaining his political motivations and seeking to answer any questions in case he didn’t survive. The attack, envisaged as a possible suicide attack, was designed to make him a martyr. He wanted his words to spread and become part of the cannon of far-right literature available online; the sort of literature that he himself had read, and the kind of material he had consumed on 8chan that had contributed to his radicalization.

A “board volunteer” for /pol/ (one of 5 moderators of the /pol/ board) removed the attacker’s post 2 hours and 49 minutes after it went up according to evidence given to Congress based on the server



Figure 44 Post on 8chan's /pol/ announcing the Christchurch attacks.

<sup>388</sup> Andre Oboler, 2019. *New Zealand Terrorist Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/new-zealand-terrorist-attack/>, accessed 12 December 2019.

logs.<sup>389</sup> Little happened to 8chan after this first attack, despite the use of the platform to announce the attack and clear evidence of a connection to the online sub-culture, such as the reference to “stop shitposting” and “make a real life effort post”, in the message. The attack led to a significant international response including the creation of the Christchurch Call.

## 5.6.2 Poway

A little over a month after the mass casualties of Christchurch, on the 27<sup>th</sup> of April 2019, John Timothy Earnest entered a Synagogue in Poway California armed with an AR-15 type semi-automatic rifle, and opened fire.<sup>390</sup> Earnest followed the same pattern of behavior seen in Christchurch. Earnest posted an announcement to 8chan’s /pol/ when his attack was imminent, along with links to a livestream on Facebook, an ‘open letter’ (manifesto) that he posted to two different sites, as well as a playlist Earnest thought featured “awesome tunes” that he appears to have intended to play during the attack over livestream [see Figure 24].



Figure 45 The Original Post (OP) made to 8chan immediately prior to the Poway shooting.

He shot and killed one woman and wounded the attending Rabbi, another man, and an 8-year-old girl. The assault was cut-short when Earnest’s weapon jammed after firing less than the 10-round capacity of one Smith & Wesson MP15 magazine, prompting a hasty retreat from the scene. Earnest was arrested soon after without incident, with police retrieving a combat utility vest outfitted with 5 spare fully loaded magazines. Clearly, Earnest had intended to carry out a much more deadly attack, considering he was armed with around 60 rounds in total. Earnest had also chosen the last day of Passover for his

<sup>389</sup> Congressional Supplemental Inquiries of 8chan, Submission to the Committee on Homeland Security, 25 September 2019, p. 3, at [https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3\\_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true](https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true), accessed 12 December 2019.

<sup>390</sup> Andre Oboler, 2019. *San Diego Synagogue Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/san-diego-synagogue-attack/>, accessed 12 December 2019.

attack, indicating a conscious decision to find a time to attack when a larger than usual number of Jews were likely to be in attendance at the synagogue.

This foreshadows the logic behind the Halle attack, which was carried out on Yom Kippur, but this is only one of several linkages between the attacks, 8chan and /pol/. The reaction to the original post featured in the two reply-posts visible in Figure 45 includes several subcultural references attributable to the \*chans and /pol/. “Based” is slang used on 4chan and 8chan to refer to things that are, put simply, ‘good’, but the term also has additional connotations, and is usually reserved as a means of ascribing (roughly) attributes of excellence to individuals. “Get the high score” is a cultural trope popular on platforms, including but not limited to the chans, that has found renewed significance and popularity on /pol/ and 8chan.

This phrase harks back to the niche interests (i.e., ‘high scores’ in *video games*) inscribed in the board cultures of the platforms from which /pol/ originates, and it is commonly used by /pol/-users to express affirmation or encouragement to achieve something to a high standard. Since chan culture has shifted away from sarcastic/ironic deployments of hate speech, and particularly given the context of 8chan, the use of the phrase here should be interpreted to mean ‘kill as many Jews as possible’. Additional references to videogames are scattered throughout the playlist in the original post, which includes music from the soundtracks of popular titles such as *Halo: Combat Evolved* and *The Last of Us*. The juxtaposition of videogame terminology and exhortations to commit mass murder is not accidental and reflects an increasingly entrenched devaluation of human life on /pol/ (i.e. a real murder is treated the same as a kill in a video game).

Much the same as with Christchurch, the Poway attack’s original post features many more distinctive subcultural markers that are readily traced to the idiosyncrasies of \*chan and /pol/’s subcultures, with even more distributed throughout the post. The use of “greentext” in a reply-post as well as references to “meme magic” and “redpill threads” all clearly point to the attacker’s connection to /pol/’s subcultural productions. Indeed, the scepticism of other 8chan-users as exemplified in the reply-post “literal spam” reflects the additional problem presented by the ambiguity of fully-anonymous online spaces which have developed subcultural norms and expectations that promote a combination of suspicion, cynicism and scepticism.

A “board volunteer” for /pol/ (one of 5 moderators of the /pol/ board) removed the attacker’s post 12 minutes after it went up according to evidence given to Congress based on the server logs.<sup>391</sup> A tweet at the time had claimed it was removed in under 10 minutes.<sup>392</sup> This is a fast removal, but even so it allowed enough time for images of the post, along with the links it provided to the manifesto, to spread.

---

<sup>391</sup> *Congressional Supplemental Inquiries of 8chan, Submission to the Committee on Homeland Security*, 25 September 2019, p. 3, at [https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3\\_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true](https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true), accessed 12 December 2019.

<sup>392</sup> @Infinitetechan, 2019. *Twitter* (28 April), at <https://twitter.com/infinitetechan/status/1122494322283167745>, accessed 12 December 2019.





Figure 46 8chan removal of Poway attackers post

The links in the post pointed to copies of the manifesto in PDF form at MediaFire and in text only form at Pastebin. The Online Hate Prevention Institute verified those links were still working around 20 hours after the attack and contacted the companies to request they remove the content. Mediafire took swift action and had already removed the file 4hours later when we first re-checked the link. Within 24 hours of our report being made they had followed up with us via e-mail to report on the actions they had taken. Pastebin was slower to respond and that copy remained live for around 50 hours after the attack. Pastebin did not meet its own goal of responding to complaints within 24 hours and took a few hours more than this to take action on our report. The delay allows the content to be viewed by far more people as shown in Figure 47.

Time since upload	21 hours	24 hours	50 hours
Reads on Paste Bin	53,118	63,500	75,950

Figure 47 Reads on Pastebin of Poway attacker's manifesto

At the time we stated that that countries such as Australia may need to consider blocking access to 8chan so long as it continues to “provide a forum for such radicalisation that leads to violence”.<sup>393</sup> We also said that:

*Blocking sites should be an absolute last resort, but sites running technology designed to make the job of police impossible, and with a track record of inciting and being part of deadly violent extremist attacks, cross that threshold. The effort to incite further attacks from people on /pol/, as stated in the manifesto, makes this a case of a clear and present danger.*

*8Chan may consider suspending /pol/ in order to avoid such government responses. Another option would be far greater cooperation with police, not just in the US, but internationally. That would require changes to the software to enable a far greater*

<sup>393</sup> Andre Oboler, 2019. *San Diego Synagogue Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/san-diego-synagogue-attack/>, accessed 12 December 2019.

*and longer term retention of data. Even so, greater moderation action against the hate that leads to extremism may well be needed.*

---

### 5.6.3 El Paso, the closure of 8Chan and the Congressional Inquiry

On the 3<sup>rd</sup> of August 2019, Patrick Crusius shot and killed 22 people and wounded 26 others outside a Walmart in El Paso Texas. Following what has now become the Standard Operating Procedure (SOP) for violent online extremism borne out of 8chan and /pol/, he posted his manifesto to 8chan's /pol/ prior to commencing his assault.<sup>394</sup> The location of the attack was chosen because of its proximity to Mexico and high numbers of Mexican tourists known to cross the border nearby, and despite being an 11 hour drive from Dallas where Crusius lived.

A "board volunteer" for /pol/ (one of 5 moderators of the /pol/ board) removed the attacker's post 45 minutes after it went up according to evidence given to Congress based on the server logs.<sup>395</sup>

In the wake of the violence and public outrage (as well as a lawsuit brought against Watkins, Brennen and Matthew Prince, the CEO of CloudFlare), 8chan was pressured into shutting down<sup>396</sup>, and was driven off the surface web and ultimately offline when hosting providers and services such as Cloudflare ceased providing services to 8chan.<sup>397</sup> Watkins was also subpoenaed by the United States House Committee on Homeland Security on the 5<sup>th</sup> of September,<sup>398</sup> where he agreed to keep 8chan offline until "tools were developed to counter illegal content".<sup>399</sup>

---

<sup>394</sup> Julia Carrie Wong, 2019. "8chan: the far-right website linked to the rise in hate crimes", *The Guardian* (5 August), at <https://www.theguardian.com/technology/2019/aug/04/mass-shootings-el-paso-texas-dayton-ohio-8chan-far-right-website>, accessed 12 December 2019.

<sup>395</sup> *Congressional Supplemental Inquiries of 8chan, Submission to the Committee on Homeland Security*, 25 September 2019, p. 3, at [https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3\\_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true](https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true), accessed 12 December 2019.

<sup>396</sup> J. Blackburn, N. McGarrity & K. Roach, 2019. "Understanding and responding to right wing terrorism", *Journal of Policing, Intelligence and Counter Terrorism*, volume 14, number 3, pp. 183-190.

<sup>397</sup> Elizabeth Findell and Erin Ailworth, 2019. "Victim's Family Sues Accused El Paso Shooter, His Family and 8chan", *The Wall Street Journal* (30 October), at <https://www.wsj.com/articles/victims-family-sues-accused-el-paso-shooter-his-family-and-8chan-11572484530>, accessed 12 December 2019.

<sup>398</sup> Bennie G. Thompson and Mike Rogers, 2019. "Thompson & Rogers Joint Statement After 8chan Deposition", *Committee on Homeland Security, US House of Representative* (5 September), at <https://homeland.house.gov/news/press-releases/thompson-and-rogers-joint-statement-after-8chan-deposition>, accessed 12 December 2019.

<sup>399</sup> Oscar Gonzalez, 2019. "8chan, 8kun, 4chan, Endchan: What you need to know", *cnet* (7 November), at <https://www.cnet.com/news/8chan-8kun-4chan-endchan-what-you-need-to-know-internet-forums/>, accessed 12 December 2019.





Figure 48 Crusius' OP, posted to 8chan shortly before he opened fire on a crowded Walmart, killing and wounding dozens.

A written submission to Congress by Watkins' lawyer seeks to present 8chan as "careful and responsible" and claims it "has never tolerated illegal speech and has a consistent track record of working with law enforcement agencies when appropriate".<sup>400</sup> The statement says "8chan has taken steps to improve its ability to identify illegal content and to act more quickly in doing so. To these ends, it hopes to be of continued assistance to law enforcement officers in times of need".<sup>401</sup> It also claims "8chan is the only platform featuring a full commitment to free speech" and that only "a small minority of users post hateful and ignorant items".<sup>402</sup>

While stating that "we understand that the restriction of some speech is necessary",<sup>403</sup> the 8chan submission makes it clear that this only applies to content which is unlawful in the United States. The United States is an exception internationally as the First Amendment to the United States Constitution has been held by the Supreme Court to also apply to hate speech. That means laws seeking to make hate speech illegal are in the United States unconstitutional. This does not prevent US companies from voluntarily creating and enforcing community standards under which hate speech is banned, but they cannot be forced to do by US law makers.

The US position is exceptional as can be seen in the reservation the United States lodged when ratifying the *International Convention on the Elimination of All Forms of Racial Discrimination* in 1994 (28 years after first signing the treaty).<sup>404</sup>

<sup>400</sup> *Congressional Primer on 8chan*, Committee on Homeland Security 8chan Inquiry, Submission to the Committee on Homeland Security, 4 September 2019, p. 1, at <https://www.benjaminbarr.com/news-updates> with the submission at [https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3\\_f869c81d6bcb495ebdd137776542fe11.pdf](https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3_f869c81d6bcb495ebdd137776542fe11.pdf), accessed 12 December 2019.

<sup>401</sup> Ibid.

<sup>402</sup> Ibid.

<sup>403</sup> Ibid.

<sup>404</sup> *International Convention on the Elimination of All Forms of Racial Discrimination*, opened for signature 21 December 1965, 660 UNTS 195 (entered into force 4 January 1969). Ratifications and reservations online at, [https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=IV-2&chapter=4&clang=en#EndDec](https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-2&chapter=4&clang=en#EndDec), accessed 12 December 2019.

---

*The Senate's advice and consent is subject to the following reservations: (1) That the Constitution and laws of the United States contain extensive protections of individual freedom of speech, expression and association. Accordingly, the United States does not accept any obligation under this Convention, in particular under articles 4 and 7, to restrict those rights, through the adoption of legislation or any other measures, to the extent that they are protected by the Constitution and laws of the United States.*

---

The rejected article 4 says that states will “condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form”.<sup>405</sup> It also says that states will make an offence punishable by law “all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts”.<sup>406</sup> This is what other countries have accepted, but the United States has rejected. Article 7, also rejected by the United States, is an obligation on states to combat prejudice leading to racial discrimination through education.

This view is in stark contrast to, for example, the Council of Europe who adopted the “Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems” in 2003.<sup>407</sup> The Additional Protocol commits states to pass legislation to criminalise “distributing, or otherwise making available, racist and xenophobic material to the public through a computer system”,<sup>408</sup> making threats against a person or group on the basis of “race, colour, descent or national or ethnic origin, as well as religion”.<sup>409</sup>

8chan is aware the US position is exceptional but made clear its position that it won't limit speech unless it is unlawful in the United States. This is another way of saying it will intentionally do nothing to prevent the spread of hate speech and incitement to hate. The submission to congress explains:<sup>410</sup>

---

*My company has no intention of deleting constitutionally protected hate speech. I feel the remedy for this type of speech is counter speech, and I'm certain that this is the view of the American justice system. This may be a contrary opinion to our friends*

---

<sup>405</sup> *International Convention on the Elimination of All Forms of Racial Discrimination*, adopted and opened for signature and ratification by General Assembly resolution 2106 (XX) of 21 December 1965, entry into force 4 January 1969, at <https://www.ohchr.org/en/professionalinterest/pages/cerd.aspx>, accessed 12 December 2019.

<sup>406</sup> Ibid.

<sup>407</sup> *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, opened for signature 28 January 2003 (entered into force 1 March 2006) ('Additional Protocol'). Online at <https://rm.coe.int/168008160f>, accessed 12 December 2019.

<sup>408</sup> Ibid, Article 3.

<sup>409</sup> Ibid, Article 4.

<sup>410</sup> *Congressional Primer on 8chan*, Committee on Homeland Security 8chan Inquiry, Submission to the Committee on Homeland Security, 4 September 2019, p. 2, at <https://www.benjaminbarr.com/news-updates> with the submission at [https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3\\_f869c81d6bcb495ebdd137776542fe11.pdf](https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3_f869c81d6bcb495ebdd137776542fe11.pdf), accessed 12 December 2019.

*in other countries. Those across the oceans may feel it necessary to stifle the voice of minority opinions. This is not what I intend to do.*

---

This immediately limits the cooperation with law enforcement as much of what is unlawful in other countries, in efforts to prevent the spread of hate and violence, will be actively permitted and protected on 8chan. The submission to congress makes this intention explicit saying “Beyond minute categories of unprotected speech remain all sorts of uneducated, ill-informed, and conspiratorial opinions. These remain protected under the First Amendment and protected by 8chan”.<sup>411</sup>

#### 5.6.4 Return as 8kun

Watkins announced the relaunch and rebranding of 8chan to 8kun with a video on October 7, 2019.<sup>412</sup> The video features the new logo appearing out of an explosion and then morphing into a logo of a black flag waving in a thunderstorm. The video has been viewed 445,600 times and retweeted 6,900 times.

From the start this was not the creation of a new board, but rather the same 8chan with content and accounts migrated to the new service (see Figure 49 and Figure 50). The rebranding and technical changes allowed 8chan to side step a range of efforts to control the flow of extremist materials, including a ban on 8chan which was imposed by Australia’s eSafety Commissioner.<sup>413</sup>



Figure 49 In a tweet 8chan board owners were invited to migrate to 8kun

---

<sup>411</sup> Congressional Primer on 8chan, Committee on Homeland Security 8chan Inquiry, Submission to the Committee on Homeland Security, 4 September 2019, p. 2. at <https://www.benjaminbarr.com/news-updates> with the submission at [https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3\\_f869c81d6bcb495ebdd137776542fe11.pdf](https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3_f869c81d6bcb495ebdd137776542fe11.pdf), accessed 12 December 2019.

<sup>412</sup> @Infinitechan, 2019. *Twitter* (6 October), at <https://twitter.com/infinitechan/status/1181054604097642496>, accessed 12 December 2019.

<sup>413</sup> Cameron Wilson, 2019. “Australia Won’t Censor 8chan Unless It Hosts The Christchurch Video, Says Internet Watchdog”, *BuzzFeed* (7 November), at <https://www.buzzfeed.com/cameronwilson/australias-internet-8chan-esafety-commissioner>, accessed 12 December 2019.



Figure 50 8kun started by migrating content and accounts from 8chan

**RECOMMENDATION 32:** Decisions by technology companies not to do business with a site should be such that a change to the ownership, brand, domain name or IP address will not circumvent the ban.

**RECOMMENDATION 33:** Decisions by governments to restrict access to a site should be robust enough that a change to the ownership, brand, domain name or IP address of the banned site will not circumvent the restriction. Government may need to monitor and update identification details to enforce such restrictions.

An ongoing battle has been wages between activists and 8chan in which companies providing the technology to keep 8chan online have been named and shamed in to dropping 8chan / 8kun, or failing that, have found their own service cut off from further upstream.<sup>414</sup> These are voluntary actions by technology companies rather than a result of legislation. This demonstrate that companies may no longer be immune from criticism and boycotts if they provide the infrastructure that enables others to keep hate online.

**RECOMMENDATION 34:** All companies providing Internet infrastructure should have clear terms of service which prohibit the use of their service for inciting hate or violence. They should also give notice that the service may be terminated without notice for serious breaches of this rule. Companies may further wish to require that any customer they provide a service to includes a similar statement in its terms of service.

## 6 Responding to the Online Sub-Culture of Hate and Violent Extremism

### 6.1 Hardening Targets to Reduce Antisemitic Attacks

The Jewish community has been subject to many terrorist attacks from a range of ideologies over the years, including at a Jewish centre in Mumbai (India) in 2008,<sup>415</sup> the United States Holocaust Memorial

<sup>414</sup> Matt Binder, 2019. "Inside the fight to keep 8chan offline", *Mashable* (6 August), at <https://mashable.com/article/8chan-down/>, accessed 12 December 2019.; Robert Evans & Frederick Brennan 2019, "The State of California Could Have Stopped 8Chan: It Didn't", *Bellingcat* (4 November), at <https://www.bellingcat.com/news/2019/11/04/the-state-of-california-could-have-stopped-8chan-it-didnt/>, accessed 12 December 2019.

<sup>415</sup> Associated Press in Mumbai, 2014. "Mumbai Jewish centre targeted in 2008 terrorist attacks reopens", *The Guardian* (26 August), at <https://www.theguardian.com/world/2014/aug/26/mumbai-jewish-centre-chabad-lubavitch-reopens>, accessed 12 December 2019.

Museum shooting in Washington DC in 2009,<sup>416</sup> a Jewish school in Toulouse (France) in 2012,<sup>417</sup> a kosher supermarket in Paris (France) in 2015,<sup>418</sup> the Great Synagogue in Copenhagen (Denmark) in 2015,<sup>419</sup> the Tree of Life synagogue in Pittsburgh (USA) in 2018,<sup>420</sup> and the Poway Synagogue near San Diego (USA) earlier in 2019.<sup>421</sup> As a result, Jewish communities around the world have developed security protocols, and hardened their physical infrastructure, protecting their institutions and spaces with both guards and secure doors and barriers.

This was effective in Halle as the reinforced door proved an effective barrier and stopped the gunman entering the Synagogue and causing the high level of casualties that were seen in the synagogue in Poway and the mosque in Christchurch. The heavy security dissuaded the attacker from engaging in additional reconnaissance and limited his ability to gain useful intelligence to better plan the attack. He was unable to get through the door despite anticipating that it would be secured and despite his attempts to shoot it open.

This is not the first time that casualties have been reduced due to security. In the 2015 attack on the Great Synagogue in Copenhagen a community volunteer on security duty, Dan Uzan, questioned the attacker when he approached the synagogue. This led to the attack being triggered outside the synagogue rather than inside. Dan tragically gave his life protecting his community, but he stopped what could have been a far more deadly attack on the community.

It is unfortunate that communities need to live within this sort of security, however, so long as these attacks and the incitement for such attacks remain regular occurrences, governments and other national bodies should provide or contribute to the costs of security. They should also provide additional support at times of increased risk, such as during Yom Kippur.

In Australia the Federal Government recently announced \$5.7 million to improve safety and security for Jewish schools and religious institutions in the state of NSW.<sup>422</sup> The funding comes from a multi-round Safer Communities Fund and is part of \$41.9 million released in the current round.<sup>423</sup> In the state of Victoria the government allocated \$3 million “towards making Jewish community centres safer and

---

<sup>416</sup> 2009. “Guard Killed In Holocaust Museum Shooting”, *CBS News* (10 June) at <https://www.cbsnews.com/news/guard-killed-in-holocaust-museum-shooting/>, accessed 12 December 2019.

<sup>417</sup> Tzvi Fleischer and Sharyn Mittelman, 2012. “Jihadism, Antisemitism and the truth about the Toulouse murders”, *ABC Religion and Ethics* (30 March), at <https://www.abc.net.au/religion/jihadism-antisemitism-and-the-truth-about-the-toulouse-murders/10100670>, accessed 12 December 2019.

<sup>418</sup> Andre Oboler, 2015. *Je Suis Humain: Responsible free speech in the shadow of the Charlie Hebdo murders*. Melbourne, Australia: Online Hate prevention Institute. Online at <http://ohpi.org.au/jesuishumain/>, accessed 12 December 2019.

<sup>419</sup> 2015. “Copenhagen shootings: Police kill ‘gunman’ after two attacks”, *BBC News* (15 February), at <https://www.bbc.com/news/world-europe-31475803>

<sup>420</sup> Chelsea Garbell, 2018. “After Tree of Life attack, don’t tell Jews all hate crimes & bigoted attacks are the same”, *USA Today* (8 November), at <https://www.usatoday.com/story/opinion/voices/2018/11/08/jews-anti-semitism-shooting-pittsburgh-europe-hate-crime-column/1890066002/>, accessed 12 December 2019.

<sup>421</sup> Andre Oboler, 2019. *San Diego Synagogue Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/san-diego-synagogue-attack/>, accessed 12 December 2019.

<sup>422</sup> 2019. “\$5.7 million federal security grants for Jewish schools and institutions within Wentworth”, *Jwire* (16 October), at <http://www.jwire.com.au/5-7-million-federal-security-grants-for-jewish-schools-and-institutions-within-wentworth/>, accessed 12 December 2019.

<sup>423</sup> Ibid.

more secure” with funding being applied to “organisations and sites with the greatest need” as identified through a collaborative approach with the peak community body the Jewish Community Council of Victoria and its subsidiary the Community Security Group.<sup>424</sup> This is an addition to a further million allocated to the security upgrades for a community centre which houses many of the Jewish communal organisations.<sup>425</sup> The Halle attack demonstrates that proper physical security can save lives and we commend both the Federal and Victorian Government for the steps they have taken.

**RECOMMENDATION 35:** Governments continue to contribute to the costs of security for Jewish communal institutions and provide additional support at times of increased risk such as during Yom Kippur.

## 6.2 Taking Down the Online Infrastructure of Extremism

The Internet is a network of networks. For content to appear on the Internet it needs to physically reside on a hard drive inside a server. Space on the server may be rented from a company (a hosting provider) that owns and manages the server, or a person may host material on a computer they own themselves. To connect the material on the server to others on the internet, the physical computer with the material needs to have a connection to the Internet. This means the hosting company (or individual who owns the computer) must be a customer of an Internet Service Provider (ISP). Even if the hosting company is itself an ISP, it must purchase bandwidth from a higher stream ISPs. Even in the case of large ISPs who run their own large networks using their own infrastructure such as cable and copper wires, at some point their network needs to connect to other networks, undersea cables or satellites. Beyond the hardware and wires, to exist on the surface web, a site also needs a domain name. These are purchased from domain name registrars who are licensed to sell domains under existing higher-level domains by the domain name owner. To sell a top-level domain (such as one ending in .com) a domain registrar must be accredited by the Internet Corporation for Assigned Names and Numbers (ICANN).

This infrastructure means a site can be taken off the internet if:

- The company that owns the servers hosting the content terminates the account
- The company that supplies the internet connectivity to the servers terminates their service
- The company that supplies the domain name terminates its use

In the last two cases if a company that is directly providing such a service fails to take action, it can itself become the subject of termination by its supplier. While small companies might be more willing to profit from the spread of hate and care little for their reputation, the larger companies that supply them with services may be susceptible to public pressure. This could take the form of adverse publicity or a direct consumer boycott. Even companies who do not deal directly with the public may be subjected to pressure when other businesses and government entities refuse to do business with them.

A problematic site, particularly a popular one, may also be protected through its use of a Content Delivery Network (CDN) service. A CDN service mirrors the content on a customer’s site allowing it to be delivered from a cached copy on the CDN’s servers rather than directly from the client’s servers. This can prevent DDOS (distributed denial of service) attacks and the CDN can replicate the content as

---

<sup>424</sup> 2018. “Security Upgrades For The Jewish Community”, *Premier of Victoria* (3 May), at <https://www.premier.vic.gov.au/security-upgrades-for-the-jewish-community/>, accessed 12 December 2019.

<sup>425</sup> Ibid.



needed to cope with an increased load, while also taking action against spurious traffic. One effect of a CDN is that as the content is accessed on the CDN's server rather than the clients, a trace to see who is providing the connectivity will stop at the CDN. While CDNs play a powerful role in protecting sites, they also carry a heavy burden in ensuring such protection is only provided when it is ethical to do so.

### 6.2.1 Lessons from Cloudflare's termination of 8chan

The first company to act against 8chan was Cloudflare, a Content Delivery Network, who on August 5<sup>th</sup> 2019 terminated their services to 8chan after the El Paso attack.<sup>426</sup> The announcement by Cloudflare's CEO Matthew Prince notes that:<sup>427</sup>

- "the suspected terrorist gunman appears to have been inspired by the forum website known as 8chan" and specifically by "largely unmoderated discussions on 8chan which glorified the previous massacre" in Christchurch
- the attacks in El Paso, Poway and Christchurch all involved posts to 8chan and that "8chan has repeatedly proven itself to be a cesspool of hate"
- "they have proven themselves to be lawless and that lawlessness has caused multiple tragic deaths. Even if 8chan may not have violated the letter of the law in refusing to moderate their hate-filled community, they have created an environment that revels in violating its spirit"

He goes to explain, "We reluctantly tolerate content that we find reprehensible, but we draw the line at platforms that have demonstrated they directly inspire tragic events and are lawless by design. 8chan has crossed that line. It will therefore no longer be allowed to use our services."<sup>428</sup>

The response from Matthew Prince continues noting that they only act very reluctantly and seldom in this manner. He explains this is not a First Amendment issue as Cloudflare is "a private company and not bound by the First Amendment". He explains "The only relevance of the First Amendment in this case and others is that it allows us to choose who we do and do not do business with; it does not obligate us to do business with everyone."<sup>429</sup> He commits to working not only with law enforcement, but also with governments and civil society. Highlighting the importance of the Rule of Law and the sovereign right of each country to determine what it permits and what it prohibits, Prince discusses the need for boundaries to be set on a country by country basis in a politically legitimate manner, rather than by companies:<sup>430</sup>

---

*Questions around content are real societal issues that need politically legitimate solutions. We will continue to engage with lawmakers around the world as they set the boundaries of what is acceptable in their countries through due process of law. And we will comply with those boundaries when and where they are set.*

---

<sup>426</sup> Matthew Prince, 2019. "Terminating Service for 8Chan", Cloudflare Blog (5 August), at <https://blog.cloudflare.com/terminating-service-for-8chan/>, accessed 12 December 2019.

<sup>427</sup> Ibid.

<sup>428</sup> Ibid.

<sup>429</sup> Ibid.

<sup>430</sup> Ibid.



He notes Europe's lead in responding to the problem of online hate and extremism and the distinction and resulting differing obligations that apply between companies that "organize and promote content — like Facebook and YouTube — rather than those that are mere conduits for that content".<sup>431</sup> This distinction has arisen as the idea that a platform like Facebook or YouTube should have no liability as it is not a publisher has fallen away in the face of significant evidence over the control they companies have over the visibility or lack of visibility of content, and the way they manage this as part of their business model.

**RECOMMENDATION 36:** Content services should create mechanisms that enable them to restrict access to specific content on their service for users from countries where that content is illegal. This will ensure content services have the technical capacity to respect national sovereignty and comply with national laws. There may be circumstances where a content service refuses to comply with national laws, for example, if the national laws conflict with customary international law, international treaties to protect human rights, or legal obligations in the content services own jurisdiction.

**RECOMMENDATION 37:** Hosting services that do not outright prohibit the use of their services to incite hate, should at a minimum ensure they don't serve content inciting hate to users in countries where such incitement is unlawful.

Prince notes that "the law may need additional remedies" when it comes to dealing with lawless platforms and suggests such law reform might "mean moving enforcement mechanisms further down the technical stack".<sup>432</sup> Such a move could mean creating legal liability for those who provide the infrastructure and connectivity to spread incitement to hate.

**RECOMMENDATION 38:** Governments should consider law reforms to create a system of sanctions that could be imposed on companies outside their jurisdiction who, after suitable notice, continue to provide unlawful content inciting hatred or violent extremism to users in that country in breach of the country's law. Such law reform could also create sanctions that impose penalties for any company within the country's jurisdiction who engaged in business with a company on the sanctions list.

### 6.2.2 The broader campaign to disconnect 8chan

The use of activism to name and shame companies whose provision of services supported the delivery of incitement to hate and extremism can be seen in the wider campaign to keep 8chan offline.<sup>433</sup>

Following its removal from Cloudflare, 8chan sought to move to a new Content Delivery Network called Bitmitigate, owned by domain registrar Epik.<sup>434</sup> In an initial statement the CEO of Epik, Rob Monster, said they did not solicit the business and would evaluate whether to provide the service, but stated that their "philosophy is, if the customer is not breaking the law, they are protected under our umbrella of services".<sup>435</sup> The statement also appeared to suggest it would be sufficient for a company to act on

---

<sup>431</sup> Ibid.

<sup>432</sup> Ibid.

<sup>433</sup> Matt Binder, 2019. "Inside the fight to keep 8chan offline", *Mashable* (6 August), at <https://mashable.com/article/8chan-down/>, accessed 12 December 2019.

<sup>434</sup> Ibid.

<sup>435</sup> Andrew Allemann, 2019. "Epik CEO Rob Monster statement on 8chan", *Domain Name Wire* (5 August), at <https://domainnamewire.com/2019/08/05/epik-ceo-rob-monster-statement-on-8chan/>, accessed 12 December 2019.

“content which is illegal in the United States”.<sup>436</sup> That would mean hate speech and incitement to hate would be permitted.

Epik rents some of its server space from a company called Voxility who soon found that their servers were now being used to host 8chan. Voxility’s business development VP Maria Sirbu explained what happened next: “As soon as we were notified of the content that Epik was hosting, we made the decision to totally ban them”.<sup>437</sup> She noted that, “This is the second situation we’ve had with the reseller and this is not tolerable” explaining that it was unlikely Voxility would resume services to Epik. The removal of service to Epik also took down the Daily Stormer which Epik was supporting.<sup>438</sup>

Soon after Epik reversed course.<sup>439</sup> In deciding not to provide services for 8chan, Epik said, “In cases whereby Epik identifies a particular publisher as being under-equipped to properly enforce its own Terms of Service, Epik reserves the right to deny service” and that in this case the decision was “largely due to the concern of inadequate enforcement and the elevated possibility of violent radicalization on the platform”.<sup>440</sup>

Evidence 8chan provided to Congress, documented earlier in this report, shows the moderation was in fact relatively fast on 8chan. The time from the post being made until it was removed was 2 hour and 49 minutes for the Christchurch attack, 12 minutes for Poway and 45 minutes for El Paso.<sup>441</sup> For comparison, Facebook first received a report of the Christchurch livestream video 29 minutes after the livestream started (and 12 minutes after it ended),<sup>442</sup> and at least one copy of the video remained on Facebook for at least 6 hours while a copy remained on YouTube for at least 3 hours.<sup>443</sup> The manifesto from Poway remained on Pastebin for 50 hours and on Mediafire for at least 20 hours.<sup>444</sup> The real issue

---

<sup>436</sup> Ibid.

<sup>437</sup> Adi Robertson, 2019. “8chan goes dark after hardware provider discontinues service” *The Verge* (5 August), at <https://www.theverge.com/2019/8/5/20754943/8chan-epik-offline-voxility-service-cutoff-hate-speech-ban>, accessed 12 December 2019.

<sup>438</sup> Paul Roberts, 2019. “‘A slippery slope’: Eastside web firm waffles on hosting online forum linked to El Paso shooter” *Seattle Times* (5 August), at <https://www.seattletimes.com/business/technology/a-slippery-slope-eastside-web-firm-waffles-on-hosting-online-forum-linked-to-el-paso-shooter/>, accessed 12 December 2019.

<sup>439</sup> Paul Roberts, 2019. “Seattle-area internet firm decides not to host extremist 8chan website linked to El Paso shootings”, *Seattle Times* (6 August), at <https://www.seattletimes.com/business/technology/seattle-area-internet-firm-decides-not-to-host-extremist-8chan-website-linked-to-el-paso-shootings/>, accessed 12 December 2019.

<sup>440</sup> Rob Monster, 2019. “Epik draws line on Acceptable Use”, *Epic Blog* (6 August), at <https://epik.com/blog/epik-draws-line-on-acceptable-use.html>, accessed 12 December 2019.

<sup>441</sup> *Congressional Supplemental Inquiries of 8chan, Submission to the Committee on Homeland Security*, 25 September 2019, p. 3, at [https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3\\_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true](https://d5e10168-1d62-4e43-8269-5d58035f234e.filesusr.com/ugd/62f5a3_72d0c2b98ca3433c82baec24e08625e9.pdf?index=true), accessed 12 December 2019.

<sup>442</sup> Alex Hern, 2019. “Facebook and YouTube defend response to Christchurch videos”, *The Guardian* (19 March), at <https://www.theguardian.com/world/2019/mar/19/facebook-and-youtube-defend-response-to-christchurch-videos>, accessed 12 December 2019.

<sup>443</sup> Alex Hern and Jim Waterson, 2019. “Social media firms fight to delete Christchurch shooting footage”, *The Guardian* (16 March), at <https://www.theguardian.com/world/2019/mar/15/video-of-christchurch-attack-runs-on-social-media-and-news-sites>, accessed 12 December 2019.

<sup>444</sup> Andre Oboler, 2019. *San Diego Synagogue Attack*. Melbourne, Australia: Online Hate Prevention Institute. Online at <https://ohpi.org.au/san-diego-synagogue-attack/>, accessed 12 December 2019.

then is that 8chan creates an “elevated possibility of violent radicalization on the platform”. This speaks to the culture of 8chan and 8chan’s /pol/ in particular.

The terminated service was not the hosting of the underlying 8chan site, just the Content Delivery Network service. Once it went down it was possible to find the address for the underlying 8chan server and the company providing them with that service. That turned out to be provided by a company called Centauri Communications.<sup>445</sup> A campaign was mounted against Centauri Communications who were supposed to be suspected by the Californian Secretary of State from doing business in that state.<sup>446</sup> While there was interest from a member of Congress in tackling this, there was also concern about potential reprisals and in particular the risk of swatting occurring.<sup>447</sup> The fear further highlights why /pol/ has the characteristics of terrorism. The servers were eventually moved interstate to a company called VanWaTech set up by the founder of BitMitigate Nick Lim.<sup>448</sup>

Another focus of the campaign is PayPal who are still providing financial services to collect donations for N.T. Technology, the company that ran 8chan and now 8kun (see Figure 51).<sup>449</sup> Given PayPal’s block on fundraising for Wikileaks,<sup>450</sup> it seems strange they continue to provide financial services to a platform that supports hosting incitement to hate and a culture which has led to multiple terrorist attacks.

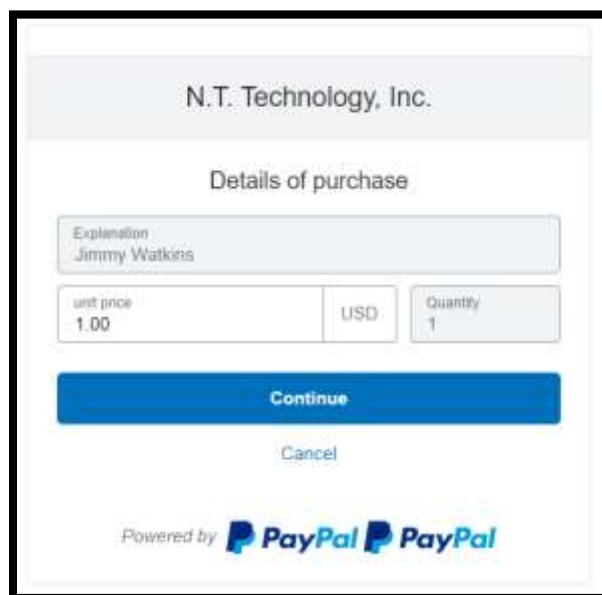


Figure 51 Paypal donations to N.T. Technology Inc

<sup>445</sup> Matt Binder, 2019. “Inside the fight to keep 8chan offline”, *Mashable* (6 August), at <https://mashable.com/article/8chan-down/>, accessed 12 December 2019.

<sup>446</sup> Robert Evans & Frederick Brennan 2019, “The State of California Could Have Stopped 8Chan: It Didn’t”, *Bellingcat* (4 November), at <https://www.bellingcat.com/news/2019/11/04/the-state-of-california-could-have-stopped-8chan-it-didnt/>, accessed 12 December 2019.

<sup>447</sup> Ibid

<sup>448</sup> Ibid.

<sup>449</sup> Ibid.

<sup>450</sup> Kevil Poulsen, 2010. “PayPal Freezes WikiLeaks Account”, *Wired* (4 December) at <https://www.wired.com/2010/12/paypal-wikileaks/>, accessed 12 December 2019.

The campaign to name and shame can produce results. It is in fact a form of counter speech with people and companies expressing their dislike by steering clear of companies that are facilitating the spread of hate. While helpful in the absence of legal remedies, as Associate Professor Chris Demaske from the University of Washington-Tacoma has noted, this is leaving the decision making to companies and “at the end of the day, their job is to make money” and “not to promote democracy” which means policy will be driven by commercial and not civil imperatives.<sup>451</sup>

### 6.3 Tackling the toxic culture

The toxic culture on /pol/ which has resulted in multiple terrorist attacks is due to a combination of anonymity, hate speech as a cultural norm, a shared political ideology (the red pill ideology) and a willingness to engage in and to support criminal and even violent action that promotes the cause.

Some in the /pol/ community are no doubt hardcore activists. Others are in it just for the thrill of being part of the unfolding train wreck; part of something that will make the news. Given their anonymity and the likely lack of any repercussions for them, they keep encouraging and egging on others to see what might happen. There is a game like culture with wins and high scores. The effort to spread fake news to get the attack pinned on Rainer Winkler (Drachenlord) in the hours immediately after the attack highlight not only a lack of empathy and basic human dignity, but an outright reveling in cruelty.

The idea of /pol/ as a “containment zone” for this poor behaviour doesn’t work. It allows the toxicity to concentrate. It establishes a new normal and, in the words of one poster, then allows that culture to “infected” other boards. Despite being anonymous, /pol/acks can move between /pol/ boards on different servers and reconnect with the community. The fact there are no lasting accounts and nothing to register or configure actually makes this easier and more resistance to the closure of a particular platform like 8chan.

It isn’t all bad as many on the various image boards are against the toxic culture. If there were a way to agree to community standards democratically, the result might strengthen community standards and force the hate to leave. This is a technical challenge in an anonymous forum. It is also a political challenge as the Image boards are not run as democracies. Some who are there to troll and participate in causing chaos in society will leave if the culture improves on one board and will seek to join or create another. If image boards that will stand against the toxic culture, as 4chan did in gamergate, can be separated from those that tolerate the toxic culture, the problem is already reduced. If image boards that tolerate a toxic culture can be regularly disrupted through the loss of their suppliers, block imposed by state authorities or blocks at the ISP level, it will create an incentive for their owners to stamp out the toxic culture on their board. For those that won’t work to stamp it out, the disrupt to community will cause a drop off in participation and send a signal that the culture is unacceptable. There will still be individual bad actors, but their ability to coordinate, feed off each other and increase the intensity will be reduced. This disruption can still be effective in limiting growth and reducing harm. Where a board or forum’s moderators are indifferent to illegal activity there should be legal penalties.

---

<sup>451</sup> Paul Roberts, 2019. “Seattle-area internet firm decides not to host extremist 8chan website linked to El Paso shootings”, *Seattle Times* (6 August), at <https://www.seattletimes.com/business/technology/seattle-area-internet-firm-decides-not-to-host-extremist-8chan-website-linked-to-el-paso-shootings/>, accessed 12 December 2019.

Professional disruption efforts aimed at undermining hateful narratives and changing board sentiment and content can be used, but there are significant challenges to this approach. The users on /pol/ assume this is already happening and often jump at shadows. They dismiss the views of anyone being even remotely moderate, usually by accusing them of being a Jew. The push back can still create resistance and derail a downwards spiral. It can, however, be halted by those with administrator rights who may act to preserve the culture.

Where there is support from board administrators, identifying users responsible for outsized influences of toxicity on /pol/ boards and selectively (and discretely) blocking them from the platform with IP based bans could be effective. At minimum it will disrupt them and increase their effort of participation, making it more likely they head to another platform.

While /pol/ increases the toxicity to dangerous levels, it reflects discontent in segments of society. As with other fascist movements, it is those disillusioned with society who are more likely to join. Blaming minorities is always presented as an easier solution than the work required to solve societal problems. A more proactive and informed political discussion, in /pol/ on the issues impacting people in the community could help to reduce hostilities.

In the end reducing the toxicity is something that needs to come from the image board community itself, but suitable pressure needs to be created on board owners who foster this toxicity. Suitable support needs to be provided to efforts within the image board community to speak out against increases in toxicity. There need to be consequences and those consequences need to be triggered much earlier in the process. Once someone is announcing an imminent attack, it is too late.

In the face of an attack, everyone needs to do their part and they should make it known they are doing this. Links sharing terrorist videos or manifestos should be report to authorities and where it is safe to do so, for example when posting anonymously, posts sharing this content should get a reply stating it has been reported. This will help establish a community standard against sharing such content as well as actively getting it removed.

**RECOMMENDATION 39:** The public are urged not to share content from terrorist attacks such as manifestos or videos. If seen, this content should be reported to the relevant authorities, in Australia this being the eSafety Commissioner.

## 6.4 Future Work

While the specific image board culture is the focus of this report, there is a wider online culture which can either permit and encourage or prohibit and discourage the spread of incitement to hate and violence.

The Online Hate Prevention Institute has developed tools for the public to report online antisemitism, categorised to reflect the IHRA Working Definition of Antisemitism, but which are able to be configured to cover other forms of hate as well. The latest version of the tool is able to be embedded in the website of other organisations and configured to meet their needs, both in terms of the types of hate that can be reported and the language of the user interface.

The next step is a range of projects in partnership with organisations around the world to enable others to empower their community to report online hate while also facilitating empirical reports on the problem. There is also a training program to teach grassroots communities to identify, report and more

generally respond to a range of different forms of hate speech. Subject to support from both donors and partner organisations we hope to roll this program out for both antisemitism and others types of hate through 2020. Our past Empirical report on Antisemitism<sup>452</sup> and Islamophobia<sup>453</sup> give an idea of what is possible.

We invite potential partners, sponsors and donors for this larger campaign to contact us through our website: <https://ohpi.org.au/contact-us/>

---

<sup>452</sup> Andre Oboler, 2016. *Measuring the Hate: The State of Antisemitism in Social Media*. Melbourne, Australia: Online Hate prevention Institute. Online at <https://ohpi.org.au/measuring-antisemitism/>, accessed 12 December 2019.

<sup>453</sup> Andre Oboler, 2015. *Spotlight on Anti-Muslim Internet Hate Report*. Melbourne, Australia: Online Hate prevention Institute. Online at <https://ohpi.org.au/anti-muslim-hate-interim-report/>, accessed 12 December 2019.

## INDEX

### /

/pol/, ii, 1, 2, 17, 24, 25, 35, 40, 42, 44, 51, 64, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 85, 86, 87, 88, 89, 90, 92, 93, 94, 96, 97, 98, 99, 100, 101, 111, 112, 113

### 2

2channel, 68, 69

### 4

4chan, 1, 15, 17, 22, 24, 25, 39, 40, 42, 43, 44, 64, 65, 67, 68, 69, 70, 71, 72, 73, 75, 78, 79, 84, 85, 86, 87, 91, 93, 99, 101, 112

### 8

8chan, 1, 2, 14, 15, 17, 19, 20, 22, 24, 25, 40, 42, 53, 64, 71, 83, 85, 86, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 108, 109, 110, 111, 112

### A

Abhorrent Violent Material, xiii, 51, 58, 59, 60, 62, 63  
*Additional Protocol*, 12, 13, 103  
Allington, v  
Alt-Right, iii, 39, 64, 72, 73, 74, 84, 86, 87, 93, 94, 95, 96  
Amazon, 17, 23, 29, 39, 48, 59  
anonfile.com, 23, 25, 26, 27  
antisemitic, v, xiii, 15, 16, 19, 21, 22, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 71, 73, 75, 76, 78, 79, 80, 88  
antisemitism, iv, v, 3, 25, 30, 31, 32, 33, 34, 35, 36, 37, 39, 40, 45, 72, 73, 75, 76, 77, 79, 80, 87, 106, 113, 114  
Antisemitism, iv, v, 30, 31, 32, 33, 35, 45, 71, 72, 75, 76, 77, 106, 114  
Anudda Shoa, 23, 38  
Anyzon, 17  
Ayashii World, 64, 65, 66, 67, 68

### B

Balliet, 17, 20, 21, 22, 42, 44  
Ben Garrison, 71, 73, 74, 75, 76  
Billen, 9  
*Broadcasting Services Act 1992* (Cth, 51, 59, 60, 62

### C

California, ii, 20, 31, 36, 98, 105, 111  
**Christchurch**, ii, xiii, 1, 2, 14, 16, 46, 51, 53, 54, 56, 59, 60, 61, 62, 63, 86, 97, 98, 99, 106, 108, 110  
Christian, 2, 17, 23, 31  
Christian Identity movement, 17  
Christianity, 17, 35  
Christians, 1, 3, 16, 17, 36, 40, 96  
CIA, 19  
CIP, 53, 54  
Clough, 10, 11  
CODOH, 37  
Committee for the Open Debate on the Holocaust, 37  
Communists, 1, 3, 16  
Content Incident Protocol, 53  
cyberbullying, 1

### D

Dark Net, 16  
Dark Web, 2, 16, 23, 27, 28  
DoKumentation, 16, 20, 52

### E

**El Paso**, ii, xiii, 1, 2, 16, 62, 63, 86, 101, 108, 110, 112  
eSafety Commissioner, xiii, xiv, 51, 58, 59, 60, 62, 63, 104, 113  
extremism, ii, iv, xi, xii, 1, 2, 3, 17, 25, 30, 33, 42, 46, 47, 56, 64, 70, 80, 85, 101, 109

### F

Facebook, iii, 7, 8, 9, 45, 46, 53, 54, 57, 59, 61, 96, 97, 98, 109, 110  
Frederick Brennan, 20, 105, 111

### G

GIFCT, xiii, 48, 51, 53, 54, 55, 59  
Global Internet Forum to Counter Terrorism, xiii, 53, 55  
Goldsmith, 5, 6, 7, 10  
Google, xiii, 51, 52, 53, 59, 62, 63, 66, 67



## H

**Halle**, ii, xiii, 1, 2, 3, 14, 20, 24, 30, 31, 33, 36, 38, 39, 40, 42, 46, 56, 57, 58, 59, 60, 62, 63, 96, 99, 106, 107  
 harassment, 1, 29, 70, 83, 84, 93  
 Hipster Hitler, 18, 19, 35  
 Hitler, 18, 22, 37, 71, 73  
 Holocaust denial, v, 25, 36, 37, 38, 39, 45, 57, 72, 79

## I

IHR, 37  
 IHRA, xiii, 31, 32, 33, 34, 36, 113  
 Institute for Historical Review, 37  
 International Holocaust Remembrance Alliance, iv, xiii, 31, 32, 33  
 Israel, iv, 31, 32, 33, 36, 38

## J

Jews, 3, 14, 15, 18, 22, 23, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 72, 73, 74, 75, 78, 94, 99, 106  
 Jim Watkins, 20, 85  
 Judaism, 34, 36, 40  
 Juice, 18  
 Justin.tv, 29

## K

Katherina Von Schnurbein, i  
 Kike, 34, 35  
 KKK, 17  
 Kohlchan, 44, 45, 55  
 Ku Klux Klan, 17

## L

Lee, 9  
 livestream, ii, xi, 2, 18, 22, 29, 47, 48, 53, 59, 70, 98, 110

## M

Manifesto, 16, 24, 40  
 Mark Mann, 19, 20  
 Marr, 30, 31  
 Meguca, 2, 24, 25, 55  
 meguca.org, 15, 23, 24, 39, 45  
 Meguca.org, 2, 24, 55  
 meme, 2, 18, 24, 38, 64, 70, 71, 75, 76, 77, 88, 92, 93, 99  
 Milo Yiannopoulos, 73, 93  
 Muslim, 17, 22, 23, 61

Muslims, 1, 3, 16, 19, 40

## N

natsoc, 24  
 Neko, 17  
 Nekomimi, 17  
 neo-Nazi, 25, 75, 77, 78, 82, 87, 94, 95  
 Neo-Nazi, 15, 95  
 neo-Nazism, 25, 71, 77, 93, 94  
 New Zealand, ii, 1, 2, 16, 60, 97

## O

**Oboler**, iv, 1, 2, 7, 10, 11, 38, 45, 57, 71, 73, 75, 76, 88, 97, 98, 100, 106, 110, 114  
 online extremism, ii

## P

Pepe, 87, 88, 89, 90, 91, 92, 93  
**Poway**, ii, xiii, 1, 2, 3, 16, 62, 63, 86, 98, 99, 100, 106, 108, 110  
 Prince, 53, 101, 108, 109  
*principle of appropriate adaptation*, 11  
*principle of generality*, 10  
*principle of inclusion*, 11  
*principle of necessary criminalisation*, 11  
 PunkSPIDER, 28

## R

Rainer Winkler, 42, 112  
 redemptive antisemitism, 39  
 red-pill, 72

## S

Scolyer-Gray, v, 85, 91  
 serious hate speech, 12  
 spilljuice", 18, 29, 34, 35  
 Stephan Balliet, 15  
 stormfront, 77, 78

## T

Tech Against Terrorism, 55  
 Telegram, 49, 50, 55  
 terrorism, ii, iii, x, xi, xiii, 3, 26, 46, 50, 51, 52, 53, 55, 56, 60, 61, 63, 69, 86, 97, 101, 111  
 terrorist attacks, ii, xiii, xiv, 63, 96, 105, 111, 112, 113

*Terrorist Content Analytics Platform*, xiii, xiv, 56

Texas, ii, 1, 101

The Onion Router, 28

Tor, 28

Trump, 87, 89, 90, 91, 92, 93, 94

Twitch, 29, 30, 46, 47, 48, 54, 55

twitch.tv, 16, 23, 29

Twitter, 43, 53, 55, 57, 59, 70, 71, 76, 84, 87, 88

*Tzedakah*, 36

## U

USA, ii, 16, 70, 96, 106

## V

Valhalla, 17, 21

## W

Waifus, 17, 21

White nationalism, 17

Winkler, 43, 44

*Working Definition of Antisemitism*, xiii, 31, 32, 33, 113

Wu, 5, 6, 10

## Y

Yukino Yukinoshita, 17

## Z

Zionist Occupied Government, 22, 38, 40

## マ

マニフェスト, 16







# Online Hate Prevention Institute

ABN 65 155 287 657

[ohpi.org.au](http://ohpi.org.au)  
[info@ohpi.org.au](mailto:info@ohpi.org.au)  
[facebook.com/onlinehate](https://facebook.com/onlinehate)  
[twitter.com/OnlineHate](https://twitter.com/OnlineHate)  
[youtube.com/user/OnlineHate](https://youtube.com/user/OnlineHate)