

TASM Conference 2026
16-18 June
Great Hall, Swansea University Bay Campus

Schedule	4
Keynotes.....	6
Breakout session 1	7
Panel 1A: Beyond the Edgesphere: A Comparative Global Study of Violent and Coercive Online Networks Targeting Youth	7
Panel 1B: Far-right narratives	7
Panel 1C: Global misogyny	9
Panel 1D: Researching on TikTok	11
Panel 1E: Jihadism	11
Breakout Session 2	13
Panel 2A: The VOX-Pol Network: Benefits, Opportunities, Expectations	13
Panel 2B: New trends in far-right extremism	13
Panel 2C: Nihilistic violent extremism	15
Panel 2D: Anonymity, security and resilience: The creative tension between regulatory policy and terrorist exploitation of the internet.....	17
Panel 2E: Open-source intelligence and security	18
Breakout Session 3	21
Panel 3A: Narratives and identity	21
Panel 3B: “The Digital Bazaar”: Understanding how extremist organisations are exploiting TikTok to share propaganda and radicalise young individuals	23
Panel 3C: Theories of misogyny	23
Panel 3D: NVE, Mixed, Salad Bar? Towards a definitional framework for modern attackers	25
Panel 3E: The current violent extremist threat landscape: networks, platforms, and technologies.....	26
Breakout Session 4	27
Panel 4A: Anti-gender ideology and the social media landscape in and beyond Canada	27
Panel 4B: Radicalisation pathways	27
Panel 4C: Far-right conspiracies	29
Panel 4D: Content moderation	31
Panel 4E: The pathway to harm: spotting missed opportunities for intervention in violent and dangerous online communities	33
Breakout Session 5	35
Panel 5A: Research practice	35
Panel 5B: Countering violent extremism.....	37
Panel 5C: Mobilisation pathways	39

Panel 5D: Misogynistic narratives	41
Panel 5E: Distinct remits, but shared mission: How regulation can protect users from terrorism content online	43
Breakout Session 6	44
Panel 6A: Crisis, connectivity, and meaning: Exploring youth extremism in the digital age	44
Panel 6B: Exit strategies for violence fascination.....	45
Panel 6C: Risk tracking	45
Panel 6D: Understanding and responding to misogyny	47
Panel 6E: Design, detect, decide: A hands-on lab for terrorism safety in AI.....	49
Breakout Session 7	50
Panel 7A: The only way is ethics: An open conversation on safety, standards, and solutions in extremism research.....	50
Panel 7B: Online safety regulation in action: Balancing rights and risk	51
Panel 7C: Designing responses	51
Panel 7D: Project Catalyst: Comparative interventions tackling violent extremism and misogyny in gaming communities and platforms	53
Panel 7E: Discord and deception: Radicalisation through the lens of Danny’s story .	54
Breakout Session 8	55
Panel 8A: Researcher safety by design: Modelling practical OPSEC for studying digital extremism	55
Panel 8B: Harnessing multistakeholder power: Driving collective action for global challenges.....	56
Panel 8C: Imagined identities	56
Panel 8D: Youth radicalisation in gaming spheres: Evolving threats, P/CVE engagement and policy responses	58
Panel 8E: Interacting networks: Collaborative clusters to counter online terror threats	59
Panel 8F: Aesthetics, identity, ideology and euphoria: perspectives from South Asia, Southeast Asia and Oceania	59
Day Three: Morning Workshops	62
Workshop A: AI for Counter-Extremism	62
Workshop B: Tackling Terrorism and Online Threats – Achievements in Law Enforcement Agency and Innovator Cooperation	62
Day Three: Afternoon Workshops	63
Workshop C: Elevating AI Safety: From Content Moderation to Benchmark Development.....	63
Workshop D: Make the Call Now: Decisions and Consequences in a Live Terrorism Crisis	63

Schedule

Day one: 16th June

- 7:50: Coach departs the Swansea Marriott/Delta hotel
- 8:10: Coach departs The Village hotel
- 8:15 – 8:50: Registration and refreshments
- 8:50 – 9:00: Welcome: Prof Alison Perry (Head, School of Law, Swansea University)
- 9:00 – 10:00: Plenary 1, Prof Paul Gill (UCL): “Terrorist Use of Online Platforms: First-Hand Accounts”
- 10:00 – 10:10: Room change
- 10:10 – 11:25: Breakout session 1
- 11:25 – 11:50: Refreshments
- 11:50 – 13:05: Breakout session 2
- 13:05 – 14:30: Lunch (includes a VOX-Pol and VOX-Pol Next Gen networking session)
- 14:30 – 15:45: Breakout session 3
- 15:45 – 16:15: Refreshments
- 16:15 – 17:30: Breakout session 4
- 17:45: Coaches depart
- 20:00: Drinks reception at [Morgan’s hotel](#)

Day two: 17th June

- 7:50: Coach departs the Swansea Marriott/Delta hotel
- 8:10: Coach departs The Village hotel
- 8:15 – 8:45: Refreshments
- 8:45 – 10:00: Breakout session 5
- 10:00 – 10:10: Room change
- 10:10 – 11:25: Breakout session 6
- 11:25 – 11:50: Refreshments
- 11:50 – 13:05: Breakout session 7
- 13:05 – 14:30: Lunch (includes a VOX-Pol Next Gen lunch ‘n’ learn session on searching for academic jobs post-graduation from 13:30 – 14:15)
- 14:30 – 15:45: Breakout session 8
- 15:45 – 16:15: Refreshments
- 16:15 – 17:15: Plenary 2, Vidhya Ramalingam (Moonshot): “Measuring What Matters: A Decade of Online Violence Prevention”
- 17:15 – 17:30: Closing comments: Prof Paul Boyle (Vice Chancellor, Swansea University)
- 17:45: Coaches depart

Day three: 18th June

9:05: Coach departs the Swansea Marriott/Delta hotel

9:20: Coach departs The Village hotel

9:30 – 10:00: Refreshments

10:00 – 12:30: Sandpit and workshops get underway

12:30 – 13:45: Lunch

13:45 – 16:15: Sandpit and workshops

16:30: Coaches depart

16:30 – 18:00: VOX-Pol Next Gen workshop on the basics of applying for research grants

Keynotes



Paul Gill is a Professor of Security and Crime Science at University College London. His work focuses on the behavioural underpinnings of radicalisation and terrorism. His current work involves developing the evidence base for risk and protective factors for violent extremist outcomes, the development of measurements of violent extremism, the evaluation of risk assessment and management processes and countering insider threats. In the recent past, he has managed projects from a range of funders including the European Research Council, NCITE, the Home Office, and CREST. Past projects focused upon various aspects of terrorist behaviour including IED development, terrorist network structures, lone-actor terrorism, insider threat, domestic abuse, and school shootings. His doctoral research focused on the underlying individual and organizational motivations behind suicide bombing. This piece of research won the Jean Blondel Prize for the best Ph.D. thesis in Political Science in Europe for 2010. He has published in leading psychology, criminology and political science journals and his latest co-edited book on violent extremism risk assessment and management is published with University College London Press. In the past couple of years, Gill has provided briefings at the White House, Quantico, Public Safety Canada, the Home Office, Norwegian Extremism Commission, Association of European Threat Assessment Professionals, Europol, and the Swedish Police amongst others. He won the 2024 Distinguished Achievement Award from the Association of Threat Assessment Professionals.



Vidhya Ramalingam is Founder and CEO of Moonshot, an organization working to end online harms, applying evidence, ethics and human rights. Under her leadership, Moonshot has pioneered the development of new technology to rapidly assess threats of violence online, and operates a proven model to prevent targeted violence and terrorism online on behalf of the Governments of Canada, New Zealand, the United Kingdom, and the United States. Moonshot has twice been named to Fast Company's World's Most Innovative Companies list, including as the 9th most innovative security company in the world. Vidhya is also recognized internationally for her role leading intergovernmental policy responses to terrorism. Following the 2011 terrorist attacks in Norway, she led the European Union's first intergovernmental initiative on racially motivated terrorism. She has been recognized by Fortune's Most Powerful Women, served as a Commissioning Panelist for the UK security and intelligence agencies, and regularly testifies before the U.S. Congress, House of Commons of Canada, and UK Parliament on threats to national security.

Breakout session 1

Panel 1A: Beyond the Edgesphere: A Comparative Global Study of Violent and Coercive Online Networks Targeting Youth

Arthur Bradley (VOX-Pol Institute): [LinkedIn](#)

Dr Suraj Lakhani (VOX-Pol Institute): [LinkedIn](#)

Ottavia Galuzzi (UNICRI): [LinkedIn](#)

This panel is the launch of a joint VOX-Pol Institute (VPI) and United Nations Interregional Crime and Justice Research Institute (UNICRI) report which examines the global manifestations of violent and coercive online networks, considered to be part of the ‘edgesphere’, with a particular focus on ‘Com’ and the True Crime Community.

Drawing on OSINT data from numerous platforms and qualitative interviews with intelligence officials, counter-terrorism units, national/local police forces, and key researchers globally, the presentation maps the tactics these networks use to recruit and radicalise minors across platforms, exploring how harmful online communities form, evolve, and spread across jurisdictional and linguistic boundaries. A central analytical thread distinguishes between direct network linkage, ideological inspiration, and independent development — a distinction with significant implications for how investigators and practitioners understand and respond to the threat. The paper will discuss four specific case studies: Brazil, Iraq, Indonesia, and Romania (though data was collected from other countries too). These cases illuminate how similar behavioural patterns and operational dynamics manifest in markedly different cultural contexts. The presentation will also critically examine whether traditional siloed approaches to prevention, enforcement, and safeguarding remain adequate in addressing a threat that is simultaneously transnational and deeply locally contextualised. Finally, the paper will reflect on several important recommendations for law enforcement and policymakers.

Panel 1B: Far-right narratives

Chair: Prof Stephane Baele (UC Louvain)

Platforms of Ideology and Action: Comparing posting behaviour, affect, and content on Stormfront and Leak Society

Mackenzie B Hart (Simon Fraser University): [LinkedIn](#)

Although research on extremism now routinely analyses data drawn from both fringe and mainstream social media platforms, much of this research is quite rudimentary, in terms of theoretical development, and narrow, insofar as it tends to focus one ideology at a time. Similarly, extant research overwhelmingly focuses on the cumulative number of user posts, without analyzing individual users’ posting behaviour over time. At the same time, there is very little comparative research or theorizing done across platforms and extremist ideologies. This study addresses these limitations by comparing Leak Society, a nihilistic violent extremist Telegram channel, with Stormfront, a right-wing extremist forum, on the following dimensions: a) posting behaviour, b) sentiment, and c) content.

We employ group-based trajectory analysis to assess users' posting behaviour over eight quarters, using Linguistic Inquiry and Word Count (LIWC-22) to highlight how the emotions evoked in posts are related to this behaviour. Finally, qualitative content analysis is used to improve our understanding of topics discussion both within and across platforms.

Decoding Radicalization: A Sociolinguistic Analysis of White Supremacist Propaganda
Jeremiah Perez-Torres (Marist University): [LinkedIn](#); [BlueSky](#)

This research employs a sociolinguistic framework to dissect the rhetorical strategies and discursive patterns used within propaganda to engender violence and radicalize consumers in digital environments. Specifically, I analyze the propaganda of three white supremacist accelerationist groups: Atomwaffen Division (AWD), the Order of Nine Angles (ONA), and The Black Order of Pan Europa (BOPE).

Analyzing a corpus spanning 8,536 pages of extremist digital content (e.g., manifestos, newsletters, and memes), this study identifies three foundational discursive patterns prevalent across all three groups: the emphasis on i) history and belief systems, ii) in-group identity and existential threat, and iii) the aggressive framing of out-groups.

The analysis further delineates how these three patterns are conveyed via sub-patterns, including, but not limited to, sophisticated narratives of perceived victimization, articulated political ideology, and urgent calls for racial preservation. This paper details the structural and linguistic mechanisms through which these discourses function. Critically, it translates these sociolinguistic findings into practical recommendations to advance the development and precision of Large Language Models (LLMs) specifically trained to detect and mitigate nuanced extremist communication across digital platforms.

Manifestos and Far-Right Narratives: Grievances, Utopian Futures and the Construction of the "Enemy Other"

Stephen Bryant (University of Cincinnati): [LinkedIn](#)

Serene Tarabishi (University of Cincinnati)

Charlotte Naser (University of Cincinnati)

[Co-author: Dr Michael Loadenthal (University of Cincinnati)]

This study examines the narratives and ideological constructions within far-right manifestos produced by groups, movements, and individual actors across the United States and Europe between 2014–2024, and distributed online. These texts, often circulated through social media ecosystems that amplify and normalize extremist discourse, serve as vehicles for articulating grievances, constructing an “enemy other,” and justifying political violence. Preliminary analysis drew from 48 documents in the Repository of Extremist Aligned Documents (READ), a database maintained by the International Centre for the Study of Radicalism. After applying linguistic, accessibility, and length-based inclusion criteria, ten manifestos (five by lone actors and five by far-right movements) were selected for narrative analysis. Researchers coded each text and iteratively refined guiding questions to identify dominant narratives, fact-claims,

audience construction, and advocacy of tactics and strategies. Using these dimensions, manifestos were plotted on a grid modeled after the Two-Dimensional Political Model, often known as a ‘political compass,’ positioning each actor according to its strategic and tactical orientation. Findings reveal both shared and divergent visions of a far-right “New World Order,” with narratives functioning as expressions of white patriarchal reactionism and circulating through online networks that bridge extremist subcultures and mainstream political discourse.

A Homological Critique of Three Right Wing Manifestos

Dr Michael Waltman (University of North Carolina at Chapel Hill)

This research will consist of a homological critique of three very different right-wing manifestos: (a) The manifesto left behind by the Buffalo shooter, (b) The Project 2025 manifesto, and (c) The manifesto of Eliot Rodger, a misogynist and involuntarily celibate man. A linguistic homology, “. . . is a formal parallel that cuts across seemingly dissimilar discourses.” Argument from homology involves examining resemblances among different discourses or texts to render judgments about the features texts may share even though they address different content, contexts, and audiences. The logic of a homological critique is that individuals are influenced by the form of the text and not simply the specific content of the text. The results of this critique may speak to forms of influence that may appeal to some U.S. politicians, violent right-wing extremists, and misogynists. Ultimately, this homological critique may illustrate where these very different groups find common ground sufficient for the formation of allyships.

Panel 1C: Global misogyny

Chair: Dr Yasmin Chilmeran (Christchurch Call Foundation)

From Terrorist Content to TFGBV: Operationalising the DSA and European Regulation

Anne Craanen (Institute for Strategic Dialogue): [LinkedIn](#)

Jakob Guhl (Institute for Strategic Dialogue): [LinkedIn](#)

This presentation looks at how ISD uses the EU Digital Services Act (DSA) in practice to assess the legality of online content and clarify platform responsibilities across different harm types. Drawing on our work advising on the Terrorist Content Online Regulation (TCO) and the Directive on Combating Violence Against Women and Girls (VAWG Directive), we show how the DSA functions as a practical framework for navigating overlapping legal regimes.

We will outline the current threat landscape across mainstream platforms and explain how ISD applies existing legislation to determine when content meets the legal thresholds for terrorist content or technology-facilitated gender-based violence (TFGBV). The presentation will highlight how lessons from the more established TCO regime can inform stronger, DSA-aligned responses to TFGBV—particularly around risk assessment, transparency, and mitigation—helping platforms move from ambiguity to clearer, enforceable action.

The Tiger and the Lamb: How Are Christian Fundamentalist Sexual Narratives Co-Opted by the Manosphere?

This paper investigates how Christian fundamentalist narratives around sex and gender are co-opted within the Manosphere to construct and legitimise extreme misogyny. It argues that actors within the Manosphere mirror three central tenets typical of Christian fundamentalist sexual discourse: enforced binary gender roles; female sexual purity; and male sexual appetite. By engaging both with scripture directly, and with familiar fundamentalist lines of reasoning, the Manosphere legitimises misogyny under the guise of embodying ‘true Christianity’. This poses significant risk on a political level because it disguises extreme misogyny as traditional Christianity in cultural contexts which value Christian ethical frameworks, such as the USA. Furthermore, invoking Christianity to legitimise misogyny poses risks on an interpersonal level, as individuals are less empowered to object to misogyny which is presented under the guise of divine expectation.

The Jordanian and Arabic-language Manosphere

Guy Fiennes (Institute for Strategic Dialogue): [LinkedIn](#)

This paper is part of the ongoing project Catalyst, exploring the Jordanian and Arabic-language manosphere. In this initial report, ISD first scoped several platforms to study the Jordanian and broader Arabic-language manosphere, ultimately focussing on TikTok content. Analysts identified different types of manosphere accounts on TikTok, categorising them into distinct ideological groups, and evidencing key themes and tactics. These included Red Pill ideology, the exploitation of Islam and Stoicism (‘Broicism’) to cloak Red Pill ideology, male-guru looksmaxxing and more extreme, racialised looksmaxxing. We also sought to identify overlaps between online misogynistic communities and violent extremism, with a view to providing a framework for interventions against online misogyny-induced harms.

‘Are There Men Among You?’: The Irish Far-Right, militarised masculinity, and the making of a homegrown ideology

Joshua Farrell-Molloy (Malmö University): [LinkedIn](#); [BlueSky](#)

This article examines how Irish far-right groups mobilise history and masculinity to construct ideological identity and meaning. Drawing on gender and radicalisation studies research, it analyses the digital practices of four far-right groups that act as cultural entrepreneurs at the helm of constructing and sustaining an ideological core within the broader movement. Through netnography and visual analysis of their Telegram channels, the study finds that these groups leverage masculinity to fuse Irish republican and nationalist traditions from Ireland’s struggle for independence and beyond to contemporary activism against mass migration as proof of manhood and national authenticity. Through the appropriation of rebel heroes, military aesthetics, and physical culture, they perform a disciplined, militant masculinity that legitimises their authority as heirs to Ireland’s “unbroken” tradition of resistance. This process has implications for the ideological development of the Irish far right, signalling the emergence of a

homegrown variant rooted as much in gendered performances of militancy as in political doctrine.

Panel 1D: Researching on TikTok

Members of the TikTok team will provide an overview of the platform's Research Tools, with a focus on case studies showcasing relevant methods for researchers at TASM. This session is primarily designed for academic researchers and will allow time for Q&A and discussion.

Panel 1E: Jihadism

Chair: Dr Kamil Yilmaz (Swansea University)

AI Caliphate

Meili Criezis (American University): [LinkedIn](#); [BlueSky](#)

Islamic State supporters are continuing to produce visual propaganda and, with the rising popularity of AI, they have incorporated it into their content. The decentralised nature of pro-IS online communities encourages independent creativity and IS supporters are able to try new methods to reproduce their narratives with the assistance of generative AI. This study examines a dataset of 286 AI-generated images (although the database is continuing to grow) created by pro-IS supporters which have been disseminated on numerous platforms including Instagram, Facebook, Pinterest, and Pixiv. It discusses the narratives conveyed through these images and explores the various visual aesthetics present in the content. More specifically, five overarching codes emerged from the data including distinct aesthetic styles, the presence of people and geographically specific places, objects (such as Islamic State flags and weapons), social bonding, and violence (including warfare).

Between games and propaganda: the role of gaming as a factor in jihadist radicalisation

Paula M. Núñez-Guerra (Complutense University of Madrid): [LinkedIn](#)

With the increasingly emerging link between gaming spaces and the vulnerability of minors, this paper aims to systematically analyse the different typologies that link the two. Through direct observation in the framework of a research stay at CITCO, the competent authority in Spain for the removal of illegal content, and under the premise that there are two main typologies – game modifications and game recordings – the aim is to offer a critical approach to understand how such content is constructed, disseminated and re-signified. The research will answer the following questions: What are the most used platforms for the distribution of this material, what are their characteristics and what messages do they convey? Preliminary results show that edited recordings function as vehicles of symbolic legitimisation and community reinforcement, while game modifications operate as tools for the normalisation and dissemination of extremist narratives in digital environments frequented by minors.

Gen-AI and Tehrik i Taliban Pakistan (TTP): Propaganda Strategies and Platforms engagement patterns

Saif ur Rehman Tahir (Victoria University of Wellington): [LinkedIn](#)

Tehrik-i-Taliban Pakistan (TTP), based in South Asia, is one of the most active and violent terrorist groups in the world. It has claimed responsibility for over 1,300 attacks in the first half of 2025. Beyond violent actions, TTP has built a highly advanced online presence. It produces more than a dozen key propaganda products and sub products, including videos, digital magazines, podcasts, and nasheeds, running the largest and most adaptable jihadist propaganda campaign online. As per recent developments, there is an increasing use of Generative AI technologies to improve the scale, quality, and reach of its messaging. This research highlights the Gen-AI methods TTP has adopted to produce its propaganda and the approaches it can adopt in the future. Utilizing digital ethnography and open-source intelligence, this research identifies specific patterns and tactics in TTP's engagement across different platforms (Telegram, Twitter, WhatsApp and Signal), adjusting its messaging strategies against changes in content moderation policies and social media algorithms. By mapping evolving propaganda and engagement strategies, the findings provide an essential insight into how TTP maintains ideological outreach, recruitment, and psychological warfare in the digital age. It also raises critical questions about the ethical, technical, and policy challenges posed by Gen-AI-enabled extremism, emphasizing the need for platform accountability, interdisciplinary research, and regulations to address the next generation of terrorist propaganda.

Islamist narratives and Islamist use of current events on TikTok

Lea Brost (Royal Holloway University): [BlueSky](#)

There are numerous studies on extremists' use of the Internet and how they adapt their methods to the evolving landscape online. With TikTok having over 1 billion active users, it is not surprising that extremists also use it to influence people's opinions. However, since it is a newer platform, to date less research has been done on it than on other platforms. Thus, this presentation will examine how Islamists use TikTok to spread their propaganda by exploiting current events and framing them to fit their extremist narratives. Most Islamist TikTok accounts veil their calls for violence to circumvent content moderation. Instead, they create content on popular topics or address (perceived) grievances, and combine this with non-violent narratives to recruit new followers. The presentation will present a case study of a sample of videos by English-speaking and German-speaking Islamist accounts on TikTok to show how Islamists generate narratives by framing current events to mobilise youths. Additionally, it will highlight examples of methods to counter these narratives by utilising alternative narratives and redirection. By producing authentic content that emulates popular TikTok formats, and by taking a broad approach of also engaging non-violent Islamist ideology, these approaches are particularly effective in preventing radicalisation.

Breakout Session 2

Panel 2A: The VOX-Pol Network: Benefits, Opportunities, Expectations

Chair: Prof Stuart Macdonald (Swansea University; VOX-Pol Institute): [LinkedIn](#); [BlueSky](#)

Panellists:

Dr Sam Jackson (University at Albany): [BlueSky](#)

Dr Ashley A Mattheis (University of Manchester): [BlueSky](#)

Dr Katy Vaughan (Swansea University): [LinkedIn](#); [BlueSky](#)

Dr Jonathan Collins (Charles University)

Are you a new VOX-Pol Network member? A longer-term member who wants to get the most out of your membership? Or a researcher that is interested in joining?

VOX-Pol is a network of university-based researchers of online violent extremism, with over 100 members from countries around the world. As a community of researchers, we work together on a variety of initiatives. Our ethos is collaborative. We engage with stakeholders at all stages of the research process, from formulation of research questions through to development of implementable policy proposals.

This session is aimed primarily at those looking to learn about or become more involved in VOX-Pol. Join members of the leadership team to discuss all things VOX-Pol, including benefits, opportunities, and expectations for members. We will cover the main opportunities for involvement, including established opportunities like the VOX-Pol blog, lecture series, and commissioned reports, as well as new opportunities around executive education, knowledge exchange programme and the VOX-Pol Institute (our commercial wing). We would also love to hear your ideas for what else we should be doing.

Stakeholders are also warmly invited, to find out more about how to engage with VOX-Pol and offer your input.

Panel 2B: New trends in far-right extremism

Chair: Lisa McLnerney (VOX-Pol Institute; Extremisphere)

Transgender Scapegoating Narratives following School Shootings

Lily Harkes (University of Oxford)

Far-right actors in the United States have increasingly weaponized school shootings to scapegoat transgender individuals, regardless of the shooter's identity. There is ample evidence underscoring the prevalence of anti-trans narratives in the media and public discourse, yet no study has systematically tracked how these narratives emerge, spread, and persist in the immediate aftermath of shootings. This paper presents the first systematic cross-case analysis of trans scapegoating dynamics on 4chan /pol/ following six school shootings between 2021 and 2024: Nashville (2023), Uvalde (2022),

Apalachee (2024), Perry (2024), Oxford (2021), and Madison (2024). Drawing on a dataset of over 17,000 4chan /pol/ posts and comparative process tracing of information environments across cases, this study documents when and how trans scapegoating narratives activate, how intensely they peak, and whether identity confirmation or ambiguity shapes their persistence. Findings reveal that trans scapegoating was present in five of six cases regardless of whether the shooter was actually transgender, emerging within hours of each event and persisting despite active factual correction by police, mainstream media, and fact-checking organizations. The single exception, the Oxford case, is consistent with a combination of factors in the information environment: a lack of identity ambiguity in reporting, the absence of elite adoption, and the crowding out effect of an alternative dominant narrative. These findings demonstrate how trans scapegoating operates as a reflexive narrative template, being deployed rather than generated anew following violent shocks. Beyond the US context, these findings have policy implications for how governments, social media platforms, and civil society organizations anticipate and respond to identity-based scapegoating in the aftermath of a mass casualty event.

Parroting the Far-Right: Discourse and the Rapid Shift on Transgender Rights in New Labour

Robert Dickinson (University of Sussex)

[Co-authors: Quinnehtukqut McLamore (University of Missouri) & Hazal Dilay Süslü (University of Surrey)]

This study examines how far-right narratives around transgender rights have migrated into mainstream political discourse in the UK, focusing specifically on the Labour Party. Building on research into polluted information and malign influence, we track the diffusion of key phrases, framings, and argumentative strategies (e.g., taught intransigence) from online far-right sources and political elites into public Labour statements. Using mixed-methods discourse analysis, we identify patterns of uptake, adaptation, and amplification over time, highlighting the mechanisms by which extremist framings influence mainstream political rhetoric, even within the purported leftwing. Findings reveal how transphobic frames and far-right manipulative strategies, initially confined to extremist ecosystems, are repurposed and parroted in Labour discourse, illustrating a subtle form of discursive radicalisation that bypasses overt violence. This process has substantially shifted the Overton Window on trans rights, transforming Labour's positions into a reflection of far-right rhetoric. By systematically mapping these rhetorical flows, the study contributes to understanding the reach and impact of extremist ideas beyond their original contexts. The research has implications for scholars and policymakers concerned with polluted information, political influence, transgender rights, and the resilience of democratic debate.

Nihilist Violent Extremism (NVE): A new form of right-wing extremism?

Felix Neumann (Konrad-Adenauer-Stiftung e.V.): [LinkedIn](#)

Maniacs Murder Cult (MMC), 764, Order of Nine Angels (09A): Security authorities around the world are warning of a new form of violent extremist movement targeting minors online to join their cult-like communities. As their content is heavily based on child

sexual abuse material (CSAM) and depictions of murder, the limited available analyses often neglect their underlying political motivation. By analysing 23 archived online manifestos, this policy-oriented presentation argues to understand NVE as a new form of right-wing extremism. By specifically focussing on ideological cues and operational aspects of the current developments, I discuss differences and similarities to other forms of right-wing extremism. Results show that elements of right-wing extremism and militant accelerationism are a central component of groups in Maniacs Murder Cult (MMC) or 764. The works of Order of Nine Angles (ONA) have significantly influenced right-wing terrorist movements such as the Atomwaffen Division. The contribution concludes by offering results-driven recommendations to effectively counter this new threat.

De-platforming and re-platforming: the limited comeback of a neo-Nazi cartoon
Harrison Pates (King's College London): [LinkedIn](#)

In 2025, 10 years after Murdoch Murdoch's (MM) first episode and breaking a period of deplatforming, its creators briefly re-emerged into mainstream discussion on YouTube following the advent of far-right content celebrating the 'most BANNED cartoon on the internet [...] banned for telling the truth.' During its production, MM was a cartoonish web series which captured far-right extremists' 'ironic' humour, following Neo-Nazi and white nationalist protagonists engaged in conflict and defeating various imagined enemies. It praised mass shooters, espoused fascist ideology, and spread violent white supremacist propaganda until the post-deplatforming finale in 2021.

Through qualitative, cross-platform analysis of MM clips, this paper examines the extent to which neo-Nazi media has returned to mainstream spaces which simultaneously celebrate and satirically 'disavow' extreme-right terrorism. It seeks to address some of the challenges which come with addressing the 'ironic' promotion of extremism by evidencing both radical views and efforts taken to conceal them and avoid censorship, tracing the movement of the show as it briefly re-emerged before returning to alternative platforms. Citing from MM fan sites and reworked content, as well as a recent 'Ask Me Anything' video, the study views the resurgence of the series as a bellwether for the repackaging of extremist content.

Panel 2C: Nihilistic violent extremism

Chair: Dr Seán Looney (University of Plymouth)

'Jailbait and lolis': Understanding the prevalence of Child Sexual Abuse Material in incel discourse

Anna Meyniel (International Centre for Missing and Exploited Children): [LinkedIn](#)
Anda Solea (University of Portsmouth): [LinkedIn](#)

For researchers examining online hate and violence, misogynistic incels' worldview toward women is well established: women are regarded as lesser beings. Children, however, occupy a less visible yet significant position within these gendered hierarchies. While the sexualisation of minors has been noted on incel forums, no research has systematically examined the scope, nature, or prevalence of online child sexual

exploitation and abuse (OCSEA) within incel ideology. Key gaps therefore remain in understanding how OCSEA and Child Sexual Abuse Material (CSAM) feature within the broader blackpill discourse, and how such content contributes to radicalisation into extreme misogyny and the legitimisation of child sexual exploitation. This study addresses these gaps by analysing references to children on *Incels.Wiki*, focusing on the intersection between established child sexual abuse terminology (e.g., *jailbait*, *loli*) and traditional incel language. It investigates the prevalence of these terms, their links to potential exploitation communities, and their role in normalising sexual violence and reinforcing extremist gender beliefs. By mapping shared keywords between incel and CSAM discourses, the study identifies conceptual overlaps from the sexualisation of minors to the endorsement of illegal content. Contextualised within research on online misogyny and child sexual exploitation, this study highlights avenues for future inquiry and prevention strategies addressing the convergence of online extremism and OCSEA.

The ‘Blackpill’ as an Affective and Symbolic Node in Nihilistic and Apocalyptic Violent Extremism

Mark Peden (University of Sussex)

This paper advances the concept of nihilistic and apocalyptic violent extremism (N/AVE) by examining how the ‘blackpill’ operates as an affective and symbolic node within online threat landscapes often characterised by mixed, unclear, and unstable (MUU) ideological formations. Building on earlier work that traced N/AVE’s philosophical underpinnings, hyperreal dynamics, and convergence with mimetic and memetic violent aesthetics, the paper – drawing on empirical data collected from Reddit – explores processes of affective and narrative capture, where existential despair, foreclosed futurity, and terminal worldviews can harden into collapse-oriented meaning-worlds where violence can become narratively meaningful and emotionally compelling, even in the absence of coherent ideology.

Introducing the HARDGORE project: Charting the Gore Digital Ecosystem and its Role in “Mixed, Unclear and Unstable” Extremism.

Prof Stephane Baele (UC Louvain)

Dr Lewys Brace (University of Exeter)

Over the past few years, cases of lethal violence with unclear motives and goals have multiplied, puzzling law-enforcement and scholars alike. The attack in Southport (UK), which seems to exemplify this type of shocking criminality, propelled it onto the policy debate and put new urgency onto law-enforcement to tackle the phenomenon. Yet the nature of this phenomenon – if there is one – is still poorly understood, and many scholars and professionals express their dissatisfaction with the dominant extremism/terrorism framing and response. Offenders’ digital footprints typically display “mixed, unclear, and unstable” ideological engagement and usually include many non-ideological types of online interactions and explorations. Among these, one stands out as particularly ubiquitous: access to “gore” websites and digital spaces curating videos and images of extreme and frequently lethal violence. This contribution aims to present the main findings of the HARDGORE project, a systematic, data-driven analysis of the structure of the “gore” ecosystem, harnessing computational techniques to extract and

study several types of (meta-)data pertaining to many such sites (forums, video-sharing platforms, Web3 platforms, and social media channels), in an effort to gain a multi-dimensional characterization and mapping of the structure of this ecosystem. Such an effort is a necessary step in reaching a sophisticated and accurate understanding of new forms of extremism and violence, and in designing sound policies tackling this threat.

Nihilist Violent Extremism & Self-Harm as Terror Tactic: Reviewing Compensation Schemes for Victims of Terrorism

Isabella Pirlogea (Leiden University): [LinkedIn](#)

Sean McCafferty (Metropolitan University Prague): [LinkedIn](#)

European victim-compensation schemes for terrorism, designed around outward-directed violence, struggle to address harms produced by post-ideological, misanthropic online networks. These communities normalise hostility, target minors, and instrumentalise self-harm through coercion, blackmail and directed “tasks” for control, recruitment and propaganda. We argue that individuals who self-harm under such terrorist influence (coercion, blackmail, recruitment or comparable “influence crime”) should be recognised and compensated as victims of terrorism, not offenders. Using comparative doctrinal analysis of Spain, France and Germany, situated within relevant EU directives on terrorism and victims’ rights, we develop a three-part eligibility test: (1) organised actor nexus, (2) coercive mechanism, and (3) causation with serious injury. We find recognition is available in principle (psychological injury, indirect victims, coercion) but often fails in application to inward-directed, digitally mediated harm. This analysis is paired with primary data collection to provide an overview of the current threat picture. Data collection was carried out throughout September 2025 to gather a sample of 31 online channels linked to groups such as 764, and the wider Com Network. Coding of the harms present in each channel established that within these channels members sought to coerce and victimise individuals through incitement to self-harm and suicide.

Panel 2D: Anonymity, security and resilience: The creative tension between regulatory policy and terrorist exploitation of the internet

Chair: Prof Maura Conway (Dublin City University; Swansea University): [LinkedIn](#); [BlueSky](#)

Panellists:

Prof Miron Lakomy (University of Silesia): [LinkedIn](#)

Dr Ali Fisher (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Arthur Bradley (VOX-Pol Institute): [LinkedIn](#)

Alessandro Bolpagni (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Eleonora Ristuccia (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Grazia Ludovica Giardini (Università Cattolica del Sacro Cuore): [LinkedIn](#)

This session examines original research situated at the nexus of Internet policy and the adaptive communication strategies of terrorist organizations, with particular emphasis on the operational security (OpSec) tradecraft these groups have developed in response to regulatory and technological pressures.

Despite regular announcements of success against terrorist actors ranging from Salafi-Jihadi to Far-Right and Far-Left, they frequently remain online and, in many cases, have expanded their activity across major platforms.

In pursuit of their objectives of galvanizing core supporters and mobilising a mass movement, the Media Mujahidin have refined the operational security needed to preserve anonymity and secure communications with core supporters, while also surviving the disruption now common across mainstream media platforms.

Far-left and Far-right networks have also engaged in a complex interplay between terrorism, violent extremism, and cybercriminality. They have exploited alternative or fringe social media platforms, the decentralised web, and gaming and adjacent platforms.

Combining the learning from the continued presence of these diverse groups, this session examines three interrelated areas that shape how terrorist groups continue to exploit social media and the internet: (1) the policy and regulatory environment in which these groups operate; (2) the OpSec tradecraft they adopt, which makes individuals difficult to identify and disrupt; and (3) the multiplatform networks that provide resilience and a persistent online presence.

Panel 2E: Open-source intelligence and security

Chair: Prof Lella Nouri (Swansea University)

Enhancing Academic Researcher Safety during Terrorism and Extremism Research Projects through Open-Source Tools and a Subject-Based Framework

Almos Huszthy (Ofcom): [LinkedIn](#)

This paper offers a critical overview of selected open-source tools and processes available to academic and civil society researchers to mitigate personal risk in terrorism or extremism-related research projects. In addition, it would introduce a subject-specific framework to assist terrorism and extremism researchers in identifying appropriate tools and determining the appropriate level of operational security for their particular area of inquiry.

In an increasingly interconnected digital and physical landscape, online research into offline terrorist or extremist activities presents heightened risks. Threat actors' potential to detect and trace researchers' digital footprints poses a tangible threat to the individuals or the research institutions conducting the research. This paper argues for a more structured and informed approach to operational security in research practice, particularly in contexts where exposure may cause real-world harm.

Pixeled OPSEC in Focus: Video content analysis of the 2023-2025 Gaza-Israel War

Dr Michael Loadenthal (University of Cincinnati): [LinkedIn](#); [BlueSky](#)

[Co-author: Soumyadeep Bidyanta (University of Cincinnati)]

Since October 2023, Palestinian armed groups have released an unprecedented volume of battlefield media, offering scholars a rare opportunity to analyze how clandestine organizations weaponize digital platforms. Armed groups increasingly rely on platforms to construct visual narratives of conflict, framing battlefield activity as both spectacle and strategic communication. This ongoing study draws on an original dataset of over 2,100 videos produced by 16 distinct military-styled groups operating in Gaza. Each video has been hand-coded across 20 variables, including military activity depicted, weaponry used, and post-production elements such as soundtracks, editing templates, visual effects, digital obfuscation, and video aesthetics. By examining single faction and co-produced outputs, this study highlights strategies groups employ to disseminate propaganda and the evolving aesthetics of extremist visual culture. Special attention is given to operational security practices evident in how video content is filmed, edited, and released. By analyzing the attack-to-release lifecycle, the study interrogates the temporal relationship between combat events and media distribution, yielding insights into operational and narrative strategies. This work advances debates around extremist exploitation of online ecosystems, situating the Israeli-Palestinian conflict within wider comparative perspectives while addressing empirical coding of large-scale datasets, non-English material, and inter-movement studies in extremist media research.

*Social Media as a Source of Operational Intelligence for Terrorist Organizations:
Hamas's October 7 Attack as a Case Study*

Dr Netanel Flamer (Bar-Ilan University): [LinkedIn](#)

Hamas's attack of October 7, 2023 was carried out on the basis of long-term, meticulous preparations that relied, among other things, on a comprehensive intelligence picture the organization possessed regarding the deployment and activities of the Israel Defense Forces (IDF) in the areas surrounding the Gaza Strip. A significant portion of this intelligence was collected from the open domain, and more specifically from the social media profiles of IDF service members.

The study will present and analyze how this information was used to construct the intelligence picture that enabled the attack, illustrating the process through primary materials originating from Hamas itself. This case study serves to demonstrate the use of social media by a violent non-state actor for operational intelligence purposes in the planning and execution of a large-scale attack. Building on this analysis, the study will examine the options available to democratic states for addressing this phenomenon in order to reduce the operational value of social media-derived information for such adversaries.

This study contributes to two central strands in contemporary scholarship. The first is the growing body of research on open-source intelligence (OSINT) in its various dimensions, and the second is the expanding literature on the intelligence capabilities of violent non-state and sub-state actors.

Open-Source Intelligence Companies - A Counter-Terrorism Actor?

Elena Martynova (Metropolitan University Prague): [LinkedIn](#)

The private sector is increasingly playing a significant role in providing open-source intelligence (OSINT) services for European counter-terrorism efforts. Companies such as Maltego, DarkOwl, and TadaWeb have established affiliations at both the supranational and member state levels within the European Union (EU). Their services encompass large-scale aggregation of social media data, automated detection of terrorist content, and the identification of emerging narratives associated with radicalization processes. The nature of these affiliations and their impact on security governance in the EU has not yet been examined. The preliminary argument of this research is that OSINT companies are becoming crucial actors in shaping counter-terrorism policy. Alongside public institutions, they co-create security governance. The research relies on data from corporate blogs, company websites, and public statements, supplemented by interview data. Case studies of several private companies, headquartered both within and outside the EU, are used to analyze the roles these companies serve as well as how and why they contribute to EU counter-terrorism. By better understanding the presence and functions of private OSINT companies in EU counterterrorism, we can recognize the strengths, limitations, and risks of their involvement in security governance and adapt policy processes accordingly to improve outcomes.

Breakout Session 3

Panel 3A: Narratives and identity

Chair: Dr Ninian Frenguelli (Swansea University)

Weapons Inscription: Understanding In-Group References

Dr Katherine Reid (University of Texas at El Paso): [LinkedIn](#)

Dr Christopher Collins (Salem State University): [LinkedIn](#); [BlueSky](#)

This research examines how online extremist ecosystems influence the inscription of text, symbols and ingroup references on weapons used in violent attacks. Drawing on a qualitative analysis of weapons inscription from multiple incidents alongside their corresponding online communities, we trace the pathways through which internet culture diffuses from an online space into physical weapons. We document a shift from inscriptions focused on historical references and legacy building narratives towards an increasingly in-group-oriented context with subculture references and memes intelligible primary to online community members. This evolution reflects the growing centrality of online audiences in motivations and the deepening integration of internet culture into extremist violence.

The Radical Right as Influencers: Online Legitimacy and the Normalisation of Extremism

Dr Keighley Perkins (Cardiff University; Swansea University): [LinkedIn](#); [BlueSky](#)

[Co-author: Prof Nuria Lorenzo-Dus (Swansea University)]

This paper introduces the *influencer role* as a new analytical framework for understanding how radical right groups legitimise their ideology and construct political credibility online. Drawing on a multimodal analysis of tweets from three organisations from across the radical right spectrum—the English Defence League, the UK and Ireland branch of Generation Identity, and Siege Culture—it examines how these groups adopt the strategies and affordances of social media influencers to engage, persuade, and mobilise their audiences. Through tactics such as self-promotion, cross-platform amplification, and self-praise, they position themselves as authentic, culturally relevant, and socially embedded voices, despite their outsider status.

The analysis draws on legitimisation theory (van Leeuwen, 2007) and research on self-praise (Rüdiger and Dayter, 2020; Dayter, 2014) to demonstrate how language and imagery intersect to normalise extremist ideology through familiar online behaviours. By appropriating influencer logics – authenticity, relatability, and interactivity – the radical right blur the boundaries between activism, marketing and political communication. The study contributes to broader understandings of how extremist movements use mainstream social media to construct credibility, offering insights for researchers, policymakers and law enforcement into the everyday communicative practices through which online extremism gains legitimacy.

Calling a Spade a Spade: Conceptualising Violent Extremist Spaces as Fandom

Dr Blyth Crawford (Moonshot; King's College London)

Since the 2019 Christchurch shooting, eleven subsequent attacks directly inspired by Brenton Tarrant have been carried out between April 2019-January 2025. While some mainstream reporting has anecdotally recognised supporters of Tarrant and other mass shooters as “fans”, little academic work has critically considered the similarities between fandom and violent extremist spaces.

This paper builds on 27 months of ethnography I conducted across white supremacist forums between August 2020 and November 2022. I argue that the four definitional characteristics of fandom described by Renee Barnes – social interaction and identity performance, collective meaning-making and appropriation, intense affective engagement, and pleasure from engagement – are manifestly present across these spaces, allowing them to be characterised as a fandom.

I then consider the implications of extending this definition of fandom to spaces linked to violent fixation and the Com Network. I suggest that regarding these spaces as fandoms has profound impacts on academic and practitioner understanding of online radicalisation, and provides a more useful lens for interpreting acts of violence.

Decoding Influence Narratives: Identifying Persuasion and Propaganda Techniques in Twitter Discourse on Violent Extremism

Shu Jia Chee (University College London): [LinkedIn](#)

[Co-authors: Sara Rubini (University College London), Dr Enrico Mariconti (University College London) & Prof Paul Gill (University College London)]

Identifying persuasion and propaganda techniques is crucial for understanding message agendas and designing culturally resonant counter-messages, yet their overlapping nature complicates both qualitative annotation and automated detection efforts. Previous research often examined persuasion and propaganda separately, overlooking their frequent convergence in everyday communication and in digital contexts. To address this gap, our study developed a codebook of 20 unique influence techniques by integrating operationalisations from prior analyses of radical Islamic publications with insights from tweets discussing the 2020 Charlie Hebdo-related terror incidents. As techniques often co-occur, we clustered them to uncover underlying intent and context, distilling the 20 techniques into seven overarching strategies, four of which centred on authority and fallacy-based invocations. A cross-cultural analysis of tweets from five Asian Islamic subgroups then examined differences in susceptibility to these strategies, moving beyond the supply of extremist messaging to reveal the demand-side dynamics of what resonated with audiences. Results revealed significant variation: the Arabic subgroup, for instance, was more susceptible to religious appeals and misinformation-related fallacies than other subgroups. These findings demonstrate that influence strategies are not universally applicable, underscoring the importance of tailoring counter-propaganda messaging to the cultural values of specific audiences.

Panel 3B: “The Digital Bazaar”: Understanding how extremist organisations are exploiting TikTok to share propaganda and radicalise young individuals

Chair: Prof Miron Lakomy (University of Silesia): [LinkedIn](#)

Panellists:

Alessandro Bolpagni (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Silvano Rizieri Lucini (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Alessandra Pugnana (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Eleonora Ristuccia (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Grazia Ludovica Giardini (Università Cattolica del Sacro Cuore): [LinkedIn](#)

Dr Kristin Weber (Centre for Criminological Research Saxony): [LinkedIn](#); [BlueSky](#)

Erik Hacker (SCENOR): [LinkedIn](#)

This breakout session aims to explore how extremist groups exploit TikTok to share terrorist propaganda and violent narratives. The participants will shed light on the presence of a great number of users active in sharing either extremist content or propaganda material to spread extremist ideologies, incite violence, radicalise young individuals, and recruit new members. Particularly, the panel will show content related to extreme right-wing accelerationism, Salafi-jihadism, True Crime Community (TCC), and Christian extremism. The authors will delve into the typologies of actors and the set of tactics and techniques employed by users to share propaganda and extremist content. To summarise, participants will delve into how the aforementioned extremist groups are exploiting TikTok, presenting possible techniques and approaches to efficiently counter the spreading of extremist propaganda and content.

Panel 3C: Theories of misogyny

Chair: Dr Joe Whittaker (Swansea University)

Masculinity as Epistemic Authority: Gender Knowledge Production in a Czech Pickup Artist Forum

Catherine Girard (Masaryk University; Charles University): [LinkedIn](#)

Kristián Földes (Charles University) : [LinkedIn](#)

This presentation examines an active Czech pickup artist (PUA) forum as a site of gendered knowledge production, focusing on how masculinity hierarchies structure epistemic authority and claims to truth. This research conceptualizes the pickup artist forum as a hierarchical, masculinity-based epistemic community in which knowledge about women, dating, gender relations, and gender is produced and legitimized through status performance rather than evidence-based deliberation or plural viewpoints. Using critical discourse analysis, this study traces how platform-specific status markers, such as ranks, badges, seniority, and post counts, intersect with discursive practices to transform personal anecdotes into universalized “facts” about female nature, often articulated through biological determinism, evolutionary “just-so stories,” and pseudo-scientific rhetoric. By situating Czech PUA discourse within broader debates on evidence-based misogyny, epistemological populism, and hegemonic masculinity, this

study contributes to research on the epistemic dynamics of the manosphere beyond Anglophone contexts. It demonstrates how misogynist worldviews are not only affectively sustained but epistemically organized, revealing the role of masculine hierarchies in transforming uncertainty and grievance into authoritative gender “truths.”

Beyond ‘super-posters’ - How do non-active or marginally active incels understand their relationship to incel online communities?

Dr Emilia Lounela (University of Helsinki): [BlueSky](#)

Research has shown that interaction on (extremist) online discussion forums is often dominated by active ‘super-posters’, but that most users are very inactive. Not much is known about these mainly silent participants. In this study, I examine these inactive posters in the context of incel communities.

This study is based on six in-depth interviews with mostly Finnish self-identified current and former incels. The participants differ considerably in both the time they spent consuming incel online material and their level of identifying with incel ideological views. However, in terms of posting and discussing, they were mostly inactive. I explore the personal narratives the participants connect to incelhood and, for many, renegotiating or leaving behind the incel identity. For most, this identity negotiation happened internally; it was not discussed with others either online or offline.

My analysis demonstrates the ambiguity, fluidity, and complexity of identifying with an extremist online community. I discuss the difficulties the participants had in defining what ‘incel’ means in the first place, whether they themselves should be considered incels or not, and what counts as disengagement from an online-based but privately held identity. My findings contribute to understanding the diverse everyday realities of online extremist communities.

Digital Subcultural Diffusion Theory – Rebranding the Incel Ideology Through Looksmaxxing, Sub5s and the PSL scale

Anda Solea (University of Portsmouth): [LinkedIn](#)

The rise of the incel (involuntary celibate) subculture has garnered significant scrutiny in recent years. However, critical gaps persist in understanding how misogynist incel ideology permeates mainstream digital spaces. This paper contributes to our understanding of online radicalisation and dissemination of digital subcultural groups and extremist ideologies through the development of Digital Subcultural Diffusion Theory (DSDT). DSDT outlines and expands upon three interrelated processes: (1) the migration of niche beliefs and artefacts from fringe communities to mainstream platforms (normification); (2) the mechanisms enabling their diffusion and popularisation (mainstreaming); and (3) the possible implications for the normalisation of these ideologies across online and offline spaces. In this context, we apply DSDT to demonstrate how incel ideology is strategically rebranded through the pseudoscientific constructs of the PSL scale (facial attractiveness framework) and looksmaxxing, which cloak misogyny and scientific racism under the guise of self-improvement. This reframing targets susceptible audiences and exploits platform affordances to amplify

and justify male and white supremacist narratives. Drawing on data from TikTok, looksmax.org, and Incels.Wiki, our analysis reveals how platform interconnectivity facilitates the proliferation of incel-adjacent terminology and encourages the legitimisation of extremist, misogynist, and racist views through ostensibly neutral or scientific rhetoric. The study underscores the urgent need to address how digital ecosystems enable the mainstreaming of hateful ideologies, with broader implications for research on online radicalisation and platform governance.

Pedagogies of Disenchantment: Influencer Cultures, Civic Learning, and the Soft Power of Extremist Discourse

Dr Miraji Mohamed (Swansea University; Dublin City University): [LinkedIn](#); [BlueSky](#)

This research explores how the “manfluencer” digital subculture contributes to the circulation and normalisation of extremist content. Influencer cultures and spaces aim at “educating” users about proper and good living. In the manfluencer space, such education revolves around gendered knowledges in ways that make the space productive for circulating extremist and extremist-adjacent content. Their form of education thus is styled and sold as self-help aiming to teach people how to: live a ‘meaningful’ life, be a ‘manly man/masculine’ and how to be ‘feminine’. I argue that influencers such as Andrew Tate, Joe Rogan and Jordan Peterson use narratives framed as self-improvement, free thinking, or lifestyle education to normalise extremist ideologies. Further these narratives circulate across linguistic and cultural contexts through what Rebecca Lewis calls an Alternative Influencer Network. By analysing a variety of materials including videos, podcasts and commentaries by Andrew Tate, Joe Rogan and Jordan Peterson and their reproduction through Dutch podcasters and influencers this research maps the diffusion of key rhetorical and affective frames. It further questions how these ‘alternative education’ ecosystems interact with digital civic learning, potentially reshaping perceptions of expertise, authority, and democratic participation. The study contributes to emerging debates on influencer epistemology and transnational ideological diffusion by conceptualising influencer spaces as informal civic classrooms. I argue that online countering violent extremism efforts should pay attention to how such spaces challenge civic education.

Panel 3D: NVE, Mixed, Salad Bar? Towards a definitional framework for modern attackers

Charley Gleeson (GIFCT): [LinkedIn](#)

Jessa Mellea (GIFCT): [LinkedIn](#)

Recent attacks, the rise in prominence of networks like Com, and irony-poisoned, incoherent motives have challenged the ideological structures used to classify and analyze terrorism. In this roundtable session, participants will collaboratively create working definitions for these emerging networks and movements. Through semi-structured discussions, participants will craft a working definition of the motivations and characteristics of these attackers.

Panel 3E: The current violent extremist threat landscape: networks, platforms, and technologies

The VOX-Pol Institute

This session will provide participants with an overview of recent developments in the use of digital technologies by violent extremist actors. First, it will examine the current tactics and capabilities of jihadist networks online, including how they operate across a range of online platforms and services, their strategies for evading detection (and the extent to which such strategies are in fact necessary), and their uses of AI. Second, it will explore the latest trends in how right-wing violent extremist groups and networks are using digital platforms and services, as well as their connections to violent communities with less clear ideological motivations.

Breakout Session 4

Panel 4A: Anti-gender ideology and the social media landscape in and beyond Canada

Prof Amy Mack (University of Lethbridge): [LinkedIn](#); [BlueSky](#)

Dr Audrey Gagnon (University of Ottawa): [LinkedIn](#); [BlueSky](#)

Dr Kathy Kondor (Norwegian Center for Holocaust and Minority Studies): [LinkedIn](#); [BlueSky](#)

Kayla Preston (University of Toronto)

Over the last decade, scholars have increasingly turned their attention to digital or cyber misogyny with the rise of incels, MRAs, and male supremacist influencers, to understand the relationship between violence, technology, and gender. In this panel, we expand this work to explore how “anti-gender ideology” groups and movements, which span the political spectrum and include populist parties, use social media to target and harass trans and gender-diverse people in Canada. Our first two papers use empirical case studies in Canada to demonstrate the complexity of these movements in terms of membership and tactics. This includes discourse analysis of the social media and web-presences of populist parties, content analysis of social media-based far-right and far-right adjacent groups, and qualitative interviews with teachers and activists grappling with social media-fuelled gender-based violence in their classrooms. The third paper makes connections between this Canadian context and the international flows of anti-gender ideology discourse. The final paper presents research on how activists and educators are pushing back against hate-based and “anti-gender ideology” forces in their communities to provide an empirical and data-driven path forward to countering hate.

Panel 4B: Radicalisation pathways

Chair: Dr Lewys Brace (University of Exeter)

Mapping the forensic psychological mechanisms driving digital hate to offline violence

Dr Rachel Worthington (Cardiff Metropolitan University; Manchester Metropolitan University)

Dr Sören Henrich (Manchester Metropolitan University)

Background: Online hate, including hate speech and other hate-motivated online behaviour such as threats and harassment, has risen sharply since the 2020 pandemic. Its impacts on individuals and online communities are well documented, from increased depression and anxiety to suicidal ideation, and in some cases, escalation into offline violence. Yet little is known about the factors that drive individuals to move from online hate to real-world aggression. This research addresses two key questions: What links exist between online hate speech and offline violence, and what are the implications for policy and practice?

Method: A multi-study combined three interrelated investigations. A new tool, the *Cyber Hate Aggression Offline Survey (CHAOS)*, was created with expert input to measure both

online hate and offline aggression, validated with a representative UK sample (N = 300). Two follow-up studies (N = 150; N = 300) applied CHAOS to examine mechanisms such as social contagion, disinhibition, and neurodiversity.

Results & Implications: Findings highlight psychological and social pathways linking online and offline hate. The presentation will summarise these mechanisms, validate CHAOS as a measurement tool, and offer practical recommendations for individual, legal, and policy interventions aimed at prevention.

Online Female Engagement in Extreme Right-Wing Terrorism (ERWT): Offender Pathways, Roles, and Future Risks

Dr William Allchorn (Anglia Ruskin University): [LinkedIn](#); [BlueSky](#)

[Co-author: Dr Elisa Orofino (Anglia Ruskin University)]

UK counter-terrorism assessments consistently identify ERWT as one of the primary terrorism threats alongside Islamist extremism, with particular concern regarding online radicalisation and lone-actor violence (MI5, 2021; HM Government, 2023). Despite this, women remain largely absent from dominant representations of ERWT within both public discourse and academic analysis. This project delivers a rapid, evidence-based assessment of women's engagement with Extreme Right-Wing Terrorism (ERWT), with a specific focus on online pathways, digital ecosystems, and virtual modes of participation within the UK TACT and TACT-adjacent context. While ERWT has received increasing attention, women's online engagement—particularly in low-visibility, non-operational roles—remains under-examined and frequently underestimated. This research addresses that gap by systematically synthesising open-source academic, legal, and policy literature on how women encounter, consume, and contribute to ERWT-related content in online environments, including spaces linked to proscribed organisations.

Online gateways: Understanding the role of the online domain in initial phases of extremist recruitment

Dr Fabienne Thijs (Netherlands Institute for the Study of Crime and Law Enforcement)

[Co-authors: Charlie Stoeldraaijers (Vrije Universiteit); Dr Elanie Rodermond (Vrije Universiteit; Netherlands Institute for the Study of Crime and Law Enforcement) & Prof Edward R. Kleemans (Vrije Universiteit)]

In recent years, it has become increasingly clear that the internet plays a crucial role in early phases of extremist recruitment. However, these phases have received little attention in existing literature. The current study attempts to fill this gap by examining the role of the online domain in initial phases of extremist recruitment. To achieve this, we combined semi-structured interviews with fourteen professionals who deal with extremism or radicalization in their work and an in-depth netnography of seven online extremist groups. The results demonstrate that the online domain has given new dynamics to extremist recruitment, yet online recruitment is closely intertwined with offline processes. Online “gateway groups” appear to play a key role in initial phases of recruitment, particularly regarding the group's appeal and underlying dynamics of community building. Furthermore, the study highlights that initial recruitment mechanisms differ from mobilization mechanisms, emphasizing that extremist

recruitment and mobilization should be understood as separate processes. Recognizing these dynamics is essential for the development of targeted counter-extremism policies and interventions.

LLMs promote radicalization via engagement with extremist content and politicized communities

Prof Laura Smith (University of Bath): [LinkedIn](#)

[Co-authors: Desislava Bocheva, Dr Catherine Lowery, Dr Olivia Brown, Melissa Torgbi, Siva Worajitwannakul, Harriet Tarpy & Dr Harish Tayyar Madabushi (all University of Bath)]

Large language models (LLMs) are used by the public to summarize, recommend, and explain online content. To prevent generation of potentially harmful output and recommendations, most publicly accessible LLMs have implemented safeguards that are triggered when users ask for illegal content or proscribed groups. However, these models are pre-trained on data from the internet that may contain connections between benign and more extreme content and communities. Therefore, users may ask for seemingly innocuous content about alternative communities but receive potentially radicalizing output. To investigate this possibility, we conducted an experiment with two publicly available, widely used LLMs (OpenAI GPT 4o and Google Gemini). We systematically manipulated the nature of prompts asking for summarization of relatively benign content about the Tradwives community during a multi-turn conversation ($N = 896$). We show that benign prompts, especially those that involve roleplay and retrieval-augmented generation (RAG), can bypass safeguards and expose users to potentially radicalizing content and connections. The implication is that even with guardrails in place and users not intending to seek illegal content, LLMs could play a role in the radicalization process.

Panel 4C: Far-right conspiracies

Chair: Dr Sara Correia-Hopkins (Swansea University)

Extremism and Disaster Relief: A Case Study of Hurricane Helene on Reddit

Dr Sam Jackson (University at Albany): [BlueSky](#)

[Co-authors: Dr Alex Greer (University at Albany) & Dr Samantha Penta (University at Albany)]

In September 2024, Hurricane Helene hit the Southeast of the United States, causing widespread damage in Florida, Georgia, North and South Carolina, Tennessee, and Virginia. As initial relief efforts began, rumors and conspiracy theories quickly spread about the government response: relief funds were spent on “illegal immigrants,” government agencies were using the storm to justify seizing private land, private aid was being blocked, and even that the government caused or directed the storm. These rumors led some people to oppose relief efforts, yelling at relief workers and even threatening violence against them.

In this presentation, we present a case study of discussions of these rumors and conspiracy theories, as well as discussions of threatening actors who disrupted relief efforts. Our case study focuses on East Tennessee and West North Carolina, with data coming from R/Asheville on Reddit (a subreddit for Asheville, North Carolina, which was one of the cities most damaged by Hurricane Helene and is near the border with East Tennessee). This case study will set up a broader study on the politicization of relief, especially where extremist groups or individuals are involved.

Capturing the Light – Framing the Post-Covid UK Conspiracist Movement

Dr Seán Looney (University of Plymouth): [LinkedIn](#)

[Co-author: Dr Rebekah Gregory (University of Plymouth)]

The increasing mainstream relevance of conspiracy theories globally has been tied to increased polarisation and political violence. The Great Replacement, Great Reset, and Q-Anon conspiracy theories have been linked to several acts of violent political extremism. Established in the UK during the COVID lockdown in 2020 The Light ‘Truthpaper’ initially focused on anti-lockdown, anti-vaccine and COVID-19 denial narratives. However, as the distance from the lockdown year has grown the paper has begun to spread Great Reset narratives amongst others. This article seeks to analyse this movement from COVID-19 denial to the incorporation of more extreme conspiracy theories which may lead to acts of political violence by its readership. Using data collected by the University of Bath, this article analyses over 1000 observations (consisting of news articles, editorials, opinions, and letters) using a mixed methods approach of thematic analysis and Structural Topic Modelling. This provides an opportunity to analyse the role organisations like the Light play in circulating conspiratorial narratives both online and offline, as well as the response of its readership.

An Analysis of Far-Right Discourse and Knowledge Building Through Wiki-Based Platforms

Dr Jonathan Collins (Charles University)

[Co-author: Brenna Helm (University of Nebraska)]

Online extremist movements are notoriously difficult to develop interventions for. The disjointed and decentralized nature of online extremist movements serves as an obstacle for intervention efforts, in part because of the difficulties associated with outlining larger uniting goals and shared ideals. This obstacle is particularly salient among far right groups that have various branches and groups with their own distinct priorities and dedicated online spaces. However, online spaces that serve as information repositories for extremist movements offer insight into the ideals, goals, and construction of shared knowledge. Whereas forums and dedicated online platforms can tell researchers and policymakers about the endorsed goals within a specific group and digital space, online information repositories that are developed and maintained by extremists can be leveraged to broaden our understanding of how co-ideologues cultivate an ontology within an ideologically driven movement. In this paper, we use a constructivist grounded theory approach, to analyze how shared knowledge and identity is developed within the far right platform, *Conservapedia*. The goal of this study is to

better understand how users use this space to develop their own far right ontology, as well as discuss the implications of this type of information repository platform for collective identify formation and future intervention efforts.

Symbols of Doomsday: The Digital Reinvention of Far-Right Accelerationism
Kate Tomkins (University of Southampton): [LinkedIn](#)

The digital landscape of extreme far-right accelerationist narratives has undergone a radical transformation in response to the increasing visibility of economic precarities and sociopolitical tensions over the past five years. Accelerationism, a toolkit for extremist actors and agencies, promotes the drastic and often violent exacerbation of sociopolitical tensions. This exacerbation aims for the ultimate destruction of incumbent governing institutions, advocating for the creation of a radically authoritarian society. This paper examines the propagation of acceleration narratives within online TikTok and Discord emergency preparedness communities. Accelerationist narratives disseminated within these communities legitimise violent action, mainstream previously fringe and ideologically fragmented beliefs, and lead to real-world harm through extremist-inspired attacks. The study investigates images, videos, and memes disseminated within these digital communities, analysing them through three levels of Barthesian semiotic analysis. Through a Critical Realist-informed morphogenetic approach, the denotative, connotative, and mythological elements of content are examined. The overarching mythology of content is systematically isolated to explore the structural conditioning and underlying assumptions informing the inherently fragmented far-right accelerationist discourses. This presentation highlights the use, modification and reinforcement of symbolic meanings, suggesting implications for understanding the legitimisation and transformation of narratives for policies needed to mitigate harm.

Panel 4D: Content moderation

Chair: Dr Miraji Mohamed (Swansea University; Dublin City University)

Online Regulation: 'Terrorist' Content and Risk Management
Dr Katy Vaughan (Swansea University): [LinkedIn](#); [BlueSky](#)

This paper examines the regulation of terrorist content, with particular attention to risk management frameworks and their implications for fundamental rights. Drawing on examples from both UK and EU regulatory approaches, it addresses the increasing tendency to rely on pre-existing terrorism offences from criminal law to define and govern online content. While this approach is often justified as promoting consistency between online regulation and offline legal standards, it raises significant challenges. Terrorism offences across jurisdictions tend to be broad, oriented toward conduct rather than communicative content, and heavily dependent on contextual factors such as intent, purpose, and available defences. Translating criminal offences into content moderation duties for online service providers risks over-enforcement, error, and the suppression of lawful expression, particularly where automated tools are used at scale. This paper will highlight how failures to account for context—such as reporting, satire, or crisis situations—can undermine access to information and political discourse. It concludes

by arguing for a rights-respecting approach to risk management that recognises and mitigates the harms arising from enforcement measures themselves.

To moderate or not to moderate? – Psychological determinants of preferences for the level of content moderation and platform regulation

Dr Brigitte Naderer (Medical University of Vienna): [LinkedIn](#)

[Co-authors: Sophia Rothut (Ludwig-Maximilians-University Munich), Anna-Luisa Sacher (Ludwig-Maximilians-University Munich), Prof Diana Rieger (Ludwig-Maximilians-University Munich) & Prof Carsten Reinemann (Ludwig-Maximilians-University Munich)]

Across democracies and online societies, content types like extremist propaganda, borderline content, and lawful-but-awful speech force an important discussion: how far should platforms and regulators intervene to reduce harm without eroding free expression? While policy and platform rules have been studied in recent years, we lack evidence on the psychological predispositions that shape citizens' positions and determine whether individuals generally tend to demand looser or stricter moderation. We argue that stable psychological characteristics mark where people position themselves in this trade-off decision. In a quota-based survey in Germany (N=1,511), we examine four conflict dimensions as predictors:

- (1) Cultural orientation, psychologically rooted in independent vs. interdependent self-construals.
- (2) Values based on the individual's moral foundations.
- (3) Perception of responsibility based on ambiguity tolerance.
- (4) Conception of representation, psychologically founded in social dominance orientation.

To test for asymmetries that are attributable to the group-affiliation of the opinion expressed (ingroup-outgroup-conflict), we include this factor in our study, assuming that individuals demand stricter moderation for outgroup members as compared to ingroup members. Findings will speak to platform policy, P/CVE, risk assessment, and evaluations of regulatory approaches, such as the EU's DSA.

Governing Algorithmic Harms: Non-Removal Approaches to Borderline Content

Ridhwan Mohd Basor (University of Cambridge): [LinkedIn](#)

Social media platforms face a persistent governance challenge: content that normalises hostility, exclusion, or ideological extremism without violating explicit policy thresholds. While platforms have strengthened enforcement against overt violent extremism and hate speech, borderline material – whether religious exclusivism, political mobilisation, or polarising identity narratives – occupies an ambiguous space between permissible expression and potential social harm.

Drawing on my prior experience as a Trust & Safety Global Policy Manager and current postgraduate research in Social Innovation, this paper examines how platforms define and manage ideologically charged content that remains technically compliant with rules yet may contribute to radicalisation pathways or erode social cohesion. Through comparative policy analysis and case studies of borderline extremist content with religious framing, it exposes fundamental tensions in platform governance: balancing

free expression with harm prevention, addressing cumulative effects of repeated exposure, and operationalising context-sensitive decision-making at scale.

The paper evaluates emerging non-removal interventions such as algorithmic dispersion, de-ranking, friction design, and contextual labelling as alternatives to binary removal decisions. It argues that borderline content governance requires moving beyond counter-violent extremism frameworks towards broader principles of proportionality, transparency, and institutional accountability. This analysis contributes practical frameworks for navigating the governance dilemmas inherent in moderating legal but potentially harmful speech online.

Free Speech Might Equal Free Reach: Understanding Freedom of Expression in the Context of Downranking and Borderline Content

Dr Joe Whittaker (Swansea University; VOX-Pol Institute): [LinkedIn](#)

Debates about free speech have been ongoing for over 2500 years, balancing the public value of challenging authority and promoting diverse viewpoints against concerns for security. These tensions are particularly salient in the context of terrorism-related expression, which is inherently political in nature – suggesting that it should, in principle, receive protection – yet which can also contribute to serious and sometimes catastrophic violence.

The rise of social media has introduced challenges for regulating such speech. First, much potentially harmful content is not manifestly illegal, meaning platforms are not legally required to remove it. Second, recommendation algorithms can amplify this content to far wider audiences than it would naturally reach. In response, platforms have increasingly adopted a practice of “downranking” borderline content: reducing its visibility without removing it entirely. This approach is often presented as a compromise between protecting public safety and respecting free expression.

Drawing on Barendt’s arguments for a free speech principle—particularly democratic participation and suspicion of government—this paper argues that downranking raises serious and underappreciated free speech concerns. It further argues that the adage “free speech does not equal free reach” is simplistic, and that a principle is needed to ensure diverse viewpoints are not unduly disadvantaged.

Panel 4E: The pathway to harm: spotting missed opportunities for intervention in violent and dangerous online communities

Holly Belcher (UK Home Office)

Che Tibby (New Zealand Police): [LinkedIn](#)

This session will use a composite, anonymised case study to explore pathways into violent and harmful behaviour, drawing on examples of individuals progressing from engagement with lower-level harmful content through to participation in violent and dangerous online communities. The case study will bring together multiple stages of escalation, enabling a structured discussion of how these trajectories develop over time.

Participants will be invited to reflect on key intervention points across this pathway, considering where earlier or more effective action may have been possible. The session will examine the roles and responsibilities of different actors, including public sector bodies, platforms and civil society, and will explore where greater co-ordination or system join-up could improve outcomes.

Discussion will also focus on the range of interventions that may be effective at different stages, including both established approaches and those drawn from related areas of harm. This will provide an opportunity to consider how existing interventions might be adapted or applied in the context of violent and dangerous online communities, and identify where evidence gaps remain.

By grounding the discussion in a detailed case study, the session aims to support a more practical, cross-system understanding of how pathways to harm can be identified earlier and disrupted more effectively.

Breakout Session 5

Panel 5A: Research practice

Chair: Dr Suraj Lakhani (VOX-Pol Institute)

From Detection to Prediction: AI and the Gradient of Hostility Framework for Mapping Online Extremism

Dr Lydia Channon (Swansea University)

This paper presents a triangulated approach that integrates social theory, computational innovation, and predictive modelling to advance the study of online extremism and hate speech. Building on an intersectional analysis of online harms, it demonstrates how transphobia, racism, and conspiracy narratives converge and adapt across platforms, fragmenting ideology while evading moderation. From this grounding, the paper introduces the Gradient of Hostility Framework (GHF), which reconceptualises hostility not as a binary category but as a continuum mapped across four axes: Directness, Intentionality, Ideological Embeddedness, and Evasion Strategy. The GHF is operationalised through AI/ML pipelines that combine DistilBERT embeddings with SVM classifiers, enabling the detection of overlapping and policy-evasive forms of extremist discourse with greater nuance than conventional systems. Moving beyond detection, the paper deploys large language models (LLMs) to simulate and anticipate rhetorical shifts in response to global events and regulatory change. This predictive capacity demonstrates the potential of AI not only to identify current extremist narratives but to forecast future trajectories, addressing data access challenges while informing proactive responses. Ethical safeguards—including confidence-weighted thresholds, trauma-informed annotation, and human-AI collaboration—ensure that innovation is grounded in responsibility, transparency, and welfare.

GNET as a Knowledge Ecosystem: Mapping How Research Frames Extremism and Technology

Dr Yannick Veilleux-Lepage (Royal Military College of Canada): [LinkedIn](#); [BlueSky](#)

This paper presents a systematic, data-driven analysis of more than 500 essays published through the Global Network on Extremism and Technology (GNET). Using a structured coding framework capturing technology type, platform, ideology, and geography, the study maps how research on violent extremism and technology has evolved within this influential corpus. The findings show that digital communication technologies remain central to the field, with social media, online propaganda, and information operations dominating discussion. Hard technologies such as additive manufacturing, drones, and artificial intelligence appear far less frequently, while areas such as biotechnology, blockchain, quantum computing, and virtual or augmented reality are largely absent. The analysis also identifies a gradual shift after 2022 toward far-right and accelerationist ecosystems and a more diverse set of platforms. Yet, despite this diversification, there is very limited exploration of technological convergence, that is, how distinct technologies combine to produce new forms of extremist capability. Rather than a critique, this study seeks to understand how GNET's

body of work has guided academic and practitioner attention, structured debates on extremist innovation, and influenced emerging research priorities at the intersection of online environments, technological change, and violent extremism.

It turns out you can get PTSD from working in a library: reflections on researcher trauma and conditions of exposure

Dr Leah Farrall

A growing body of scholarship focuses on resilience and prevention for researchers undertaking or institutions supporting work involving traumatic materials, including in our own field through the important contribution of REASSURE. However, a gap remains in accounts of what trauma actually looks like in our research community; how it presents, what it does to thinking and capacity to work, and what it means to live with it, particularly in relation to the journey from unharmed, to harmed but still functional, to incapacitated.

This presentation contributes an account of my PTSD injury from a research role —a reality hard for me, and for some others, to accept because my earlier career in operational work saw me exposed to traumatic events. While it could be easy to conclude that it must have been this work that caused the harm, it did not. Drawing from both these earlier career experiences and the role in which my PTSD injury was incurred, and reflecting on this through autoethnographic approaches, my presentation explores what did and did not cause lasting psychological harm, why this was the case, and what it may suggest about gaps in existing frameworks for prevention, recognition and treatment within our field.

Evaluating Risk: Ethics Departments' perception and understanding of the risk of online violent extremism research

Dr Nicola Matheison (University of Liverpool)

Dr Audrey Gagnon (University of Ottawa): [LinkedIn](#); [BlueSky](#)

Dr Ashton Kingdon (University of Southampton)

A growing body of scholarship focuses on researchers' experiences with institutional ethics processes in the context of online violent extremism (OVE) research. This research notes that ethics departments often lack the expertise to appropriately understand and evaluate the risks of OVE research, which can lead to overestimating or underestimating those risks. This project takes a different approach by analysing how ethics departments assess OVE research projects. To do so, we are conducting a survey of ethics professionals in universities across the UK, US, Australia, Canada, and Ireland that asks them to assess the risk level, perceived ethical considerations, and likelihood of approval in their institutions of a range of OVE project proposals. These project vignettes draw on a range of common methods in the field across different ideological groups. Importantly, we also test for the impact of gender in ethics departments perceptions of risk.

Panel 5B: Countering violent extremism

Chair: Prof Alastair Reed (Coventry University)

Online content moderation and the new AI challenge

Dr Joana Cook (Leiden University): [LinkedIn](#); [BlueSky](#)

Jan Dudra (Leiden University)

[Co-authors: Dr Graig Klein (Leiden University), Ona Jurkevičiūtė (Leiden University)]

In this paper, we present a PRISMA literature review to better understand how existent content moderation methods may still be effective in the online environment increasingly shaped by AI-generated content, and LLMs. Specifically, we ask: How are existent content moderation models affected by AI? This review will specifically investigate how contemporary literature on content moderation has accounted for the rise of AI, with an aim to consolidate contemporary knowledge, and identify important contemporary research gaps. It will do this systematically by summarizing content moderation methods in the literature that have been used to deal with terrorist content online, and how they are affected by AI.

Combatting Online Extremism: The Algorithmic Amplification of Counter-Speech

Ellie Rogers (Swansea University): [LinkedIn](#)

Violent extremists use social media to share content, which can be algorithmically amplified in certain contexts. One countering violent extremism (CVE) strategy aiming to address this problem is algorithmically amplifying counter-speech to target audiences. Examples include Redirection, automatically generating counter-speech and hashtag campaigns. However, there is limited research on the effectiveness of these interventions, due to the challenges of measuring long-term impact. Moreover, these campaigns face ethical challenges such as interfering with users' personal autonomy and choice, and unintentionally generating reactance, thereby reinforcing extremist beliefs. Despite this, limited research addresses the ethical principles underpinning these campaigns. Part of a collaborative project with Moonshot, this presentation aims to address these gaps by exploring the effectiveness and ethics surrounding the algorithmic amplification of counter-speech as a CVE intervention. A mixed-methods design is adopted, including: semi-structured interviews with CVE professionals; and the analysis of evaluation data on algorithmically amplified counter-speech campaigns. This is important to inform policymakers, practitioners, and tech companies of how to ethically and effectively use algorithms to amplify counter-speech. The presentation will identify where resources and research can address existing challenges. This will aid in combatting online extremism efforts and mitigate against potential negative impacts associated with counter-speech.

Addressing the Problems of Social Media and Terrorism in Sub-Saharan Africa: The Civil Society Approach

Ibe Christogonus Chidiebere (African Youths Initiative on Crime Prevention)

Ibe Nkechika Perpetua (Impact Her World Foundation)

The digital frontier in Sub-Saharan Africa has become a double-edged sword. While social media facilitates connectivity and economic growth, it has simultaneously emerged as a potent tool for violent extremist organizations to recruit, radicalize, and disseminate propaganda. Traditional state-centric security measures often struggle to address the nuances of online radicalization, frequently leading to heavy-handed censorship that stifles democratic expression. This study argues for a Civil Society Approach as a more resilient and localized alternative for countering digital terrorism.

Civil Society Organizations (CSOs) occupy a unique position as intermediaries between the state and the grassroots. By leveraging their community trust, CSOs can implement deradicalisation leveraging digital and social platforms, online literacy programs and counter-narrative campaigns that resonate culturally and linguistically in areas where government messaging often fails. Furthermore, CSOs play a critical role in monitoring human rights abuses during state-led counter-terrorism operations, ensuring that security efforts do not inadvertently drive further grievance-based radicalization.

The findings suggest that a collaborative framework, integrating CSOs into national security strategies, is essential. Rather than relying solely on kinetic force or platform bans, Sub-Saharan African states must empower civil society to build community-level cognitive resilience. This multi-stakeholder approach addresses the root causes of extremism while safeguarding the digital rights of African citizens.

Positive alternative narratives as a response to terrorist/extremist propaganda: evidence from formers

Anna Kruglova (University of Salford): [LinkedIn](#)

[Co-authors: Dr Bruce White (Organisation of Identity and Cultural Development) & Dr Jon Wilson (London Metropolitan Police)]

This project's question is: how can people be prevented from supporting/joining violent extremist groups through the use of positive messaging? The first stage of the project aims to establish an evidence-based understanding of the psychological and environmental factors leading to people's decision to disengage from extremist/terrorist groups by gaining direct input from interviews with thirty former terrorist and extremists and people from their close circle. The respondents will be asked to reflect on how they (or their loved ones) became radicalised, deradicalised and, equally, what could have prevented them from becoming radicalised. The theoretical approach informing data collection and analysis will be positive alternative narratives and marketing principles – an idea that to effectively counter terrorist propaganda, it is necessary to adopt a marketing mentality and think about terrorist groups as brands promoting their 'product' (e.g. lifestyle, achievement of a certain goal, etc) and thus a terrorist target audience needs to be offered an alternative to terrorists' offerings – something that would still satisfy their needs but in a peaceful, non-violent manner. The second stage will involve the creation of a series of media (video) materials based on the participants' responses, to be used both directly for campaign facilitation and as training materials.

Panel 5C: Mobilisation pathways

Chair: Prof Maura Conway (Dublin City University; Swansea University)

Re-examining the relationship between neurodiversity and complex cyber-crimes through the lens of strengths, skills and capabilities

Prof Zainab Al-Attar (UCL; Cardiff Metropolitan University)

Dr Rachel Worthington (Cardiff Metropolitan University; Manchester Metropolitan University)

Research shows that neurodivergence is not a risk factor for crime in the general population, but in small sub-groups of neurodivergent individuals engaged in complex cybercrimes, neurodivergence may play highly nuanced roles in shaping many different aspects of the behaviour, motivation and capabilities associated with the cybercrime. The prevalence and relevance of neurodivergent conditions and traits associated with autism and ADHD have been debated in the fields of terrorism, cybercrimes, and a range of online harms. Such debates are commonly contextualized by references to impairments, deficits, vulnerabilities and exploitation. What is often overlooked is the role that specifically advanced skillsets, aptitudes, capabilities and online competencies play in neurodivergent individuals' decisions to engage in complex cyber-crime and the specific capabilities they may possess when doing so. The current paper addresses this gap by examining a range of skills, aptitudes, and traits shown by research and practice to be commonly associated with autism and ADHD. The relevance of such skillsets in shaping capabilities for a range of online crimes and harms will be explored, including terrorism, com networks, nihilistic violent extremism, and mass violence, true crime and shock/gore sub-cultures. Opportunities to divert such skills into protective factors in rehabilitation will be highlighted.

Understanding Hybrid Harms: Disaggregating patterns of engagement with The Com

Dr Caitlin Clemmow (UCL): [LinkedIn](#), [BlueSky](#)

[Co-authors: Dr Bettina Rottweiler (NCITE) & Dr Sandy Schumann (UCL)]

Violent online Com groups (such as 764) are an emerging hybridised threat that blurs the boundaries between organised crime, child sexual abuse, and violent extremism. Operating across both encrypted and mainstream platforms, these groups normalise harm, gamify violence, and use peer validation to recruit and retain members. While often described as 'nihilistic,' little is known about what actually drives engagement. Are participants motivated by ideology, personal grievances, the search for recognition, or thrill-seeking? How do online platforms shape and amplify these pathways, and are these routes into harm distinct from those observed in other violent online movements? This study analyses approximately 70 known cases of Com group members to systematically map trajectories of involvement. Using open-source records, we examine behavioural indicators such as mental health struggles, major life events, thrill-seeking, and peer dynamics that define pathways to a range of harms (doxxing, swotting, inciting self-harm, child sexual abuse, vandalism, etc). By analysing the interplay between motivation and online settings, this research seeks to provide systematic evidence on why individuals participate in violent online Com groups and whether these pathways

represent a truly ‘new’ threat. The findings aim to inform strategies for early detection, disruption, and harm reduction.

The Rising Threat of Nihilistic Violence: Examining Mobilization Pathways of 764 Members

Dr Bettina Rottweiler (University of Nebraska Omaha)

[Co-author: Dr Caitlin Clemmow (University College London)]

The counterterrorism community faces growing challenges as youth and young adults become increasingly involved in terrorism-related activities. In recent years, more young individuals have mobilized toward nihilistic forms of violence that disproportionately target minors and other vulnerable populations, often within online, networked environments. In response, the U.S. Federal Bureau of Investigation (FBI) has identified these groups as an extreme threat and introduced the category of nihilistic violent extremism (NVE). Despite this attention, little is known about the radicalization and mobilization pathways of those involved.

The data for this analysis is drawn from several hundred U.S. federal court records involving individuals who have been either charged and/or convicted of violent crimes and who are affiliated with 764 or adjacent groups. Our case study-based research examines key radicalization factors and compare mobilization pathways across perpetrators. This research seeks to advance understanding of the emerging threat posed by nihilistic online networks and the individuals who engage in this form of violence. In doing so, the study aims to generate empirically grounded insights that can inform more effective prevention, early intervention, and disengagement strategies.

Understanding the complex relationship between algorithms and autism in individuals engaged in online terrorism, nihilistic violent extremism and violence fixation related offending

Prof Zainab Al-Attar (UCL; Cardiff Metropolitan University)

Dr Rachel Worthington (Cardiff Metropolitan University; Manchester Metropolitan University)

The vulnerability of autistic individuals, especially adolescents, to online harmful spaces has been a growing topic of debate in academia, policy and practice. Within this debate, there are common references to the particular susceptibility of autistic people to AI algorithms. However, there is no clinical forensic research to elucidate if and how different features of autism may intersect with AI algorithms. In order to develop our understanding of the complex relationship between autism and AI algorithms in pathways to extremist, mass attack, school shooting, nihilistic and violent fixation related offending, we will synthesise the findings from multiple international research projects on autism and extremism, clinical expertise on autism, and forensic expertise on online terrorism and violence fixation risk pathways. The interactions of algorithms with multiple features of autism will be addressed, including several neurocognitive, behavioural, and sensory facets of autism. Furthermore, the moderating role of common co-morbidities such as ADHD, anxiety, OCD, depression and behavioural addictions, will be considered. A clinical forensic hypothesis on the complex intersections between

each feature of autism and AI algorithms in offence pathways will be presented. Finally, opportunities to deploy these same autism features and the online space to build resilience, will be highlighted.

Panel 5D: Misogynistic narratives

Chair: Dr Brigitte Naderer (Medical University of Vienna)

Media mujahidin: influencers, women and AI

Brontë Philips (BBC Monitoring)

Umaima Zia (BBC Monitoring)

Jihadist groups utilise a variety of online platforms and tools, including mainstream social media, to disseminate messaging both consolidating bases of existing support, as well as finding new audiences. In this presentation, BBC Monitoring's Jihadist Media Monitoring team outlines some of the most recent trends across jihadist groups such as Islamic State (IS) and Tehreek-e-Taliban Pakistan (TTP), based on extensive monitoring of online jihadist environments. This includes self-styled influencers, who mimic popular tropes to sell an aspirational image of the TTP militant lifestyle, as well as the strategic use of women's representation in jihadist messaging. In addition to targeting women as audiences through specific pain points and aesthetics, content depicting women also seeks to sell jihadist ideals, presenting a holistic vision of such groups as viable and cohesive communities by manipulating masculine tropes of defenders and protectors. Such developments illustrate how jihadist groups are able to disseminate content and evade detection through decentralised networks, even mirroring conventions of mainstream social media to reach wider global audiences, particularly among younger users.

Emergency Meeting 63: Extreme Misogyny, Andrew Tate, and the Stoking of Collapse

Dr Elizabeth Pearson (Royal Holloway, University of London): [LinkedIn](#); [BlueSky](#)

[Co-author: Dr Ashley Mattheis (University of Manchester)]

In July and August 2024 far-right rioters targeted asylum hotels, immigrants and shopping centres across England, following online misinformation suggesting the killer of three small children in Southport was an illegal immigrant. British influencers including anti-Islam actor Tommy Robinson and manfluencer Andrew Tate were both active in stoking 'resistance' online, and inciting violence. This presentation analyses the video 'Emergency Meeting 63: Collapse', broadcast by Andrew Tate on Rumble in July 2024 immediately after the Southport attack. The presentation illustrates how Tate's narratives—democracy is collapsing, women are to blame, multiculturalism means ruin—draw on far-right, manosphere, and accelerationist discourses. By presenting violence as both inevitable and righteous, and by invoking fear, shame, and emasculation, Tate draws on a diverse, yet incoherent, set of narratives to resonate as widely as possible with male youth and translate into mobilisation, particularly when amplified by influencers, mainstream media, and political actors.

This paper argues that Tate seeks to escalate digital hate speech into real-world hate crime through three interlinked mechanisms: (1) the normalisation of violent imaginaries (2) emotional scripting and (3) the creation of symbolic events, where attacks or crises are re-framed as evidence of systemic collapse, demanding action.

‘They hate us cause they aint us’: An in-depth analysis of conversations on extreme misogynistic forums; themes, narratives, and justifications

Dr Simone Long (University of Exeter): [LinkedIn](#); [BlueSky](#)

This paper qualitatively scrutinises user threads from four manosphere forums online. Specifically, it pursues an understanding of the narrative practices within the everyday conversations of extreme misogynistic communities (including incels) on the internet. It focuses especially on the (re)construction of users’ extreme beliefs surrounding gender, closely investigating the various rhetorical strategies that serve to reinforce hegemonic masculinity. Furthermore, it examines how such discourse narratively intersects with other hate-based ideologies. Ultimately, it shows how individuals within manosphere spaces draw on widely accepted societal narratives to legitimate their beliefs; in particular, by exploring how more *normalised* expressions of misogyny, racism, etc. in routine interactions can passively facilitate radicalisation into other forms of extremism and enculturation into violent prejudice.

Red Square to Red Pill: Russian Narratives in Reddit’s Manosphere Communities

Catherine Girard (Masaryk University; Charles University): [LinkedIn](#)

Rebecca Rempe (Charles University): [LinkedIn](#)

The manosphere, an online subculture composed of groups that share antagonism towards women, opposition to feminism, and misogyny, has emerged as a salient case study in the evolving landscape of online extremism. The widespread diffusion and normalization of manosphere ideologies, coupled with the community’s emotional grievance-based discourse and decentralized online structure, create fertile ground for exploitation by foreign actors involved in information warfare. Among these actors, Russian influence campaigns stand out for their sustained efforts to deepen existing societal divisions by amplifying emotionally charged content, co-opting digital subcultures, and promoting pro-Kremlin narratives. Between 2016 and 2024, the escalation of Kremlin-backed disinformation campaigns targeting elections, societal stability, and historical grievances coincided with the mainstreaming and normalization of content from formerly fringe manosphere spaces. This convergence raises critical questions about how online misogynistic communities may intersect with broader information operations. Employing Sass and Kuhnle’s gender cleavage theory within a mixed-methods framework, this study combines qualitative analysis of manosphere discourse with social network analysis of the communities that engage with it. Drawing on data collected from five manosphere subreddits, the study explores how Russian information operations may have amplified division, deepened societal discord, and promoted pro-Kremlin narratives within online manosphere communities.

Panel 5E: Distinct remits, but shared mission: How regulation can protect users from terrorism content online

Chair: Jonathon Deedman (Ofcom): [LinkedIn](#)

Panellists:

Dr Murtaza Shaikh (Ofcom): [LinkedIn](#)

Patrick Goodliffe (Coimisiún na Meán)

Hollie Keating Akehurst (Coimisiún na Meán)

Folkert ter Bekke (ATKM)

Kimberly Wakkary (ATKM)

Colleagues from the UK's Ofcom, Ireland's Coimisiún na Meán and the Netherlands' Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) will deliver a joint session that seeks to outline the divergent approaches each regulatory body takes, but the shared objective of preventing users' exposure to terrorism content online. Working from different national legislative and regulatory frameworks, Ofcom, Coimisiún na Meán and ATKM seek to protect users in our constituent locales from terrorism content in distinct ways. We hope this session can both inform TASM attendees how these different systems operate, and improve our own understanding of the harms we seek to regulate through solicitation of prevalence data, definitional frameworks and other theory work to address borderline content, understanding of users' experiences and perspectives etc. This will see colleagues from Ofcom, Coimisiún na Meán and ATKM identifying our remits, our duties and responsibilities under the different legal frameworks, the challenges we have experienced in the last year, and how we intend to move forward and improve, including with input from breakout session participants.

Breakout Session 6

Panel 6A: Crisis, connectivity, and meaning: Exploring youth extremism in the digital age

Dr Brigitte Naderer (Medical University of Vienna): [LinkedIn](#)

Dr Sören Henrich (Manchester Metropolitan University): [LinkedIn](#)

Dr Seán Looney (University of Plymouth): [LinkedIn](#)

Dr Jeremiah Perez-Torres (Marist University): [LinkedIn](#)

This round table session marks the launch of the newly funded Critical Applied Thinking (CAT) Call 2026 project, supported through the Network of European Institutes for Advanced Study (NETIAS), and delivered by a VOX-Pol team. Building from emerging research on nihilistic youth extremism, the panel explores a broader generational shift that underpins contemporary forms of violence, alienation, and disengagement. While complementing other conference panels focused on specific extremist ecosystems, this session deliberately adopts a wider societal lens, asking how changing generational experiences, identities, and perceptions of agency shape contemporary pathways into harmful online communities and extremist cultures.

The session is structured around four short presentations delivered by members of the interdisciplinary research team, spanning psychology, criminology, criminal justice, and communication science. Each presentation acts as a distinct thread for a structured but open roundtable discussion in which all attendees are invited to participate. Together, the presentations trace how previous generational shifts have transformed understanding within adjacent fields and disciplines. These include, for example, how mental health in counterterrorism and political violence was historically marginalised, pathologized, or securitised, and how contemporary frameworks have evolved toward more complex understandings of vulnerability, identity, trauma, and social belonging.

Central to the discussion is a guiding question at the heart of the CAT project: how should researchers, policymakers, practitioners, lawyers, educators, and counterterrorism professionals engage with younger generations experiencing disenfranchisement, dissociation, or loss of agency? The session will critically reflect on both the opportunities and caveats of researching vulnerable youth populations, including ethical, methodological, and practical considerations. At the same time, participants will explore what examples of best practice already exist, within policy, education, community engagement, or justice systems, that demonstrate how younger generations can be meaningfully empowered to feel agency over their futures rather than alienation from them.

Panel 6B: Exit strategies for violence fascination

Christopher Stewart (Human Digital): [LinkedIn](#)

Gareth Harris (Human Digital)

Immersion and participation in digital ecosystems, often from an early age, and the convergence of overlapping harm sets such as pornography, violent misogyny, gore and school massacre ideation have contributed to the emergence of individuals with a non-ideologically motivated fascination with violence. Globally there are efforts from governments and law enforcement to collect evidence on the function violent content plays within pathways to violence, and to use that evidence to design proportionate intervention and exit strategies. This session is designed to get attendees thinking practically about how existing strategies could be applied to this growing harm set.

Panel 6C: Risk tracking

Chair: Dr Katy Vaughan (Swansea University)

When Minutes Matter - Google's Efforts to Stop Online to Offline Violence

Adam Calabro (Google's CyberCrime Investigation Group - Imminent Threats Lead): [LinkedIn](#)

Orlando - Parkland - Buffalo - El Paso. These are the sites of some of the largest mass shootings in US history. Each one of the shooters publicly announced online their intentions to commit an act of violence hours, days, and sometimes weeks beforehand. And there are more examples just like this from around the world. Google's CyberCrime Investigation Group: Imminent Threats (CCIG-IT) seeks to discover, investigate, and report these online threats of violence that occur on Google products before they manifest into real world violence. The team has successfully stopped political assassinations, school shootings, racial and ethnic hate crimes, and child abuse, among many other crimes. This presentation will present some of the real ways that the team discovers these threats, the threat methodologies that the team employs for investigations, the legal basis for informing law enforcement, and real-world case studies of online to offline violence that the team has encountered.

After the Attack: Managing Bystander Footage Online Following Terrorist Attacks – Harms, Rights and Regulatory Responses

Prof Alastair Reed (Coventry University): [LinkedIn](#)

Anne Craanen (Institute for Strategic Dialogue): [LinkedIn](#)

Arthur Bradley (VOX-Pol Institute): [LinkedIn](#)

The widespread online circulation of bystander footage has become a defining feature of terrorist attacks and other acts of public violence in the digital age. Captured and disseminated by members of the public, bystanders, victims, first responder bodycams or CCTV footage, such content can play an important role in informing the public, supporting journalistic reporting, and countering mis- or disinformation. However, it can also generate significant harms. These include supporting the aims of terrorists,

facilitating hate speech and harassment, exposing users to graphic violence, violating the dignity and privacy of victims, and even contributing to misinformation and conspiracy theories by amateur observers misinterpreting the content.

In this paper we analyse the circulation of bystander content online in the aftermath of attacks, highlighting how it can be exploited and weaponised, developing a typology of potential harms. Next, we evaluate platform policies and regulatory approaches, before arguing for a harms-based response and setting out recommendations for victims' organisations, competent authorities and regulators, platforms, EU policymakers, and crisis protocol operators.

From Shared Grievances to Collective Violence: A Cross-Country Comparison of Linguistic Markers for Anti-Government Extremism (AGE) on Parler and Telegram
Leoni Heyn (University of Kiel): [LinkedIn](#)

Berlin 2020, Washington 2021: since the pandemic, surges of anti-government violence have united heterogeneous actors through conspiracy theories and transnational digital networks. Despite this acknowledged reliance on social media, our empirical understanding of (a) the role of digital platforms for the radicalisation of the heterogeneous groups involved in these AGE events in (b) transnational comparison remains limited. This paper examines how digital communication on alternative social media platforms foreshadows collective episodes of political violence in ideologically fragmented anti-government movements. Empirically, it explores theory-driven linguistic markers of radicalisation among verified participants in the attempted storming of the German Reichstag (2020) and the U.S. Capitol (2021), using natural language processing (NLP) on a 17-week longitudinal dataset of over 26,000 Telegram messages and a matched Parler sample. Addressing the low specificity of group-level radicalisation research, the study advances a comparative approach to understanding how increasingly diffuse, internationalised, and cross-platform extremist networks utilise social media prior to offline violence. These findings capture a broader shift in extremism, where decentralised online cultures continue to play an important role in the radicalisation of not only groups, but individuals across a wide spectrum of political contexts.

Examining Online Posting Profiles of Violent and Non-Violent Right-Wing Extremists
Dr Ryan Scrivens (Michigan State University): [LinkedIn](#); [BlueSky](#)
[Co-authors: Dr Garth Davies (Simon Fraser University) & Prof Richard Frank (Simon Fraser University)]

Identifying violent extremists online before their engagement in violence offline is an ongoing need for researchers, practitioners, and policymakers around the world. Yet the evidence base about their posting footprints or differences in their online behaviors compared to their non-violent counterparts is noticeably scarce. Even less is empirically known about the composition or posting profiles making up their online presence. This study drew from a unique sample of violent and non-violent right-wing extremists and used a sentiment analysis-based algorithm that adapts criminal career measures to develop and describe extremist posting profiles (high-intensity, high-frequency, and

high-duration) in the most conspicuous right-wing extremist forum, Stormfront. The results highlight the multi-dimensional nature of the posting profiles of violent and non-violent right-wing extremists, many of which may inform future risk factor frameworks used by law enforcement and intelligence agencies to identify credible threats online. We conclude with a discussion of the implications of this analysis, its limitations, and avenues for future research.

Panel 6D: Understanding and responding to misogyny

Chair: Catherine Girard (Masaryk University; Charles University)

Mainstreaming Misogyny: A social network analysis of incel-related content on TikTok

Christopher V David (Neu-Ulm University of Applied Sciences): [LinkedIn](#); [BlueSky](#)
[Co-author: Marten Risius (Neu-Ulm University of Applied Sciences)]

Incel ideology is increasingly less confined to niche forums, but visible on mainstream platforms such as TikTok. To capture this shift, we apply a network-analytic approach to incel-related activity using data collected through the TikTok Research API. Our study responds to recent findings that incel-associated concepts such as *looksmaxxing* or the *blackpill* undergo a process of ‘Normiefication’ on TikTok, in which formerly fringe narratives are blended into digital youth culture and men’s mental health discourses.

While prior research based on ethnographic observation or sockpuppet accounts has offered valuable insights into misogynistic narratives and suggests that incels use strategic overlaps with financial gain, men’s mental health, and right-wing extremism for their messaging, less is known about structural clusters and cross-community dissemination patterns of misogynistic ideology.

Through a network approach, we investigate three central dynamics: 1) whether incel-related hashtags and creators form distinct structural clusters, 2) whether men’s mental health and self-improvement content has a bridge function into incel-related content, and 3) whether overlaps exist between incel clusters and far-right or white supremacist content. By mapping these network structures, we give actionable insights for content moderation efforts, and provide an understanding of how extremist narratives diffuse across mainstream platforms.

Breaking the Black Box: Social Network Analysis as a Tool to Track Algorithmic Recommendations in the Manosphere

Clara Jammot (King’s College London): [LinkedIn](#); [BlueSky](#)

The network is a prominent concept in the study of extremism and of social media with Social Network Analysis (SNA) being used to study extremist structures both online and offline. Even though today’s era of algorithmic recommendation means that online social networks are constantly forming and re-forming, there has been a lack of innovation in SNA applications. As this paper demonstrates, a novel approach can be taken to SNA to make it more flexible and to study not only traditionally visible community relations but also the less visible online radicalization process.

Drawing on Manosphere research that collected over 38,000 TikTok accounts, this paper discusses how SNA can allow for the algorithmic recommendations of extremist content to be mapped and for the, normally invisible, connections that the algorithm makes between this recommended content to be revealed. In doing so, it sheds light on how extremist content is recommended, how it evolves over time, and the influence extremist accounts have compared to the other accounts that a user may consume. This application of SNA finds a way to break through the algorithmic black-box that has presented a long-standing challenge to the study of extremism on social media, encouraging further methodological innovation.

Calling out, calling in: Assessing grassroots responses to countering male supremacism in support-focused manosphere subreddits

Dr Allysa Czerwinsky (University of Manchester): [LinkedIn](#)

Drawing on Lee's (2019, 2020) work tracing uses of informal countermessaging for ideological extremism online, this research challenges an increasing reliance on top-down deradicalisation efforts by exploring how naturally occurring peer-driven interactions can help drive disengagement from male supremacist extremism. In analysing user-to-user interactions across 50 threads posted to two support-focused manosphere subreddits (r/ExRedPill and r/IncelExit), I highlight six strategies that non-manosphere and former manosphere users employed in interactions with current and exiting users, often aimed at addressing distinct concerns within individual posts related to the belief systems and ideologies shaping and motivating participation in manosphere spaces; the weaponisation of subjective experiences with victimisation, rejection, and harm, and identity-based motivations and emotional impacts of community involvement. Importantly, findings explore how different approaches impacted conversational flow, prompting either repeated engagement in replies or stymying opportunities for additional support. The results illuminate how online spaces can foster bottom-up approaches to countering harmful ideologies, highlighting the importance of citizen-led initiatives to build resilience, resistance, and trust through everyday conversations on public online platforms. Moreover, the strategies used organically in online spaces both complement and enhance existing approaches to preventing and countering male supremacism and misogynist extremism.

Countering male supremacist influencers through "campaigns to promote resilience and digital literacy"

Dr Luc Cousineau (Dalhousie University): [LinkedIn](#); [BlueSky](#)

There is robust and ever-growing evidence that misogynistic, masculinist, and male supremacist ideas, promoted heavily by swaths of manosphere influencers and grifters, are having deep social and cultural impacts beyond their viewer/listenership. We see these impacts in politics (Dovi, 2025), sport (Vollbrecht, 2025), and especially educational settings like classrooms (Sandau & Cousineau, 2025). This paper presents data from Canadian research, contextualized through international work exploring the prevalence and impact of misogyny in educational spaces and on teachers themselves. Data from social media and interviews shows that the exfiltration of misogynist and male

supremacist rhetoric from the masculinist influence-sphere is changing educational settings and some boys and young men feel (re)empowered to refuse women's authority, make derogatory remarks about women and teachers, and in some cases engage in non-consensual sexual touch of teachers and classmates. Data also suggests that the work of countering these influence(r)s can be accomplished, in part, through campaigns that promote resilience to anti-equity messaging and promote more fulsome understandings of boyhood and manhood, as well as digital literacy education for teachers, parents, and children. The data presented here compliments ongoing international efforts by organizations like Movember, Equimundo, and White Ribbon to build new interventionist strategies to counter and counteract this (re)invigorated wave of misogyny.

Panel 6E: Design, detect, decide: A hands-on lab for terrorism safety in AI

Representatives from OpenAI

As generative AI becomes embedded in social and information ecosystems, platforms must rapidly adapt their safety processes for violent extremist content and related harms. This workshop, led by OpenAI's Protection team, is a structured, hands-on exercise where participants collaboratively design and test a simplified end-to-end Trust & Safety system for how high-risk content may surface across AI platforms and services. Focused on usage policies and user behaviour, the session blends policy thinking, detection strategy, AI-assisted analysis, and case evaluation, reflecting the operational approaches used by real-world platforms.

Breakout Session 7

Panel 7A: The only way is ethics: An open conversation on safety, standards, and solutions in extremism research

Dr Ashton Kingdon (University of Southampton)
Dr Allysa Czerwinsky (University of Manchester)
Bradley Galloway (Ontario Tech University)
Dr Antonia Vaughan (Moonshot)
Dr Elizabeth Pearson (Royal Holloway University)
Dr Nicola Matheison (University of Liverpool)
Dr Audrey Gagnon (University of Ottawa)
Dr Meili Criezis (American University)

Extremism research has expanded rapidly, but ethical frameworks and institutional support lag behind. Researchers face challenges beyond standard protocols: accessing sensitive data, exposure to traumatic content, physical and digital safety risks, and the danger of amplifying extremist narratives. Institutional responses remain inadequate and inconsistent, with protection gaps varying by resources, location, and discipline. This interactive roundtable critically assesses the current state of research ethics in extremism studies and charts a path forward. Using a ‘fishbowl’ format, audience members are actively encouraged to share experiences and ideas alongside panellists, generating honest reflections and healthy debate.

Key questions to be explored include:

- How do we balance understanding extremism with risks of amplifying harmful content?
- What protections are needed for researchers’ mental health when engaging with traumatic material?
- As platforms restrict data access, how can we maintain research transparency while respecting ethical boundaries?
- How do we better prepare and protect the next generation of extremism researchers?
- What does robust ethical infrastructure look like?

Participants will examine the adequacy of current ethical guidelines, researcher wellbeing and mental health support, cybersecurity challenges, the ethics of working with closed-source data, and institutional responsibilities in safeguarding researchers.

This session moves beyond problem identification toward actionable solutions, including specialised training, dedicated safety resources, and recognising digital security as integral to research ethics. Through cross-disciplinary knowledge exchange, we will establish a shared vision for ethical practice that prioritises both research integrity and researcher wellbeing while advancing understanding of critical societal challenges.

Panel 7B: Online safety regulation in action: Balancing rights and risk

Alistair Pullar (Ofcom): [LinkedIn](#)

Murtaza Shaikh (Ofcom)

Laura Waters (Ofcom)

Almos Huszthy (Ofcom)

In this session, after each convenor/panellist provides a brief presentation on their team and its functions, we will provide workshop participants with a cross-platform, multi-service scenario and details of where risks arise. These risks could be the result of a risky functionality, a particular user demographic, a cultural proclivity etc. We will then split the workshop participants into groups who will act as constituent internal Ofcom teams represented by the above speakers who will take each smaller group through the process of Ofcom engagement by their constituent team. This will include identifying data needs, forming necessary stakeholder partnerships to identify compliance, engaging with services to identify what changes can be made through informal engagement, and establishing appropriate and proportionate policy responses. Ofcom colleagues will go around the smaller teams and provide insight and support while these teams identify what activities would be necessary as part of the wider objective of ensuring compliance and delivering user – especially child user – safety. The room will then reconvene and identify where the process is effective, but also where it could and/or should be improved to better ensure user safety and/or affirm user rights, whilst fulfilling Ofcom’s regulatory duties under the law. We hope this breakout session will both improve our internal processes, and improve stakeholders’ understanding of these processes, but also allow stakeholders to understand where engagement with Ofcom could be valuable and appropriately targeted in the future.

Panel 7C: Designing responses

Chair: Dr Sören Henrich (Manchester Metropolitan University)

Doing Terrorism or Doing Crime: Locating “Nihilistic Violence” from “Com Networks” in Relation to Online Extremism

Dr Ashley A Mattheis (University of Manchester): [BlueSky](#)

Concerns regarding “nihilistic” violence conducted by members of so-called “com networks,” like 764, are increasing across research and policy arenas. These networks conduct a wide range of criminal activities including violent acts. And, they have some connections to violent online extremist ideologies. However, calls to categorise them as a new form of violent extremism problematically do not account for digital processes of adaptation and admixture that encourage engagement between these digital cultures (e.g., criminal and extremist) through shared interests like glorifying violence. Primary reasons for not categorising com networks as violent extremism are their lack of ideological drivers and political goals. Instead, com network practices produce collectives focused on committing crime, violence, and victimisation, even using manipulation and sextortion within the networks to force members to participate in violence and crime. Com networks, then, are not extremist per se, but represent: 1) new

modes of committing violent, criminal action, 2) highlight (s)extortion as a method of socio-behavioural control within digital networks, and 3) show how gamification of violence (brinksmanship, one-up-man-ship) contributes to violent action. Understanding these com network practices along with digital processes of admixture and adaptation may better prepare researchers and practitioners for violent extremist adoption of such techniques.

“DDoS Rockets on Russophobic Countries” - An Examination of a Pro-Russian Hacking Forum

Sara Rubini (UCL): [LinkedIn](#)

[Co-authors: Prof Paul Gill (UCL) & Dr Brian Klaas (UCL)]

Since Russia’s full-scale invasion of Ukraine in February 2022, cyberattacks have intensified across Ukraine and Western nations. Despite the strategic importance of these operations, limited research has examined the role of pro-Russian hackers in the conflict. This study addresses that gap through a qualitative content analysis of 5,858 posts from a filo-Russian hacking forum, sourced via the Cambridge Cybercrime Centre, spanning August 2022 to July 2024. It investigates four key questions: (1) Who are the individuals involved in this forum? (2) Who are the primary targets of filo-Russian hackers in the war against Ukraine? (3) Which cyberattacks do Filo-Russian hackers carry out? (4) Do these actors employ neutralisation techniques to justify their actions? Findings reveal that hackers are self-organised, transnational, and frequently target both state and private entities, with a particular focus on critical infrastructure. Notably, the cyberattacks are not limited to Ukraine; we identified operations targeting organisations in 42 different countries worldwide. We also found evidence of neutralisation techniques, especially denial of victim and defence of necessity, suggesting attempts to justify their actions within an ideological framework.

Countering Online Extremism in Pakistan

Dr Shabana Fayyaz (Quaid-i-Azam University): [LinkedIn](#)

Pakistan, with its rapidly expanding internet penetration and large youth population, faces significant challenges related to digital extremism. This study examines the emergence of online extremism in Pakistan and evaluates the effectiveness of state policies designed to counter it. Using a mixed-methods approach, it maps the ecosystem of virtual extremism and identifies the digital platforms used to disseminate extremist narratives, drawing on examples from violent non-state actors to understand their modus operandi.

The study analyzes the state’s response, tracing a shift from initial denial to policy recognition, and evaluates the legal and institutional measures undertaken. While Pakistan has developed a comprehensive framework to address digital extremism, the findings highlight persistent implementation gaps, technological limitations, and concerns regarding digital rights that hinder effective outcomes.

The study emphasizes the need for a proactive, multi-sectoral approach, including investment in indigenized cyber literacy, improved regulatory coordination, and efforts

to bridge the trust deficit between the state and society. Empirically, the research integrates qualitative and quantitative methods, including interviews with policymakers, legal experts, and institutional stakeholders, along with focus group discussions involving university youth and digital rights groups.

Digitally Mediated Threats: Ideological Grievance, Platform Use, and Escalation in Federal Threat Prosecutions

Grant Van Robays (the Prosecution Project)

Carter Langham (the Prosecution Project)

Michael Loadenthal (the Prosecution Project)

Digital platforms have reshaped how ideologically motivated threat and harassment activity is communicated. In the U.S., attention has focused on how such threats target public and elected officials. Analysis is needed to understand how these communications are produced and adjudicated across targets, platforms, and technologies. Our research addresses this by examining data and evidentiary materials from felony criminal cases. We investigate motivations, profiles, and communication platforms in threat and harassment cases, distinguishing those driven by extremist ideologies from non-ideological cases. Ideological cases, specifically those including terrorism and violent extremism, are analysed to identify behavioural and tactical patterns among those using threats or harassment as a form of criminality.

This research examines changes in the frequency and nature of threat and harassment cases. It analyses how platforms are used by ideological actors and the differences between threats transmitted through traditional services versus security-centric (i.e., end-to-end encrypted) platforms. It assesses threats against various targets, considering how those directed at public and private figures relate to legal outcomes, accounting for factors like platform and ideology. This work strengthens the understanding of how individuals driven by extremist ideologies use digital platforms to threaten or harass, and how this translates into legal consequences.

Panel 7D: Project Catalyst: Comparative interventions tackling violent extremism and misogyny in gaming communities and platforms

Galen Lamphere-Englund (Christchurch Call Foundation): [LinkedIn](#)

Anne Craanen (Institute for Strategic Dialogue): [LinkedIn](#)

Amee Wurzburg (American University): [LinkedIn](#)

Hesbone Ndungú (Search for Common Ground): [LinkedIn](#)

In 2025, the Christchurch Call Foundation (CCF) started work on Catalyst, an 18-month initiative designed to address online misogyny and gender-based violence linked to violent extremism, focused largely on gaming and gaming adjacent platforms and communities. Implemented through a Consortium led by CCF, Catalyst brings together expert partners including the Institute for Strategic Dialogue (ISD), Meedan, Search for Common Ground, the Polarization and Extremism Research & Innovation Lab (PERIL) at American University, and the Blavatnik School of Government at the University of Oxford.

The project encompasses 12+ programmatic, research, and policy tracks in Canada, Jordan, and Kenya, as well as across transnational gaming communities. During this panel, we will share preliminary insights from research in Arabic, Swahili, and English, along with comparative offline and online interventions to addressing online misogyny and its connections with violent extremism.

At TASM, the Catalyst Consortium will present on key pillars of work that explore Catalyst research and interventions that are designed to support online communities to better tackle misogyny and extremism. Members of the Consortium will present findings from their respective areas of intervention: livestreamer led campaigns; community moderators bystander training on gaming platforms; offline peer mentor programs; building LLM classifiers to detect tech facilitated gender-based violence content in low-resource languages; and, the mapping and responses to the ‘manosphere’ across the three contexts. Other efforts on civil servant policy training and global policy dialogues are also underway. The session is intended to share research findings and lessons learned from direct interventions designed to build resilience amongst gaming communities along with support mechanisms for platforms working to address harmful content.

Panel 7E: Discord and deception: Radicalisation through the lens of Danny’s story

Samuel Kashti (Shout Out UK): [LinkedIn](#)

How can we make a counter-terrorism case study feel relevant to young people in Swansea? That was the central issue we grappled with when designing this project. This panel pulls back the curtain on a unique collaboration where we took a raw Cardiff CT case study involving the Extreme Right Wing (‘Danny’ Story’) and “Swansified” it through the lens of local intelligence, with a target audience in mind. The goal was to devise a resource capable of being engaging as well as prebunking a section of society from harmful narratives.

We didn’t just guess what radicalisation looked like; we tracked it. By combining SOCMINT (scraping and analyzing local Facebook groups looking for particular hot topics that the Extreme Right Wing were engaging in) with boots-on-the-ground OSINT (mapping extremist graffiti and physical identifiers across the city), we built a hyper-localised narrative. This involved searching the streets of Swansea for symbols of extremism, where this very conference is taking place. This data didn’t just sit in a spreadsheet or inform an academic journal, it helped inform a skeleton script of a fictitious story inspired by true events, designed for schools and universities.

We’ll be discussing ‘Danny’s Story’ not as a theoretical exercise, but as a practical demonstration of how multimedia resources and storytelling can bridge the gap between police/OSINT data and classroom/public engagement, to bolster people’s resilience to harmful narratives and disinformation online.

Breakout Session 8

Panel 8A: Researcher safety by design: Modelling practical OPSEC for studying digital extremism

Dr Michael Loadenthal (University of Cincinnati): [LinkedIn](#); [BlueSky](#)

This interactive, hands-on workshop invites researchers, practitioners, and policymakers into a practical exploration of how to work safely, sustainably, and confidently in the study of violent extremism and contested digital environments. Rather than treating risk as an abstract concern, the session equips participants with concrete tools to identify, contextualize, prioritize, and mitigate threats that emerge across physical, digital, and psychosocial dimensions of research. Drawing on threat modeling and public health-inspired harm reduction frameworks, the workshop emphasizes resilience, adaptability, and long-term well-being.

The session unfolds in three dynamic stages. First, participants build individualized threat models using accessible, creative techniques such as asset inventorying, mind mapping, and structured analytic tools. This process helps attendees clarify how risks vary by research topic, method, and positionality. Second, these models are transformed into actionable mitigation strategies using a harm reduction lens that prioritizes realistic, proportional interventions over one-size-fits-all solutions. Participants learn how to decide what matters most, what can wait, and where small changes can meaningfully reduce harm.

The final stage delivers an engaging “101 crash course” in operational and digital security, tailored specifically to research workflows. Through live demonstrations, participants explore tools such as VPNs, secure cloud storage, password managers, virtual machines, browser extensions, identity separation techniques, and secure messaging platforms. These tools are applied directly to everyday research practices, with a focus on protecting identity, safeguarding sensitive data, and using technology to maintain healthy boundaries when engaging with violent or disturbing material.

Blending case studies, scenario-based exercises, and collaborative discussion, the workshop is designed to be energetic, inclusive, and immediately useful. Participants leave with both a clear risk-management framework and practical skills they can deploy right away—making this session especially valuable for early-career scholars and anyone seeking to build safer, more sustainable research practices.

Panel 8B: Harnessing multistakeholder power: Driving collective action for global challenges

Chair: Andy George (Christchurch Call Foundation)

Panellists:

Anne Craanen (Institute for Strategic Dialogue): [LinkedIn](#)

Dina Hussein (OpenAI): [LinkedIn](#)

Georgia Wake (UK Home Office)

Dr Katy Vaughan (Swansea University): [LinkedIn](#); [BlueSky](#)

Global challenges, such as eliminating terrorist and violent extremist content online, cannot be solved by governments, tech companies, or civil society alone. They demand shared responsibility and coordinated action. This workshop will:

- Discuss how multistakeholder frameworks operate to create impactful, scalable solutions in increasingly complex geopolitical and policy environments.
- Drawing on the Christchurch Call as a leading example, explore how multistakeholder approaches are evolving in increasingly complex geopolitical and policy environments.
- Look at the future of global multistakeholderism, generating ideas for future frameworks and collaboration.

Panel 8C: Imagined identities

Chair: Dr Ashton Kingdon (University of Southampton)

Comparing Far Left and Far Right Group Identities Online: Expanding ‘Imagined Political Communities’ to Account for Inclusion-Based Formations

Prof Lella Nouri (Swansea University): [LinkedIn](#); [BlueSky](#)

Dr Ninian Frenguelli (Swansea University): [LinkedIn](#); [BlueSky](#)

Social media platforms have become central infrastructures for political participation and community formation. Existing scholarship on political engagement online has identified the discursive practices involved in the creation of far- and extreme-right group identities and how this contributes to radicalisation, polarisation, and antagonistic mobilisation. Less studied is how left-wing groups create these identities and how, and if, this differs from the processes of the right. This article addresses that gap through an integrated mixed-methods study of 37 left-wing activist groups in south Wales, analysing 1,154 Facebook and Instagram posts. Building on prior work on threat-based imagined political communities, we extend Anderson’s theorisation of imagined community to demonstrate how left-wing activist groups enact political belonging through solidarity, coalition-building, and mutual recognition rather than exclusion-based rhetoric. This extends to outgroups. Outgroups were constructed in a minority of posts in our dataset, and, where they were constructed, the majority of the posts did this in an ‘agonistic’ way whereby the outgroup was seen as legitimate and not as a threat to the ingroup, differentiating this from far-right posting. We offer a comparative framework distinguishing threat-based and solidarity-driven imagined political communities to

analyse how political belonging is imagined, enacted, and sustained across divergent ideologies.

Imagined Extremist Communities: The Paradox of the Community-Driven Lone-Actor Terrorist

Inger Storm Sandboe (University of Oxford): [LinkedIn](#)

This article introduces “imagined extremist communities,” a term that encapsulates the unique social landscape where right-wing lone actors, despite not being affiliated with organised groups, partake in a form of communal interaction. By examining the cases of Breivik, Tarrant, and Manshaus, this article illuminates how group-based and lone actors are more alike than what is conventionally expressed in existing research. Although lone actors are not subject to an external command like group-based actors are, the imagined extremist community functions as a “group” for lone actors and is, for all practical purposes, a corresponding alternative to a terror cell. During the radicalisation process, these individuals seek and turn to the imagined extremist community, enabling them to form a sense of belonging and identification and underscoring that these actors, although conventionally labelled as “lone,” are immersed in an alternative culture that nurtures their ideas and sustains their extremist ideology. This becomes particularly evident through their cognitive radicalisation, a process amplified by their psychological predispositions. The concept of the imagined extremist community elucidates how lone actors, especially those embracing right-wing ideologies, are subject to radical influences. Their conservative traits and psychological dispositions make them particularly receptive to the appeal of such communities.

Files, Firearms, and Fantasies of Insurgency: The Myanmar Conflict in Online 3DPF Culture

Jake Wright (Leiden University): [LinkedIn](#)

[Co-authors: Dr Yannick Veilleux-Lepage (Royal Military College of Canada) & Dr Ayse Lokmanoglu (Boston University)]

This article examines how the insurgency in Myanmar has been interpreted, discussed, and symbolically appropriated within the 3D-printed firearms community by analyzing Reddit discussions from the FOSSCAD subreddit, the platform’s primary hub for 3DPF discourse. Drawing on a dataset of posts and comment threads referencing Myanmar between 2021 and 2024, we explore how distant armed struggles are used to construct meaning, legitimacy, and purpose within this decentralized, transnational, and largely Western community. Using qualitative thematic analysis and informed by notions of imagined solidarity, vicarious militancy, and symbolic boundary-making, we show that the Myanmar conflict serves not merely as a site of tactical inspiration but as a crucial symbolic reference point. 3DPF community members interpret the actions of Myanmar rebel groups as a validation of their own technical efforts, ideological commitments, and visions of resistance. We argue that these discussions reflect a process of reflexive identity formation, in which an imagined connection to foreign insurgency provides a narrative scaffold for interpreting local activities and broader political goals. The findings contribute to our understanding of how online extremist or fringe technical communities

engage in meaning-making by selectively projecting themselves into distant conflicts, thereby constructing imagined communities across space and context.

Discursive performance of collective identity in a white nationalist forum: A social movement theory perspective

Dr Amy Booth (Aston University): [LinkedIn](#)

The concept of collective identity has been highly influential for social movement theory, and, more recently, in the study of extremism. Defined as an interactively negotiated sense of ‘we’-ness (Snow, 2001), collective identity serves as a ‘reward’ for engaging in a social movement, and is therefore a crucial component in motivating collective action and sustaining movements (Melucci, 1989).

Social media plays an ever-increasing role in all forms of activism, including extremism. However, some scholars have questioned whether true collective identity, in the sense described by social movement theorists, can emerge in online spaces, highlighting the supposed *networked individualism* of social media and arguing that this inhibits the development of a truly shared, collectively negotiated identity (Bennett & Segerberg, 2012).

In this paper, I demonstrate the existence of a collective identity in a white nationalist forum by exploring how individuals’ discourse in the forum changes over time, showing their assimilation to a collective identity. I do so with reference to the three elements of collective identity described by Taylor and Whittier (1992): the drawing of *boundaries*; the raising of a socio-political *consciousness*; and the *negotiation* of the meaning of everyday symbols and practices, imbuing them with movement-related meaning.

Panel 8D: Youth radicalisation in gaming spheres: Evolving threats, P/CVE engagement and policy responses

Dr Erin Saltman (GIFCT): [LinkedIn](#)

Julien Bellaiche (GNET): [LinkedIn](#)

Dr Jessica White (RUSI): [LinkedIn](#)

Eve Marron-Bonathan (Twitch)

The gaming sector is the world’s largest entertainment sector with around three billion people playing video games. In recent years, violent extremists of various ideological leanings – including right-wing extremists, jihadists, and violent nihilists – have been seeking to exploit the popularity and social connectivity of gaming spaces to spread their message, mobilise, and recruit. These efforts include the production and dissemination of propaganda games, the instrumentalisation of existing games, the exploitation of in-game communication features and gaming-adjacent platforms, the use of gaming aesthetics and cultural elements for propaganda, and limited use of fundraising via gaming surfaces. This activity raises concerns over threats of radicalisation of users - particularly among young audiences - as evidenced in recent national and regional counter-terrorism strategy reviews (e.g., in the UK and EU), with an increasing number of minors being charged with terrorism offences.

Since 2024, GIFCT has invited researchers, policymakers and subject matter experts to investigate these dynamics and offer actionable insights for prevention and countering extremism in gaming communities. The Extremism and Gaming Research Network has also convened and commissioned regular research on the subject since 2020 in partnership with RUSI. Building on this work, and over 133 published articles in the last five years, this panel will bring together GIFCT, GNET, EGRN, and RUSI experts to examine the state of violent extremist exploitation of gaming (-adjacent) platforms and the threat this poses for youth radicalisation in these spheres. It will discuss the latest threat trends and forthcoming changes in the field, including rapid digitization across new contexts (West Africa, for example), and the increasing hybridized ecosystems of violence underpinning youth radicalization.

The discussion will also highlight promising prevention and positive intervention strategies as well as policy responses and best practices to prevent and disrupt violent extremist exploitation of gaming spaces.

Panel 8E: Interacting networks: Collaborative clusters to counter online terror threats

Chair: Meredydd Hughes (SAHER (Europe))

With representatives from the NOTIONES and TATE projects, and SAHER (Europe)

This session will begin by introducing the NOTIONES project, the aim of which is to establish a network to connect researchers and industries with the intelligence community, facilitate exchange on new and emerging technologies, and equip solution providers with insights on the corresponding needs and requirements of practitioners. Members of the Tech Against Terrorism Europe (TATE) project will then present some of its key findings, including an analysis of platforms being exploited to host terrorist content and challenges faced by those implementing the EU's Terrorist Content Online (TCO) Regulation. Finally, SAHER (Europe) will provide an introduction to the TCO Cluster.

Panel 8F: Aesthetics, identity, ideology and euphoria: perspectives from South Asia, Southeast Asia and Oceania

Chair: Ottavia Galuzzi (UNICRI): [LinkedIn](#)

Trends and Dynamics of Online Extremism in Southeast Asia

Benjamin Mok (S. Rajaratnam School of International Studies): [LinkedIn](#)

This presentation examines the changing dynamics of online extremism in Southeast Asia, arguing that the regional threat landscape is no longer adequately captured by older frameworks centred primarily on platform migration, localised propaganda, or the persistence of Islamic State-supporting networks. Instead, recent monitoring indicates a more fragmented and event-responsive ecosystem in which extremist narratives circulate across jihadist, far-right, nihilistic violent extremist, and non-violent Islamist

milieus. The presentation also examines the growing importance of youth-facing and affective online cultures within Southeast Asia, including nasheed archiving, TikTok edits, gaming spaces, Jemaah Islamiyah “fandom”, and nihilistic violent extremist aesthetics. These environments blur the boundaries between ideology, performance, grievance, and fascination with violence.

Key dynamics include how online extremist ecosystems within the region have adapted to disruption through replacement archives, multilingual groups, and renewed emphasis on decentralised movements focused on subcultures and niche communities. At the same time, regional and global crises have been repeatedly reframed as validation for extremist worldviews – this involves online communities actively re-scaling grievances, reframing distant conflicts as local obligations, and transforming global extremist identities into regionally meaningful subcultures. As such, this presentation approaches Southeast Asia not merely as a passive recipient of global extremist content, but an active site of localisation and conceptual recombination, capable of generating distinct pathways through which violent ideas, identities, and aesthetics are normalised.

Mapping Southeast Asia’s Nihilistic Violent Extremist Online Subcultures: Inside the True Crime Community

Saddiq Basha (S. Rajaratnam School of International Studies): [LinkedIn](#)

In recent years, scholarship on nihilistic violent extremism (NVE) and its associated online subcultures has remained overwhelmingly Western in focus. This presentation extends that work to Southeast Asia, a region long framed as the ‘second front’ in the Global War on Terror against Islamist militancy, but whose threat landscape is now quietly diversifying.

It takes as its point of departure the November 2025 SMAN 72 bombing in Jakarta—after which Densus 88 reported dozens of online-radicalised adolescents—and a parallel wave of intercepted minors in the Philippines, where police have formally invoked NVE. Drawing on open-source analysis of Southeast Asian TCC milieus across TikTok, Telegram, and gaming platforms, it examines their narratives and aesthetics, their platform-level activity, and their porous intersections with other extremist communities. It further traces how these communities track and amplify domestic incidents, situating Southeast Asia within the transnational flows of NVE discourse not as a passive recipient but as an active site of localisation.

Polarization and Euphoria: Disinformation and Hate Speech in Electoral Contexts in South Asia

Janeen Fernando (United Nations Nepal): [LinkedIn](#); [BlueSky](#)

The presentation examines broad trends in social media misinformation and hate speech, looking at data in South Asia (primarily Sri Lanka) with a focus on electoral contexts to inquire as to why under some conditions, despite signs of continued online political polarization and misinformation, countries see an apparent decline in hate speech, as well as the role of ‘euphoria’ in political change moments in displacing hate

speech narratives and its impact on the popularity and circulation of violent extremist narratives.

The Growth of Post-Ideological Threats in Aotearoa/New Zealand

Che Tibby (New Zealand Police): [LinkedIn](#)

As Western democracies grapple with militant accelerationism and the growth of extremist communities gamifying nihilistic, misogynistic, and misanthropic extremist material online, New Zealand Police are posing the question, “How is violent extremism moving post-ideology?” This study unpacks the extremism motivating or informing a cohort of persons of interest categorised by our system as of “Mixed, Uncertain, or Unclear” ideology, and discovers that idiosyncratic, non-ideological stochastic influence over these individuals is high, and that clear patterns in behaviour are present.

Day Three: Morning Workshops

Workshop A: AI for Counter-Extremism

Hosted by [Hedayah](#)

The rapid evolution of AI, especially generative models, presents both emerging threats and exciting opportunities in the field of countering extremism and violent extremism. Malicious actors are experimenting with ways that AI can be used as a tool to support their tactics and amplify their narratives. Similarly, AI holds potential to be leveraged as a tool to counter the threat posed by extremists by enhancing content analysis and moderation, early analysis, strategic communication, among other uses. This session will build on Hedayah's recently published research brief - [Artificial Intelligence for Counter Extremism](#) - that offers an evidence-based assessment of AI risks, opportunities, and other policy considerations for the field of countering extremism and violent extremism. It will delve into the applications of AI for counter extremism in key emerging use cases, with presentations on these issue areas or case studies at the beginning of the workshop followed by teamwork to develop out a proposed use of generative AI for counter extremism, based on the teams' own needs as researchers and practitioners or needs that the team have identified, with facilitated ideation, concept development, and risk assessment.

Workshop B: Tackling Terrorism and Online Threats – Achievements in Law Enforcement Agency and Innovator Cooperation

Hosted by [NOTIONES](#)

The NOTIONES project – *Interacting Network of Intelligence and Security Practitioners with Industry and Academia Actors* - is funded by the European Commission (2021–2026; Horizon 2020 Coordination and Support Action). Its mission is to build a network of practitioners from security and intelligence services of EU Member States and associated countries. This network now supports the needs of security and intelligence services and equips them to participate in research and innovation actions. The project has brought together practitioners from military, civil, financial, judiciary, local, national and international police authorities, and retains a focus and active interest in the intersection of terrorism, technology, and social media.

The NOTIONES project draws together innovative research, case studies, and technical demonstrations. The event shares best practices in making security and intelligence practitioners work together with academia and industry. Rapid technological change and advances in applying the technologies to the everyday work of security practitioners are broken down into shareable knowledge for the benefit of maintaining secure, adaptive, and resilient societies. This workshop offers research and practitioner knowledge from the NOTIONES network, other EU projects in the field, and invites participants to share recent findings and new insights.

Day Three: Afternoon Workshops

Workshop C: Elevating AI Safety: From Content Moderation to Benchmark Development

Hosted by the [Christchurch Call Foundation](#)

The Christchurch Call Foundation (CCF) will lead an interactive half-day workshop exploring the intersection of artificial intelligence and terrorism and violent extremism (TVE) prevention. This session will focus on two critical challenges: developing effective TVEC policies for open-source AI safety reasoning models and creating AI safety benchmarks to measure risks like grievance amplification and radicalization to violence in AI chatbot interactions. Participants will work directly with tools currently under development through CCF's Elevate project, providing valuable feedback that will be used to update and improve these tools over time.

The workshop will be structured in two segments, each featuring small group exercises. In the first segment, participants will test TVEC policies using open-source models in a sandbox environment, evaluating how AI interprets and applies content moderation policies. The second segment will focus on CCF's effort to create an AI safety benchmark related to grievance amplification and radicalization to violence. Participants will review evaluation criteria, assess test scenarios, and annotate sample outputs from our minimum viable version of the benchmark. By the end of the session, participants will have contributed directly to shaping tools for responsible AI use in preventing the spread of terrorist and violent extremist content while gaining practical insights into emerging AI safety challenges.

Workshop D: Make the Call Now: Decisions and Consequences in a Live Terrorism Crisis

Hosted by the [VOX-Pol Institute](#) and [Extremisphere](#)

This interactive tabletop simulation invites participants to step into the role of founding policy team members in a fictional social media start-up. Tasked with developing a response framework for terrorist content and live incidents online, they must define core principles, escalation thresholds, information-sharing protocols, and coordination mechanisms from the ground up.

The scenario then pivots. Participants move into sector-based roles representing tech Trust & Safety, regulators, law enforcement agencies, civil society, and academia. They are immersed in a rapidly evolving crisis that immediately stress-tests the framework they have designed. As events escalate and information remains incomplete, curveballs and unintended consequences force teams to negotiate across mandates, manage uncertainty, and make time-sensitive decisions under pressure.

Fast-paced and experiential, the exercise reveals how institutional incentives, sectoral tensions, and governance trade-offs shape real-time crisis response. Participants leave with practical insights into cross-sector coordination, accountability, and the complexities of responding to terrorism-related content in a live digital environment.