TERRORISM AND SOCIAL MEDIA

INTERNATIONAL CONFERENCE

Swansea University
Prifysgol Abertawe

CYTREC
CYBER THREATS RESEARCH CENTRE

BREAKOUT SESSION ABSTRACTS

BREAKOUT SESSION 1 ABSTRACTS

Panel 1A: Extremism and the Covid pandemic

Chair:

Propaganda weaponization within the Italian context

- Federico Borgonovo (Catholic University of the Sacred Heart of Milan)
- Luca Cinciripini (Catholic University of the Sacred Heart of Milan)
- Marco Zaliani (Catholic University of the Sacred Heart of Milan)

The COVID-19 pandemic has allowed various extremist entities to exploit the multiple facets of the health emergency for propaganda purposes. This analysis outlines a mapping of right-wing extremism and no-vax groups based on their communication strategies within the Italian context. This is carried out by combining digital ethnography, social media analysis and open-source data collection on Telegram and Gab. The existing literature on the subject has not yet provided an in-depth study on the use of propaganda during the pandemic in Italy. This study focuses on the recognition of narratives, communication objectives and recruitment methods, which are essential for an effective counterstrategy. Within the Italian context, the strategic use of the pandemic was observed; especially by two categories of actors, namely the right-wing extremism and the no-vax movement. From the mapping of the propaganda tools, it emerges that no-vax protest groups and far-right organizations exploited pandemic-related propaganda as means of transmitting their ideological message. This was carried out to expand their pool of followers and organize demonstrations. Through a mapping of the actors, national institutions would acquire knowledge with regards to the communication processes and subsequently intervene both on a digital and kinetic level.

The Far-Right, Conspiratorial Thinking, and the Pandemic: A quantitative and qualitative analysis of Australian social media

- Lise Waldek (Macquarie University)
- Dr Julian Droogan (Macquarie University)
- Dr Brian Ballsun-Stanton (Macquarie University)

This paper presents the results of an Australian government funded project exploring the intersection between the far-right online, the Covid-19 pandemic, and Australian public sentiment through 2020-21.

The project incorporated quantitative and qualitative data to create a comprehensive picture of how the far-right appropriate the pandemic and associated public health measures to spread their narrative, and to determine in a statistically significant manner the extent to which far-right and conspiratorial discourse was adopted on Australian-aligned social media accounts. Qualitative analysis of the Telegram and Instagram pages of far-right groups and individuals showed high diversity in how the pandemic was appropriated, with some emerging leaders and wellness entrepreneurs adopting strong conspiratorial and militant narratives while harnessing public anxiety and anti-government sentiment. Quantitative analysis involved the collection of big-data from Australian representative YouTube channel comments and a random 1% sample of Australian Twitter content over a two-year period between January 2019 – January 2021. Statistical analysis demonstrated that far-right terminology increased in a significant way and there was a pronounced growth in conspiratorial and QAnon terminology that aligned with domestic and international events. Together, these trends illustrate the growth of an online conspiratorial and far-right aligned 'creeping threat' to Australian political discourse. The crisis created by the pandemic has provided the far right with opportunities to capitalise on this growth of anti-democratic sentiment and, to a lesser degree, advocate of revolutionary and militant solutions.

Preventing and Countering Violent Extremism During the Pandemic and Onwards: Responses and Intervention Strategies to Ideologically Motivated Violent Extremism Movements Online

- Dr John McCoy (Organization for the Prevention of Violence)
- Bradley Galloway (Organization for the Prevention for Violence)

In recent years, and particularly over the course of the recent Covid 19 pandemic, contemporary in- person mentoring and counselling strategies in P/CVE have largely been moved to the online context. Intervention work has shifted to online means often through video conferencing platforms, encrypted apps, social media, and online telehealth providers. Various non-governmental organizations have operated regionally, internationally and transnationally to service various client bases to prevent, intervene and assist in the multifaceted response to IMVE. Additionally, this study looks at the limited evaluation work and the challenges that these programs face, particularly to those practitioners and former extremists who are on the front lines working in this space.

Panel 1B: Online interactions

A Corpus Linguistic Analysis of the Language Associated with Different Forms of Extremism on Twitter

- Hollie Sutch (Birmingham City University)
- [Non-presenting co-author: Dr Pelham Carter (Birmingham City University)]
- [Non-presenting co-author: Prof Imran Awan (Birmingham City University)]

With the rise in extremism and endless shifts in the landscape of extremism online the need to establish the linguistic features of different forms of extremism online is imperative (Sutch & Carter, 2019). The current research adopts a quantitative design to investigate the language associated with different types of online extremism as well as exploring how factors including anonymity, membership length, postage frequency and follower count play a fundamental role in the levels of different types of extremism online. A series of corpus linguistic analyses will be conducted to measure how anonymity, membership length, postage frequency and follower count is associated with language that is evident within far-right, anti-abortion, anti-LGBTQ and animal rights extremism. AntConc will be used to develop wordlists which represent the linguistic features of each type of extremism. Keyness tests will be performed to demonstrate the significant associations for each word list and its relationship with anonymity, membership length, postage frequency and follower count. This aims to demonstrate whether anonymity, membership length, postage frequency and follower count are indicative of the levels of extremism online. Understanding how extremists and their content differs can help to isolate the appropriate solutions to reduce the levels of extremism online.

Eco-fascism online: Conceptualising extreme right actors' response to climate change on cross-national social media

- Dr Imogen Richards (Deakin University)

Often referred to as 'eco-fascist' are extreme population control measures advocated by right-wing activists and ethnonationalist governments, and the accelerationist propaganda of violent actors hastening the social and economic collapse of societies worldwide. Far from representing an isolated phenomenon, these expressions of eco-fascism emerge from political-ideological environments in which media and political actors in the Global North have placed blame for climate change on the Global South through rhetoric about population control and fossil fuel usage. In response, this paper presents insights from a mixed-methods analysis of media platforms exploited by extreme right actors, such as Stormfront, Gab, and Discord. Combined with a review of grey and scholarly conceptual literature on eco-fascism, the investigation maps the key ecological-environmental priorities of extreme right actors communicated online, including as they relate to Australia-based groups. An initial scoping exercise revealed that key thematic areas of interest in online extreme right discourse include: debates about economic growth imperatives versus environmental priorities; eugenicist or Malthusian population control measures; political treatment of regular or irregular migrants as a 'foreign species' or 'pollutant'; and expressions of denialism, resignation or accelerationism in response to the gravest impacts of ecological-environmental devastation, with reference to Global South countries in particular.

Erstwhile Allies and Community Convergence: A Study of Online Interactions Between Salafi-Jihadists and White Supremacists

- Dr Brian Hughes (American University)
- Meili Criezis (American University)

Previous research has explored interactions and overlaps between Salafi-jihadists and white supremacist movements including individuals who ideology switch, white supremacist praise for Salafi-jihadist groups, and thematic narrative overlaps. Drawing and expanding on these topics, we examine direct interactions in decentralized online spaces where proponents of these respective ideologies interact with one another in group chats and Salafi-jihadist channels incorporate white supremacist themes in their propaganda messaging. The study is contextualized within wider communications and terrorism studies scholarship. It seeks to contribute towards better understanding the roles and effects of user-generated contents well as platform affordances, how decentralized online communities allow for varying degrees of ideological exchanges across porous borders, and various propagandizing strategies that focus on drawing from extremist aesthetics across ideologies.

Hate speech predicts engagement on social media: A case study from Turkey

- Dr Kamil Yilmaz (Swansea University)

What drives engagement on social media has been the focus of scientific inquiry especially in recent years. Among various established predictors of virality on social media are emotional language, language about in- and out-groups, notions of positivity and negativity, and so on. In light of the prior work, this study explores whether hate speech in the form of demonization of a social group is associated with engagement on social media by using a case study from Turkey: The Gülen Movement (GM), a once-admired social movement that has been going through a decade-long demonization, stigmatization, criminalization and persecution, a process culminating in the group being designated as a terrorist organization. The results show that demonizing language against GM (a specific out-group) is a strong predictor of virality in three of the largest social media platforms in Turkey's social media ecosystem: Facebook, Instagram and Twitter. The results also show that demonizing language about a specific out-group has the largest effect size compared to other well-established predictors of virality such as the moral-emotional language, language about the in-group and language about the (general) out-group.

Panel 1C: Actors and identities

Chair: Ninian Frenguelli (Swansea University)

Nothing in Common? Analysing Identity Formation in the Far Right & Jihadi Extremist Rhetoric

- Dr Weeda Mehran (University of Exeter)
- Dr Stephen Herron (Queen's University Belfast)
- Dr Ben Miller (Emory University)

Promoting political action, forging affiliations and propagating hatred and misinformation online is rather a common phenomenon amongst far right and jihadi extremists. While there is an extensive body of literature on the online rhetoric campaigns of jihadi extremist groups and the online ecosystem of the far-right, less is known about what sets the discourse of these extremist groups apart. What are the emotional, cognitive, psychological and social dimensions of the textual discourse in the online ecosystem of far right and jihadi extremists? What function do these dimensions play in the construction of group identity? In this paper, we conduct a semiotic comparative analysis of online text material by eight selected far-right groups (American Renaissance, Britain First, Daily Stormer, Front Page Magazine, Heritage and Destiny, Knights Templar International, Rebel Media) and jihadi extremists such as ISIS, Al Qaeda, the Taliban and Tahrik-e Taliban Pakistan. Our data corpus consists of more than 3,000,000 words. We adopt a mixed method approach of qualitative and quantitative analysis (Natural Language Processing) in analysing the data. We highlight similarities and differences between the far-right and jihadi extremist narratives particularly in association with construction of group identity through cognitive processes, psychological processes, temporal outlook and personal concerns.

The Glorification of Extremists on Social Media

- Emily Thompson (Simon Wiesenthal Center)
- [Non-presenting co-author: Rick Eaton (Simon Wiesenthal Center)]

The advent of social media platforms has provided numerous and innovative ways for extremists and terrorists to spread hateful propaganda to new audiences around the globe. In decades past, notorious individuals such as David Lane and Robert Jay Mathews (The Order) and Ian Stuart Donaldson (Blood and Honour) were heralded in close-knit circles for their actions in advancing the agenda of white supremacy in violent and deadly ways. Since platforms such as Telegram have become the new digital meeting place, the glorification of extremists has exploded to unprecedented levels. Individuals such as Brenton Tarrant, Dylann Roof and Robert Bowers have been heralded as "saints" – martyrs for white supremacy who "did something" rather than simply being keyboard warriors. Glorification in the form of artwork, videos and channels lionizing their actions is prevalent on Telegram, and has even seeped out into mainstream platforms such as TikTok. This paper explores how individuals responsible for hate crimes motivated by extremist ideologies are celebrated, used as role models for recruitment to the white supremacist cause, and the copycat effect this has had in subsequent attacks where these so-called "saints" are referenced as points of inspiration for new attacks.

Emotion as deeply felt, the experiences of current and 'former' far-right extremists

- Tomas Cartmill (University of Melbourne)

Historically curtailed by limited data, terrorism research is now enriched with the quantitative possibilities yielded by social media metadata. Quantitative analysis is an attractive tool for analysing radical online commentary and social networking, however it is limited in assessing extremists' and their sympathisers' emotion. The extremist experience is one of emotional motivation and inspiration. This paper argues that quantitative 'top-down' approaches, such as sentiment analysis of digital utterances, cannot help but be blind to extremists' private thoughts, feelings and urges to act over time. This paper reports on the qualitative emotional experience of current and 'former' cis and transgender 'far-right' extremists recruited from Twitter, reddit and gab. Participants ranged in ideological intention from 'sympathiser' to 'personal moral obligation', and from 'activist' to 'terrorist' in online and offline behaviour.

Interviews were conducted by a clinical psychologist, and analysed in accordance with interpretative phenomenological philosophy. Emotional experience propelled radicalisation through; an unstable sense of self, over-identification with masculinity, trust and empathy, joy and anger. In contrast, emotional experience motivated deradicalization through; openness, fear, feelings regarding feminism, shame and guilt. That which is actually driving extremist expression reveals itself only to qualitative analysis. What is thought and felt is hidden from the quantitative.

Panel 1D: Curating Extremism: Workshop on Housing, Organising, and Researching Primary Documents

- Dr Amarnath Amarasingam (Queen's University)
- Marc-André Argentino (International Centre for the Study of Radicalisation)
- Dr Aaron Y. Zelin (Brandeis University)
- Sarah Pollack (Interim Chief of Staff, GIFCT)

This workshop will seek to highlight the challenges of collecting primary sources of ideologically motivated violent extremist (IMVE) data. The presenters are working on projects that seek to curate repositories of extremist and terrorist primary sources, which seeks to provide a secure and controlled means for researchers and experts to access these primary sources, that have been collected and curated with academic rigor.

Those who research or monitor violent extremists and terrorists are presented with an important duty of care when analysing or reporting these materials. The sensitivity of researching IMVE actors and content can potentially harm those who visit extremist digital ecosystems. This can be via exposure to upsetting and traumatic content or potential threats to a researcher's safety. By having a curated archive of primary sources, these repositories help reduce these risks for their users.

In creating these repositories and curating primary extremist and terrorist documents we have all faced many methodological, technical, ethical, and legal considerations that need to be made, as well as gleaned important insights into how threat actors use primary materials that cannot be overlooked by researchers and practitioners. This workshop will provide a deep dive into repositories, but also seek to mine insights from the terrorism studies community about how they might use these repositories, and the kinds of measures they would like to see put in place so that they can benefit researchers.

BREAKOUT SESSIONS 2 ABSTRACTS

Panel 2A: Mapping extremism

Chair: Dr Alastair Reed (RESOLVE Network; Swansea University)

Using Python to map extremist websites: Ethical and methodological issues

- Ninian Frenguelli (Swansea University)

This presentation will discuss the ethics and methods involved in web crawling extremism websites. This works comes from a PhD project that aims to map right wing extremist websites that exist on the surface web and will discuss how hyperlink network analysis can be used as a form of social network analysis in the online space. Websites link to each other for a number of reasons: they may have an "Our Supports" page on their website, they may use hyperlinks in blog posts as evidence, they frequently link to places where merchandise can be purchased. Mapping of this nature allows us to see where clusters form, such as neo-Nazi websites being closely linked to each other, libertarians linking to similar groups, etc. It also allows us to see which websites in the network act as bridges between these clusters, which websites appear across many, as well as which websites and clusters are ostracised from the rest.

This presentation will discuss what can be gained from a research method of this nature, as well as the ethical issues that go along with it.

The Con.Cel project: Exploring the online spread of Incel ideology

- Dr Lewys Brace (University of Exeter)
- Dr Debbie Ging (Dublin City University)
- Dr Stephane Baele (University of Exeter)

The work presented here will be drawn from the Con.Cel project, which focuses on the InCel (short for "involuntary celibate") ideology, a misogynistic worldview whose proponents blame women for their lack of sexual activity, and the "Incelosphere", a loose conglomerate of online InCel communities spread across various digital platforms. Specifically, it will present the results of an ongoing effort to use both interpretive examination of textual content and advanced computational methods to both map out the Incelosphere and to track its dynamics of contagion along four key axes:

1. Extremist contagion: The dynamics through which the most extreme ideas gain (or lose) traction within the InCel subculture.
2. Online contagion: To determine how the InCel ideology spreads across different digital platforms, such as Reddit, 4chan, YouTube, and dedicated InCel forums.
3. Ideological contagion: The pathways by which InCel subcultural practices have contributed to - but also drawn from - other extremist ideologies to create a "cross-pollination" of ideas, chiefly with aspects of the online far-right.
4. Geographical contagion: Developing an understanding of the geographical contagion of the InCel movement, with the aim of evaluating its prominence in the UK and the Republic of Ireland.

Under the magnifying glass: The impact of the U.S. Capitol attack on online far-right communication on Telegram

- Dr Aaron Rudkin (Trinity College Dublin)
- [Non-presenting co-author: Dr Constantine Boussalis (Trinity College Dublin)]
- [Non-presenting co-author: Callum Craig (Trinity College Dublin)]

This study investigates online discursive processes among far-right groups following the January 6th, 2021 attack on the U.S. Capitol. The 1/6 insurrection has emerged as a focal point of the American far-right. By virtue of being an unmoderated space, and surviving provider takedowns which disrupted activity on Parler, another major far-right social media outlet, Telegram provides the most complete before-and-after picture of online activity among the far-right. In the wake of 1/6, far-right Telegram groups experienced huge increases in viewership. While scholarship has begun to focus on far-right activity on Telegram, current research remains mainly descriptive (Urman & Katz, 2020; Walther & McCoy, 2021; Bovet & Grindrod, 2020). Our study seeks to investigate to what extent the insurrection has affected online far-right communication. Using a snowball ampling approach, we gather an exhaustive view of the U.S. far-right Telegram ecosystem, comprising 4+ million messages and we subsequently analyze the activity of the most central, active groups. Treating the events of January 6th as an exogenous shock, we employ an interrupted time series design to analyze outcomes including toxicity, topic focus, level of activity, and citation of other far-right groups.

A Comparative Analysis of Misinformation and Disinformation posted on Twitter during the 2016 and 2020 U.S. Presidential Elections

- Karmvir Padda (University of Waterloo)

This study examines misinformation and disinformation posted by hostile foreign actors on Twitter in connection with the 2016 U.S. presidential election and the 2020 U.S presidential election. The paper offers an empirical understanding of these events, and also reports on the divisive language that promoted a pro-Republican (and in particular a pro-Trump) agenda. Qualitative content analysis of the sampled Twitter tweets found that the majority of the "false discourse" tweets discussed immigration, 2nd amendment rights, the LGBTQ+ community, and pro-life, many of them in alignment with Donald Trump's main narratives.

Panel 2C: Looking beyond social media

Chair: Dr Sara Correia (Swansea University)

Back to the Future? Twenty First Century Extremist and Terrorist Websites

- Seán Looney (University of Exeter)
- [Non-presenting co-author: Prof Maura Conway (Dublin City University; Swansea University)]

Extremist and terrorist websites never really went away, they were just overlooked by researchers and others in the 2010s due to a not unwarranted narrowing of focus to social media platforms and, latterly, messaging applications and adjacent online spaces. This paper argues that while there is less reliance on websites by extremists and terrorists than there once was, websites remain an important component of contemporary online extremist and terrorist ecosystem(s) and could re-emerge more strongly with accelerated disruption of extremist and terrorist content and accounts by social media platforms and adjacent services unless providers further down 'the tech stack' take more concerted action. With this in mind, the paper opens by locating extremist and terrorist websites within an ecosystem framework. It follows-up by grappling with the question of what constitutes a 'terrorist website' and lays out a three-part categorisation that accounts for terrorist-operated websites, supporter sites, and ideologically adjacent sites. The content, purpose, and reach of eight ideologically diverse websites are analysed within this framework as well as the refusal of hosting or other crucial services, such as DDos protection, by website providers, which has led to the disappearance—sometimes for a short period, sometimes more permanently—of some extremist and terrorist sites from the Web.

After Christchurch: Mapping the Australian far-right across online platforms

- Dr Brian Ballsun-Stanton (Macquarie University)
- Lise Waldek (Macquarie University)
- Dr Julian Droogan (Macquarie University)

This paper presents findings from a government funded research project 'Mapping Networks and Narratives of Online Right-Wing Extremists in New South Wales'. The analysis drew on a large-scale multi-platform dataset from Facebook, Twitter, Gab (pre and post mastodon), Reddit, 4Chan, and 8Chan to generated evidence-based insights into the online right-wing extremist milieu in NSW following the 2019 Christchurch terrorist attack. We identified two distinct but connected threats posed by these online communities; 1. A creeping threat to democracy fueled by influencers, networks, and content that challenges the principles of pluralistic liberal democracy; 2. A risk of violence perpetrated by individuals and groups that advocate the use of violence as a tactic to achieve an ideological end. These online communities were characterized by networks of individuals as opposed to formal groups. Despite being hateful and extreme, these right-wing extremist milieus were spaces of sociability where social networks were maintained through shared values and norms centered on the delegitimization of government and the dehumanization of others. The incorporation of multiple platforms generated comparative analysis across the digital environment resulting in the observation and identification of five distinct stages of moderation and echo-chamber strength. These have ramifications for policy communities regarding proscription and moderation.

Panel 2B: U.S. elections and the far-right

The interaction between the producer and the consumer: the alt-right on Reddit and YouTube during the US Presidential Election 2020

- Antonia Vaughan (University of Bath)

Reactionary and far right creators have established a strong presence on YouTube, becoming political influencers and disseminating their ideas to a wide audience. YouTube has been demonstrated to be a pipeline of extremism, funnelling viewers towards the far right through a combination of algorithms, platforms norms, and presenter practices. A number of these YouTubers have unaffiliated fan communities on Reddit where users congregate to discuss and disseminate content. However, research on the far right on YouTube tends to focus predominantly on the presenters themselves or YouTube comments in isolation.

Focusing on Tim Pool and his fan community on Reddit, this paper offers an understanding of the discursive interaction between a far-right content creator and their receptive audience. Through a mixed methods approach of inter- and intra-platform discourse analysis in conjunction with SNA, this paper will elaborate on the discursive negotiation of identity, and ideas such as democracy, during the US 2020 Presidential Election and attempted insurrection. With Pool deemed a 'superspreader' of election misinformation (EIP 2021) and a 'sanitised conduit to the far right' (Silverman 2021) it is critical to understand how discourse evolves and is received by the users most aligned with him.

Digging in the Dark: Exploring the Digital Jihadist Underground on The Onion Router (TOR)

- Miron Lakomy (University of Silesia)

This paper, founded on open-source intelligence techniques, aims to fill a gap in research on exploiting the dark web by Salafi-jihadist violent extremist organizations (VEOs). It maps all existing and accessible digital jihadist hotspots accessible on The Onion Router (TOR). It also discusses the scope of Salafi-jihadist VEOs' propaganda on this layer of Internet communication. Finally, this paper explores other aspects of exploitation of TOR by these groups and their followers, including, for instance, their attempts of networking or facilitating terrorist attacks. This discussion is provided in the broader context of CVE strategies that can be used to curb these activities.

This paper argues that in contrast to many studies claiming that digital jihad is moving to the dark web, the true scale of Salafi-jihadist propaganda in the TOR is surprisingly small and related mostly to activities of the Islamic State, al-Qaeda and Chechen extremists. However, the .onion pseudo domain has been utilized by VEOs to illegally acquire arms and explosives. It is also permeated with professional manuals related to, for instance, cyber-security and privacy on the Internet (Kybernetiq). Last but not least, it serves as a platform enabling terrorist activities to be funded.

Quis Custodiet Ipsos Custodes? Content Takedowns and the Censorship of Academic Research

- Dr Aaron Y. Zelin (Brandeis University)

Over the past two years there has been greater evidence that there are broader consequences for researchers examining, archiving, and collecting extremist materials online. When social media companies began taking down extremist content -- most notably with the Islamic State first -- it mainly focused on particular users within a network that were promoting extremist materials and ideas online. Yet with advancements in algorithms and artificial intelligence these tools have become far more blunt and less discriminant in who is being banned from particular platforms. As a consequence, a number of researchers were banned from Telegram in 2019, while a steady stream of researchers have on and off been taken down from WhatsApp, among other platforms in the past two years. Any redress is an ad-hoc process that does not follow any particular protocols and when researchers have been allowed back on such platforms, many of the extremist groups they had previously been following remained online, illustrating gaps and issues with the algorithmic system in of itself. Beyond stifling academic research, this growing trend inhibits any accountability on the part of these technology platforms, which has longer-term implications for those conducting primary source research online.

Panel 2D: Video-Gaming & Violent Extremism: An Exploration of the Current Landscape, Trends, and Threats

Chair: Claudia Wallner (Royal United Services Institute)

- Galen Englund (Love Frankie)
- Dr Ashton Kingdon (University of Southampton)
- Jacob Davey (Institute for Strategic Dialogue)
- Katie Passey (Moonshot)

Video-gaming is considered to be one of the most consistent and fastest growing sectors, with online gaming, as part of this, representing one of the biggest industries globally. This growth is not only attributed to the development of online games and communities, but also to the game hosting and adjacent communications platforms that have been specifically designed for gamers and gaming, including Steam, Twitch, Discord, and DLive. However, a growing concern within policy, security, and counter-terrorism circles is the increasing intersection between video gaming and (violent) extremism. This panel will explore this intersection, examining the current landscape, trends, and threats.

The panel will be hosted by members of the Extremism and Gaming Research Network (EGRN).

BREAKOUT SESSIONS 3 ABSTRACTS

Panel 3A: Terrorist use of emerging technologies

Chair: Seán Looney (University of Exeter)

The Role of Financial Technologies in US-based ISIS Terror Plots

- Dr Joe Whittaker (Swansea University)

This study explores how terrorists use financial technologies in their plots. Using a database of 231 US-based Islamic State actors, it analyses how they move money and make purchases, as well as whether the use of technology affects success. Fundamentally, terrorists opt for simplicity; there is little evidence sophisticated financial technologies are being exploited. Terrorists tend to use the Internet in two ways: to make purchases and to coordinate transactions. Transactions via Money Service Businesses are more likely to be part of successful plots. Finally, the paper discusses factors which explain this simplicity as well as discussing whether this may change moving forward.

Two Sides of the Same Coin? Comparing Crowdfunding, Cryptocurrency, and Blockchain Use by Extreme Right and Jihadi Groups

- Shahed Warreth (Swansea University)

Previous academic research and policy work has focused predominantly on terrorist, i.e. jihadi, financing, while extreme right financing has predominately received the attention of journalists and media outlets. While there exists some research on extreme right and jihadi groups' use of crowdfunding, cryptocurrencies, and blockchain, no published research has compared both ideologies in this respect. My research found that extreme right groups are far more successful than jihadi groups in their use of these methods and technologies due to three factors: the accessibility and proliferation of online crowdfunding platforms, and integration of cryptocurrencies and blockchain; the impact of geographical location and legislative constraints on accessibility; and the influence of ideology. Nevertheless, there are many aspects that require further research. In particular, further research is required regarding the legislative constraints in the US, EU, and especially non-Western countries; the impact of digital colonialism on non-Western countries, and how this impacts groups' use of cryptocurrencies and blockchain; as well as ideological constraints, particularly with regards to Islamic law. This research will focus on all of the aforementioned areas. This will allow both researchers and practitioners to better understand extremists and terrorists' use and misuse of these methods, thereby identifying not just further avenues for academic research, but additional policy-relevant considerations, too.

Learning from Foes: How Terrorists Embrace and Mimic Emerging Technologies

- Dr Yannick Veilleux-Lepage (Leiden University)
- [Non-presenting co-author: Chelsea Daymon (American University)]

While the existence of alliances amongst terrorist groups is well established in existing literature and supplemented with rich empirical accounts of collaboration and information exchange between terrorist groups, how terrorists learn from and mimic their adversaries' (whether state or non-state) uses of emerging technologies have remained woefully under examined. Building on existing terrorist innovation and, more broadly, communication literature, this paper examines not only how and why terrorist groups embrace emerging technologies, but also how the malevolent use of emerging technologies can spread from one group to another and thus dramatically change the security landscape. By focusing on three case studies: the use of (1) cloud-based instant messaging services; (2) social media bots and Artificial Intelligence base text generators, and lastly (3) unmanned aerial vehicles, this paper lays out a theoretical framework addressing why terrorist groups, in their quest to gain competitive advantages, tend to mimic their adversaries' practices. Understanding how groups learn for one another may offer roadmaps on potential trends in terrorist innovation and tactics, while offering insight into the organic nature of online learning.

The making of far-right platforms – Alt-Tech affordances and their impact on online community-building

- Greta Jasser (University of Hildesheim; Leuphana University)
- Paula Matlach (Institute for Strategic Dialogue Germany)
- Ed Pertwee (London School of Hygiene and Tropical Medicine)
- [Non-presenting co-author: Jordan McSwiney (University of Sydney)]

With large social media platforms coming under increased pressure to deplatform far-right users, the Alternative Technology movement (Alt-Tech) emerged as a new digital support infrastructure for the far right. Though these platforms began as little more than poorly functioning mirrors of their mainstream competitors, they have grown into their own, providing a unique set of affordances with a specific, political user base in mind. In this paper, we examine two of the most successful Alt-Tech platforms: Gab, a microblogging platform, that was used by the perpetrator of the Pittsburgh Synagogue terrorist attack to post his last messages before the attack; and Odysee, a blockchain based video sharing platform, harbouring a wealth of anti-Semitic and other extremist content. We argue that both platforms represent technological as well as movement innovations, enabling content propagation with close to zero moderation. They rely on either their own servers or decentralization to shield themselves from consequences of these moderation-policies. In this paper, we conduct a qualitative analysis of the technological affordances of Gab and Odysee, comparing the market and ideology-driven features of the platforms. We argue that these technological features, and the kinds of communicative interactions they encourage and enable, have a direct impact on the specific far-right communities forming on these platforms.

Panel 3B: Understanding extremist groups and responses

Jihadi Competition, Contestation, and Cooperation: An Analysis of ISIS, Al Qaeda, and the Taliban

- Dr Weeda Mehran (University of Exeter)

This research explores how jihadi organisations depict each other. The study is based on analysing 82 English magazines published by the Taliban, ISIS, Al-Qaeda and Tahrik-e Taliban Pakistan (TTP). The research takes a mixed method of analysing data both qualitatively and quantitatively. The findings point to statistically significant differences amongst these groups in whether the groups endorse, undermine, compete with and contest each other. For example, ISIS is more likely than Al-Qaeda, the Taliban or TTP to undermine and question the legitimacy of other groups. Al Qaeda and the Taliban, on the other hand, demonstrate a positive narrative when referring to each other. The Taliban & Al Qaeda appear to have cemented their alliance in seeking to prevent ISIS and TTP from hijacking jihadist fronts.

What's in a Name? Social Media, Reputation, and Transnational Affiliation with Al-Qaeda and the Islamic State

- Caroline M. Brandt (Uppsala University)

Jihadist terror organizations have undergone a profound restructuring in the 21st century. Al- Qaeda (AQ) and the Islamic State (ISIS) have adopted a transnational organizational structure, incorporating terror groups across the globe into their fold. Scholars have theorized that AQ and ISIS do so to burnish their global reputations. Attacks by affiliate groups provide the central organization a veneer of momentum and omnipresence. Limited work has examined how joining a transnational organization affects a terror group's reputation. I argue that pledging allegiance to a transnational organization gives terror groups a strategic advantage, enhancing both their reputation and their reach. To test this theory, I examine social media coverage of six terror groups before and after the group became a transnational affiliate. I find that Western social media gives terror groups more exposure and describes the group with more severe language, even when accounting for the number and severity of the group's terror attacks.

What to Say in Response? An Analysis of State Countermessaging against Terrorist Organizations

- Dr Daniel Milton (Combating Terrorism Center, United States Military Academy)

How do states approach countermessaging against terrorist organizations on social media platforms? Despite the increase in scholarly attention to the messaging of terrorist organizations on social media, comparatively less focus has been paid to the nature of state countermessaging campaigns, leaving a gap in the literature regarding how states approach the "war of ideas" against terrorists. This paper addresses this shortcoming by conducting a content analysis of three prominent state-level messaging campaigns on Twitter using data collected from each respective campaigns' content feeds in English and Arabic. The content analysis will identify key messaging themes utilized by states, compare them with key messaging themes employed by terrorist organizations as identified by previous research, and offer some insights into how state campaigns can better respond to the messaging of terrorist organizations in the future. Moreover, this paper endeavors to provide the foundation for more analysis of three state messaging campaigns in the future.

Panel 3C: A Comparative Analysis of Islamic State and Atomwaffen Division Activity on Telegram

Chair: Dr Alastair Reed (RESOLVE Network; Swansea University)

- Arthur Bradley (Tech Against Terrorism)
- Joost (Moonshot CVE)
- Connor Rees (Swansea University)
- Hirah Azhar (University of Southampton)
- Farangiz Atamuradova (Hedayah)
- Dr Kamil Yilmaz (Swansea University)
- Dr Ashley Mattheis (University of North Carolina at Chapel Hill)

This panel will present findings from a multi-stakeholder research project examining the activity of Islamic State (IS) and Atomwaffen Division (AWD) on Telegram. Drawing on a dataset of 13,798 posts, collected from a total of 27 public-facing channels, the panel will begin with a description of how data was collected and an overview of the dataset. This will compare the frequency of three content-sharing strategies (outlinking, inlinking and attachments), in order to understand how each group utilises this online space, and use outlink analysis to locate each group's use of Telegram in the context of the wider online ecosystem. This will be followed by a series of short presentations on the following topics:

- What are the strategic considerations that lead IS sympathisers to use particular file-sharing sites?
- The strategic ways IS supporters use hashtags on Telegram for outreach and to evade takedown
- Self-presenting as a legitimate news outlet in order to disseminate terrorist propaganda
- The contrasting discursive strategies used to maintain the appearance of a legitimate news outlet and construct in-group and out-group identities
- Atomwaffen Division and its affiliates on Telegram: variations, practices, and interconnections

Panel 3D: Online Extremist Ecosystems? A Critical Cross-Disciplinary Discussion

Chair: Jade Hutchinson (Macquarie University; Groningen University)

- Prof Noemie Bouhana (UCL)
- Prof Maura Conway (Dublin City University; Swansea University)
- Dr Stephane Baele (University of Exeter)
- Prof Stuart Macdonald (Swansea University)

Online extremism does not develop in siloed domains, but rather within dynamic networks of social media platforms and websites. The idea that violent extremists inhabit such an 'ecosystem' of interrelated online spaces has recently been popularized by both scholars and practitioners who sought to capitalise on the analytical potential of ecology to understand and govern otherwise perplexing natural and artificial environments.

Yet, despite its popularisation, there remain gaps in understanding the benefits and limits of using ecology and related concepts (such as evolution, biotopes, or ecological niches). In this panel session, we explore the analytical application of ecology in understanding ideological consolidation and fragmentation across social media platforms and how to govern violent extremism emerging from networked digital environments. The panel hopes to better understand what we can observe and understand with ecology that we cannot observe and better understand without.

BREAKOUT SESSIONS 4 (ABSTRACTS)

Panel 4A: Empirical and theoretical understandings of radicalisation

Where Propaganda and Madness Meet: The techno-capital origins and accelerationist intentions behind "Schizowave"

- Dr Brian Hughes (American University)
- Emmi Kuhn

Schizowave is a new genre of online media, characterized by stroboscopic video, electronic music, ironic, "shitpost"-style imagery and sloganeering, and far-right mysticism. Using a database of over 1000 examples, the authors identify key aesthetic and affective patterns in the schizowave genre. Its purpose appears threefold: 1.) to trigger acts of violence in vulnerable viewers 2.) to direct viewers toward currents of spirituality and politics associated with far-right occultism and accelerationist terror, and 3.) to serve as in-group identification for those already involved these practices.

Schizowave thus exhibits both an esoteric and exoteric dimension, an outer face and an inner core of meaning. This is reflected in its use of social media platforms. Large, public-facing platforms such as Instagram are used to spread more digestible content to the uninitiated. From here, vulnerable audiences may pursue deeper levels of engagement on more obscure platforms. Calls for violence are cloaked in layers of irony, and the process of persuasion begins with an invocation of extreme nihilism and misanthropy. Its preliminary appeals are not to explicit moral values or a social-political agenda, but rather in a more amorphous and affective appeal to desire—the desire to be unrestrained, unlimited, and (quite literally) unmedicated.

Digital Manifestos, Conspiracy Theories, and Offline Violence: A Framework of Investigation

- Dr Julian Droogan (Macquarie University)
- Jana Vanderwee (Macquarie University)

Conspiracy theories have been linked to attacks by violent extremists, creating a view that believing in one may be a motivating factor for violent extremism. The 2019 Christchurch attack, 2019 El Paso shooting, and 2019 Poway shooting were all cited in the popular press as referencing a white-genocide conspiracy theory known as the 'great replacement'. This paper examines whether any such link is supported conceptually and empirically. We compare Renaud Camus' great replacement conspiracy theory (They Will Not Replace Us) and the online, social media distributed manifestos of the three violent extremists linked to the theory (The Great Replacement, The Inconvenient Truth and An Open Letter). Three novel theoretical frameworks were selected to provide the basis for a comprehensive analysis: 1. conspiracy theory elements (agency, coalition, threat, secrecy), 2. radical narrative construction (crisis, solution, justification), and 3. mobilising emotions (anger, contempt, disgust - ANCODI). All four sources were found to contain the elements of a conspiracy theory presented as crisis narratives with significant in-group, out-group, and traitor-group construction. All four sources had mobilising anger, contempt, and disgust coded as the dominant emotions. These findings may contribute to the improved automated detection of online violent extremist material on social media platforms.

Exploring the Role of the Internet in Radicalisation and Offending of Convicted Extremists in England and Wales

- Dr Jonathan Kenyon (Her Majesty's Prison and Probation Service)
- [Non-presenting co-author: Dr Jens Binder (Nottingham Trent University)]
- [Non-presenting co-author: Dr Christopher Baker-Beall (Bournemouth University)]

This study sets out to explore the role of the Internet in radicalisation pathways and offending of individuals convicted of extremist offences in England and Wales. A comprehensive database of 269 convicted extremists was developed by reviewing and coding content of specialist assessment reports by professionals with access to a range of restricted information sources and direct contact with those concerned. Cases were grouped based on whether they primarily radicalised online, offline or subject to influence in both domains. Central areas of investigation include whether the Internet plays a prominent role in radicalisation for convicted extremists, if those taking various radicalisation pathways utilise the Internet in different ways, if offender demographics and offence-type variables differ when pathways are compared, and whether pathway taken impacts on assessed levels of engagement with an extremist group or cause, along with assessed levels of intent and capability to perpetrate violent extremist acts. Findings suggest the Internet is playing an increasingly prominent role in adicalisation, with changes in use over time, along with variations in online activities depending on pathway taken. General profile and vulnerability factors differed between pathway groups, along with assessed levels of engagement, intent and capability to commit violent extremist acts.

A New Politics of Terror: How Radicalization Became the Dominant Framework for Understanding Terrorism

- Dr Derek Silva (King's University College)

Since the tragic events of September 11, 2001, terrorism has become a central theme of concern for academics, government officials, and policymakers alike. For this study, I adopt a mixed-methods approach to what can broadly be defined as a comparative-historical project, to illuminate discourses reflected by texts/communications related to radicalization in order to understand how those ideas are constructed, negotiated, and configured in the public sphere. This project explores political, legal, scientific, and mass media communications (n=11,617) as well as publicly available tweets related to "radicalization" (n=~2.7M) to trace the discursive field related to the topic. I engage with theories of governmentality, literature within the othering paradigm traced back to the work of Edward Said, and John Mohr's notion of "discursive fields" as "dynamic terrains where meaning contests occur" and thus define the limits of a discussion on a particular topic, to explore the global diffusion of radicalization discourses online and throughout dominant institutions and illustrate how practices of governing terrorism through radicalization disproportionately impact certain individuals and groups preemptively identified as risky. In this way, I conceptualize radicalization as an emergent "pre-crime" space that, for many, requires various forms of governmental and nongovernmental intervention. The project offers insight into the social conditions which make radicalization preemption strategies more or less likely, and this study focuses on problematizing the taken-for-grantedness of radicalization discourses throughout Western Liberal democracies.

Panel 4B: Stakeholder responses

Introducing the Online Harms Observatory

- Dr Bertie Vidgen (The Alan Turing Institute)

The Online Harms Observatory is a new analytics platform from the Alan Turing Institute's Public Policy Programme. It combines large-scale data analysis and cutting-edge AI developed at The Turing to provide real-time insight into the scope, prevalence and dynamics of harmful content online. It aims to help policymakers, regulators, security services and civil society stakeholders better understand the landscape of online harms. Initially, it will focus on online hate, personal attacks, extremism and misinformation. The Observatory is supported by the Department for Digital, Culture, Media and Sport (DCMS).

During the session Dr. Bertie Vidgen, Head of Online Safety at The Turing, will introduce the Observatory, explain why it is needed, and give a live demo of how it works with a case study on tracking abuse against Premier League football players on Twitter.

Notions of intelligence in the digital age: Exploring the intersection of social media intelligence (SOCMINT) and human intelligence (HUMINT) – Challenges, priorities, and trends

- Andrew Staniforth (Swansea University, SAHER (Europe))
- [Non-presenting co-author: Prof Stuart Macdonald (Swansea University)]

Citizens across the world receive protection from terrorism under the aegis of various agencies across the landscape of their government's national security architecture. Critical to the future success of counter-terrorism is the cooperation between state agencies and social media companies, to swiftly remove harmful online terrorist content and harness the power of social media intelligence (SOCMINT). In this paper, the cooperation between very different emanations of state power and private enterprise is examined, seeking to identify ways in which to meld and amplify their approach to tackle terrorism together, despite opposing cultures and operating practices that are not without their imperfections. This paper also explores ways in which closer cooperation could be delivered for mutual benefit and examines whether a truly collaborative and interoperable approach to tackle terrorism is achievable, together with an analysis of the impact and unintended consequences of SOCMINT on the future viability of traditional intelligence gathering disciplines in the digital age.

GIFCT Tech Trials: Combining Behavioural Signals to Surface Terrorist Content Online

- Sarah Pollack (Global Internet Forum to Counter Terrorism)
- [Non-presenting co-author: Tom Thorley (Global Internet Forum to Counter Terrorism)]
- [Non-presenting co-author: Dr Erin Saltman (Global Internet Forum to Counter Terrorism)]

This paper explores the results from testing and analyzing approaches to the deployment of multi-layered content and behavioural signals for surfacing terrorist and violent extremist content (TVEC) online. Technical approaches for surfacing, reviewing, and removing TVEC online have grown in recent years. However, little is known about the layered or hybrid models deployed by tech platforms to combine signals and ensure greater accuracy in removal processes or counter-narrative targeting. Photo and video matching technology and linguistic processing are two of the more commonly discussed tools. Photo and video matching is used in cross-platform approaches such as the GIFCT Hash Sharing Database1 while many CVE approaches employ various "search redirect" methods using terms lists or linguistic matching.2 This research discusses initial results from GIFCT tech trials that test approaches for combining TVE signals and tooling in order to assess how best to decrease the likelihood of false/positives and increase higher accuracy in surfacing TVEC. This paper also explores how these tactics might be deployed in instances of crisis response, where specific location and language understanding can increase efficacy. Lastly, this research will openly discuss ethical and human rights considerations and suggested parameters for the deployment of the methodologies it explores.

Technology: Helping everyone to report terrorism concerns

- Jim Scarrott (Metropolitan Police Service)
- Prof Tom Chen (Raven Science)
- [Non-presenting co-author: Prof Jorge Blasco (Raven Science)]

Formed in 2010 the Counter Terrorism Internet Referral Unit (CTIRU) is part of UK Counter Terrorism policing. The unit investigates online terrorism content. Within the UK we encourage members of the public to report their online terrorism concerns. Each year thousands of reports are made by the public direct to the CTIRU.

Raven Science is a spinout from cyber security research at City, University of London, with initial support from the Innovate UK Cyber ASAP programme. The company's mission is to develop science and engineering solutions to protect the public from online harms, focusing on counter extremism. In 2020, the company won the Mayor of London's Civic Innovation Challenge (counter extremism theme) and developed the iReportIt app to report online terrorist materials via smartphone in cooperation with the CTIRU and London Mayor's Office. The company is also developing an iReportIt browser extension to allow reporting within a web browser.

Panel 4C: Extremist narratives

Chair: Dr Kamil Yilmaz (Swansea University)

Navigating semi-legitimacy in the online space: Investigating the Taliban's engagement with mainstream narratives within its post-takeover social media strategy

- Hirah Azhar (University of Southampton; Imperial War Museum)

After its August 2021 takeover of Afghanistan, the Taliban's social media strategy is simultaneously focused on maintaining the group's enduring identity as the mujahideen and enforcers of Sharia law, while also toning down its narratives for international recognition and legitimacy. Examining how the Taliban's influence operations interact with other sources of information in the online space will demonstrate how it is co-opting others' narratives and strategies for its two very different purposes: legitimacy and outreach. This paper will focus on how Taliban and pro-Taliban accounts engage with mainstream narratives, and what this reveals about their digital strategies. Not only does the sharing of mainstream narratives have a legitimising effect, it also provides the Taliban with room to manoeuvre within a divided online space, where its content is presently banned by one social media platform (Facebook) but allowed by others (Twitter, Telegram). This includes the adoption of a neutral linguistic tone and multimedia content, as well as the use of different languages and online platforms to effectively tailor its messaging. While this paper will focus mainly on Twitter and public Telegram channels, its findings can both help develop a more cohesive social media policy towards the Taliban, and better content moderation strategies.

'The Right to Bear Attack Helicopters Shall not be Infringed': Contemporary Events, Historical Precedent, and the Supercharging of Conspiracy Theories

- Ashton Kingdon (University of Southampton)
- Dr Chris Fuller (University of Southampton)

The defeat of the world's preeminent military power at the hands of the Taliban insurgency, combined with the chaotic withdrawal from a war sold as vital for the national security of the West, created a level of cognitive dissonance that has fed conspiratorial minds. The impossibility of balancing the loss of 'blood and treasure' in Afghanistan with the transient result of the mission provided confirmation to those who subscribe to the conspiracy theories that 9/11 was 'an inside job' to feed the military-industrial complex, and that the 'War on Terror' was a creation by the 'deep state' to enable the introduction of an authoritarian world government. The research presented here combines the academic disciplines of history, criminology, and computer science, to explore the conspiratorial narratives emerging from memes disseminated from both far right and pro-Taliban accounts. Utilising evidence collected from Twitter and Gab during the month of August 2021, this paper will outline how conspiratorial information spreads from the mainstream to the fringe and back again through coded imagery. Ultimately, this paper will argue that these beliefs, reasserted across social media via memes following their apparent confirmation by contemporary events, have been rendered more durable due to their similarity to actual historical conspiracies, such as Iran-Contra and Operation Cyclone. Collectively, this overlap of the imagined and the real has supercharged and accelerated the dissemination of well-established conspiracy theories, deepening anti-government sentiment to dangerous new levels, and increasing the risk of extremism.

IT'S OVER: The Manifestation and Implications of Conspiratorial Narratives on Incel Forums

- Or Goldenberg (King's College London)

Discussions about the 'involuntary celibate' (incels) milieu are widespread in traditional media and are increasingly gaining traction in academia. Research usually addresses the phenomenon by focusing on misogyny or violent extremism. This study provides insight into an underexplored dimension of the incel milieu by examining the manifestation of conspiratorial narratives on three different online platforms on which incels are active. The three assessed forums are Incels.is, Blackpill.club, and two different incel Discord servers. This study takes an inductive approach and starts with a digital ethnography and expert interviews to understand the nuances and jargon of the heterogeneous and flexible incel milieu. Data collected for the purpose of this study was examined using content analysis and subsequently scrutinised thematically to understand broader implications. While the selection of forums for this study accommodates the more outspokenly extremist incels and by no means represents everyone who self-identifies as an incel, this study establishes that conspiratorial narratives are prevalent in the examined forums. Subsequently, the ramifications of conspiratorial thinking are considered vis-à-vis the gradual radicalisation processes within the milieu. While this does not imply a spillover to offline violence, it reflects how incels either approach life fatalistically or glorify violence.

Panel 4D: The Impact of Studying Online Extremism on Researchers' Mental Health: Mitigating and Overcoming the Challenges

- Broderick McDonald (University of Oxford)
- Stevie Voogt (Moonshot CVE)
- Dr Lizz Pearson (Royal Holloway, University of London)
- Olivier Caubergh (University of St Andrews)

Researchers who face repeated exposure to extremist content are at significantly higher risk of developing symptoms of generalized anxiety and depression. While these symptoms become more acute the more time a researcher spends exposed to this content, complete avoidance of this material is often not an option, especially for early career researchers. To address this issue, this breakout session will facilitate a discussion of the mental health challenges associated with researching extremist content, as well as offer practical insights and advice from clinical psychology to mitigate these risks. The panel will explore new research on this topic and practical interventions to reduce the risks to researchers and practitioners, as well as the broader systemic issues involved. Broader systemic changes can include greater use of automated and quantitative methodologies to review and analyse content, allocating greater funding for mental health training, developing peer support networks, learning from other professions such as law enforcement who are required to view and analyse graphic content. All of these approaches are intended to work in tandem and the issue cannot be fully addressed with only one tool. Despite its importance for academics, think-tankers, and employees of technology firms, this issue is rarely discussed or even acknowledged. Ignoring or avoiding the mental health challenges associated with researching extremist content is dangerous and can lead to more severe symptoms and outcomes. As such, this breakout sessions seeks to tackle one of the most difficult but important challenges to studying terrorism on social media and provide real support to researchers in this field. This session addresses one of the most serious and limiting issues facing researchers studying online extremism from a variety of different angles and perspectives.

BREAKOUT SESSION 5 ABSTRACTS

Panel 5A: Audio-visual content

Exploring Anti-Modern Aesthetics on Audiovisual Platforms

- Meghan Conroy (Investigator, U.S. House of Representatives)
- Robin O'Luanaigh (Center on Terrorism, Extremism, and Counterterrorism at Middlebury Institute of International Studies at Monterey)
- Matt Kriner (Center on Terrorism, Extremism, and Counterterrorism at Middlebury Institute of International Studies at Monterey)

There has been a noticeable dissemination of nature-centric, rural, and "cottagecore" aesthetics on social media. These aesthetics became heavily entrenched within more progressive subcultures online, such as the LGBTQ+ community. However, some of the values imbued in these aesthetics—preference for rural residency and traditional women's fashions—can also be found among tradwives, preppers, survivalists, primitivists, and violent extremists. This trend reflects a moral panic and rejection of modern principles in favor of traditional values that serve as shared romanticized ideals across ideological lines. A significant through line in these varied subcultural spaces is the repudiation of liberal democratic values in lieu of arcane philosophical connections more commonly aligned with violent, extreme worldviews, namely fascism.

This paper will explore the spread of this aesthetic on social media platforms that emphasize audio-visual content. In the process, it will evaluate to what extent progressive and reactionary causes overlap in their aesthetic choices on mainstream platforms. This paper will conduct monitoring and analysis of anti-modernity aesthetics on TikTok and Instagram and will assess the interplay of mainstream and extreme ideography. Importantly, it will explore what this interplay means for those on social media who shift seamlessly between seemingly disparate extreme and mainstream spaces.

Images as narrative: Analysing how the Islamic State manipulates images for storytelling purposes

- Dr Simon Copeland (Swansea University)

Analysing extremist images in a systematic and rigorous manner way remains a significant methodological challenge. This paper seeks to address this gap by proposing how the photographs employed in the Islamic State's propaganda may be 'read' narratively – that is as artifacts evocative of implicit, emergent stories in the minds of those that consume them. Whilst the presence of symbols, motifs, or representations of societal or cultural meanings are often noted in reference to extremist propaganda, the images contained also inherently trigger imagination; in any given image individuals naturally see a succession of incidents or events that have led up to it, just as they envision those that follow it. Given that extremists seek not only to persuade but also to inspire – something that necessarily rests on the capacity to imagine – it is crucial to understand how their images are manipulated to shape how they may be read. The methodology proposed in this paper highlights the 'texture and techniques' by which the Islamic State carefully composes, frames and edits images to tell certain stories.

Making Sense of (Millions of) Far-Right Images: A Machine Learning Approach

- Prof Stephane J. Baele (University of Exeter)
- Dr Lewys Brace (University of Exeter)
- Dr Aaron Rudkin (Trinity College Dublin)
- [Non-presenting co-author: Prof Nicole Doerr (University of Copenhagen)]
- [Non-presenting co-author: Dr Elahe Naserian (University of Exeter)]

ISIS' use of graphic imagery and the widespread dissemination of far-right memes emerging in online image-boards have rightly pushed an increasing number of scholars to analyse the visual dimension of extremist and terrorist communications (e.g. Winkler & Dauber 2014, Baele, Boyd & Coan 2020). Although these studies have disclosed crucial insights, their reliance on qualitative or hand-coding methods has meant that they usually both rest on small or very limited samples and depend on researchers' pre-existing theories and assumptions about their empirical cases. While these two characteristics can be seen as strengths, they restrict the type of analysis at hand and work best when complemented by other methods of visual analysis following a more inductive approach and using very large corpora.

The present paper offers one such method: we put forward a model of image clustering through machine learning, designed to be applied to very large amounts of extremist visual imagery. We show the usefulness of this model by applying it to a new, unprecedently large database of extremist images coming from three different online spaces populating the US far-right online ecosystem: Telegram, forums, and websites. This novel approach, akin to a "topic model of images", allows us to identify the main types of visual tropes constituting today's far-right online communities, thereby shedding a new light on how these images participate to the construction of today's far-right in-/out-group identities.

Drei Steine and Kreativ gegen Rechts: Responding to Right-Wing Online Extremism through Visual Creative Futures

- Dr Orla Lehane (National University of Ireland Galway)

Visual materials play a significant role in the online activity of violent extremist organisations. Provocative visuals, including memes, gifs, videos and more, are shared widely by right-wing extremist groups via social media platforms including Facebook and Instagram. While the sharing of such images online is a key element of the online activity of right-wing extremist groups, many grassroots violence prevention practitioners do not counter this material only with online visual messaging, viewing their online and offline work as synonymous. This paper explores a selection of images shared by right-wing groups on social media platforms and the harnessing of visual materials, namely in the form of the graphic novel Drei Steine by Nils Oskamp, to counter this messaging. This paper draws on textual/visual analysis and creative futures approaches to compare this work with the images shared via social media by right-wing extremist groups. Both can be conceived of as spaces for relational encounters, and use affect to influence the public to create change. This work seeks to understand the mechanisms involved and how the differences between online and offline media feed into this. Ultimately this work considers how these understandings can be used to inform future policy responses to online violent extremist materials.

Panel 5B: Effective and Ethical Pedagogical Praxis in Extremism and Terrorism Research Online: An Interactive Discussion

- Dr Cori E. Dauber (University of North Carolina at Chapel Hill)
- Mark Robinson (University of North Carolina at Chapel Hill)
- Dr Ashley Mattheis (University of North Carolina at Chapel Hill and Centre for Analysis of the Radical Right)
- Brian Ladd (North Carolina State University)

This roundtable-style discussion focuses on the methods and challenges involved in effective and ethical pedagogical practices for training advanced undergraduate and graduate student researchers of extremism and terrorism online. Using our recent multi-semester, advanced undergraduate research "task force" course as a case study, our discussion focuses on our planning, issues we have encountered, and our experiences to highlight contemporary discussions within the wider community of researchers. These wider discussions include topics such as mental health and wellbeing, researcher safety online, and ethical research practices (see for example: Allam 2019, Winter 2019, Mattheis and Kingdon 2021). To this conversation we add a discussion of incorporating such ethical considerations within an effective model of pedagogical training drawn from our own teaching and research training experiences inclusive of work with graduate trainees (PhD and Master's levels) and advanced undergraduate students. This pedagogical discussion foregrounds collaborative, hands-on training approaches and a commitment to "engaged" scholarship such that students coming out of our programs (graduate and undergraduate) have the applied skills to seek future pathways both inside and outside the academy.

Panel 5C: Tech Against Terrorism: Open-source intelligence, research, and policy on countering terrorist use of the internet whilst respecting human rights

Chair: Lord Carlile QC

- Anne Craanen (Senior Research Analyst, Tech Against Terrorism)
- Arthur Bradley (Senior OSINT Analyst, Tech Against Terrorism)
- Fabienne Tarrant (Senior Policy Analyst, Tech Against Terrorism)

Tech Against Terrorism is a public-private partnership focused on knowledge sharing and providing support to small tech platforms in tackling terrorist exploitation of the internet whilst importantly upholding human rights.

In this session, we aim to highlight research studies from our open-source intelligence, research, and policy teams. Our panel will include three presentations, followed by a Q&A. It will be focussed on trends in terrorist exploitation of the internet, including: terrorist and violent extremist operated websites; a research study on designation of terrorist groups and the effects on the online content produced by those groups; and, human-rights considerations and recommendations when it comes to moderating such content. We aim to make these presentations engaging for both academics and practitioners, and welcome all stakeholders to participate.

Panel 5D: Countering (Online) Violent Extremism: Practitioners from the Global South

To add

BREAKOUT SESSION 6 ABSTRACTS

Panel 6A: Extremist culture

The Evolution of Siege Culture in the UK

- Dr Benjamin Lee (University of St Andrews)
- [Non-presenting co-author: Dr Sarah Marsden (University of St Andrews)]

Siege culture is an extreme ideological tendency within the far-right. Militant rhetoric, violent imagery, and real-world violence associated with the subculture have generated substantial interest from security practitioners but available research has concentrated on specific texts, most notably James Mason's Siege, and related groups, rather than recognising the subculture as a whole. In contrast, this paper offers a case study of Siege Culture as a subculture, with a specific focus on how it manifested in the UK. The case study suggests that Siege Culture is dynamic, evolving as the result of UK based participants interacting with transnational ideas, norms and aesthetics. This paper contributes to knowledge in three ways: it extends knowledge of Siege Culture itself; it applies the concept of a subculture as a way of expanding understanding of extremist communities beyond a focus on single platforms or groups; and it highlights how transnational ideas play out in local contexts.

White Power music: It's Role in Radicalization Online, and Challenges in Policy Development

- Abhishek Roy (Google)
- Bradley Galloway (Organization for the Prevention of Violence)

"White Power Music" is used as an umbrella term to denote a variety of pro white supremacy music scenes from around the world. In the last decade, a series of well documented instances of real-world violent acts have materialized where assailants were either avid consumers or active producers in the white power music scene. Internet platforms have been used to host, distribute and sell white power music or related paraphrenalia online. In this user study, we conducted 60-minute semi-structured user interviews with four participants who were formerly associated with the white power music scene in USA and Canada. We gathered foundational knowledge about white power music, it's role in the radicalization process and how it is used as a tool for propaganda, to raise money and to recruit people for the White Nationalist movement. We further propose a typology for classification of white power music songs to help guide policy development conversations on online platforms. We evaluate this typology on a sample of songs from 50 bands found on major streaming platforms online. We find this typology to be helpful in a lab setting and a helpful input for policy development for online platforms, although it warrants further calibration and assessment in light of the design and environment specific to each service.

Far-Right 'Reactions': A Comparison of Australian and Canadian Far-Right Extremist Groups in Facebook

- Jade Hutchinson (Macquarie University; Groningen University)
- Dr Julian Droogan (Macquarie University)

Little is known about which social media affordances appeal to users of extremist groups, how such affordances influence a user's interaction with far-right themes and narratives, and how this is being experienced across nations. In this study, we used a mixed methods approach to conduct a cross-national comparative analysis of over eight years of 'Reaction' use across 59 Australian and Canadian far-right extremist groups in Facebook. We assessed the level of user-engagement with Facebook public group posts using 'Reactions', and identified the types of posts, themes and narratives that generated the most user engagement specific to each (Like, Love, Haha, Wow, Sad , Angry). This was paired with a qualitative analysis of the more popular 'Reactions' used over time, and the themes and narratives that attracted the most user engagement. Results highlight the 'Anger' and 'Love' Reaction as effective generative mechanisms for user engagement with far-right themes and narratives, while producing dangerously broad spectrums of referential meaning with moral and ideological implications. This study contributes to research on how personalisation algorithms may exacerbate the influence of affordances when assigned to far-right themes and narratives.

Sticking it to the Islamic State: User-Created Telegram ISIS Stickers

- Meili Criezis (American University)

Substantial studies have provided insightful and ground-breaking findings on extremists' use of social media ranging from mainstream platforms to more fringe spaces including applications with encrypted capabilities. Telegram, perhaps one of the most well-known platforms preferred by decentralized pro-IS online supporter networks has, and is continuing to be, extensively researched. Although mentioned by researchers in passing, the topic of pro-IS Telegram propaganda stickers has not received much examination. For this study, I have collected a total of 80 user-generated Islamic State-themed sticker sets totaling over 500 individual stickers within a two-year period and analyse the following: why and how usage of sticker sets contribute to a sense of community in online extremist spaces, the various ways in which these stickers are employed within pro-IS channels and private group chats, the array of narrative themes conveyed by imagery representation, and the presence of gendered messaging expressed by sticker sets focused on portraying women of the Islamic State. Importantly, sticker content completely falls under the category of unofficial propaganda therefor providing a unique window into a case study of extremist supporter communities as opposed to official terrorist propaganda.

Panel 6B: The role of regulation

Chair: Dr Katy Vaughan (Swansea University)

Terrorist content, regulation, and compliance: how regulation can better categorise social media platforms to ensure compliance

- Dr Amy-Louise Watkin (University of the West of Scotland)

This research is taken from a doctoral thesis that analysed existing regulation to counter terrorist content on social media platforms. One of the findings was that existing regulation has had a tendency to either neglect the challenges that different platforms may face when complying with regulation to counter terrorist content on their services, or, it categorises social media platforms by size (e.g., large platforms and smaller platforms). Both of these are problematic. The former creates unfair burdens on certain types of platforms and could result in reduced market competitiveness. The latter typically results in larger platforms having to comply with greater demands than smaller platforms. This is problematic given that research by Tech Against Terrorism has revealed that smaller platforms are heavily targeted by terrorist organisations. This paper proposes that future regulation should consider categorising platforms based on: 1) awareness; 2) capacity; and 3) willingness. This presentation will put forth arguments for categorising platforms in this way as well as tailored responses and enforcement strategies that regulation could adopt for platforms in each category. These tailored responses take both an educative and punitive approach (the latter only where necessary), as opposed to many existing regulatory frameworks that only take a punitive approach.

Necessity vs. Fundamental Rights: Civil Society and the EU Regulation on Addressing the Dissemination of Terrorist Content Online

- Reem Ahmed (University of Hamburg)

Research suggests that counter-terrorism legislation tends to be guided by precaution, risk, and selected knowledge. However, recent examples have shown that civil society actors' influence on counter-terrorism legislation cannot be underestimated, especially when issues of internet governance come into play. During the negotiations of the EU Regulation on addressing the dissemination of terrorist content online, civil society groups raised concerns regarding the safeguarding of fundamental rights and challenged the proportionality of the proposed measures. Civil society actors were partially successful in influencing key aspects of the final text of the Regulation; thus, raising the question of how such groups have managed to influence traditionally "exceptional" security policy and effectively "politicise" this area. This paper seeks to explore this further by looking at the evolution of the EU Regulation and the impact that civil society actors have had on the formulation and wording of key Articles in the final text. Using associated legislative documents and debates, as well as the websites of civil society groups and activists, this paper examines the extent to which the EU institutions acknowledged civil society demands and how they weighted these contestations against the perceived risks of extremist online content and its potential links to violence.

The Politics and Realities of Far-Right Deplatforming and Persistent Engagement

- Dr Michael Loadenthal (University of Cincinnati)

Beginning in 2018, the US Department of Defense, led by Cyber Command and the National Security Agency, promoted the doctrinal strategy of Persistent Engagement (PE). PE as a cyber strategy seeks to establish and maintain a combative initiative through a continuous orientation towards defense and attack. Rather than a reactive policy which seeks to respond to intrusions, data breaches, and exfiltration, PE encourages adoptees to constantly practice both a proactive protective posture and a desire to degrade the opponents' capabilities. While such a shift represents a national security course correction for Cybercommand, this approach has been the doctrine of choice for digital deplatformers challenging the far-right (and to a lesser degree Salafi-Jihadists) for decades. Through examining the efforts of those battling 'racially-motivated violent extremists,' this paper explores the politics, practices, and strategy of deplatforming in light of the wider shift towards PE. How have activists damaged the online social media and operational capabilities of their opponents through the use of misdirection, resource sapping, tampering, and 'doxxing'? How have the recent experiences of White Lives Matter organizers and accelerationist neo-Nazis demonstrated the potent value of long-term, disruptive engagement? What can we learn about the utility of counter-recruitment and counter-radicalization efforts through examining these disruptions?

Panel 6C: Accelerationism Research in Practice: A Workshop Facilitated by the Accelerationism Research Consortium

- Meghan Conroy (Investigator, U.S. House of Representatives)
- Jon Lewis (Program on Extremism, George Washington University)
- Matt Kriner (Center on Terrorism, Extremism, and Counterterrorism at Middlebury Institute of International Studies at Monterey)
- Alex Newhouse (Center on Terrorism, Extremism, and Counterterrorism at Middlebury Institute of International Studies at Monterey)

In December 2021, a group of extremism researchers co-founded the Accelerationism Research Consortium (ARC). The overarching goal of ARC is to provide a forum for researchers to generate empirical analysis on the topic of accelerationism. We aim to bridge the divide between practitioners, researchers, policymakers, and journalists by establishing cross-industry working groups that will collaboratively discuss, debate, and level-set approaches to understanding and addressing the threat of accelerationist actors and groups. Through engagements with internal partners and external stakeholders, ARC is positioning itself as a trusted partner to all on evaluating accelerationism.

At TASM 2022, ARC will host a workshop during which attendees will learn how to identify accelerationism in online spaces. Accelerationism, by design, exploits trends in the extremist landscape, including but not limited to groups, movements, and aesthetics. This workshop will arm researchers, practitioners, and policymakers, among others, with the practical capabilities to identify and evaluate both explicit and veiled accelerationist presence across the online ecosystem.

The 90-minute session will be broken into two parts:

- Part A: The first part will consist of a 60-minute workshop focused on the symbols, slogans, rhetoric, and aesthetics of accelerationism; the multi-layered messaging undertaken by accelerationists; and a network analysis of known accelerationist actors. This will include 15 minutes earmarked for a Q&A with attendees.
- Part B: The workshop will then be accompanied by a 30-minute demonstration of how to identify indicators that can be used to detect evolutions and emerging trends within the accelerationist space. The demo will feature an explanation of the practical application of indicators in research, including a discussion of specific projects and clients who benefit from indicator-driven research. Additionally, the panelists will discuss policy outcomes.

Panel 6D: Technical Approaches to Counter Terrorism Online: Partnerships & Cross-Platform Methods

- Sarah Pollack (Interim Chief of Staff, GIFCT)
- Adam Hadley (Director, Tech Against Terrorism)
- Marc-André Argentino (International Centre for the Study of Radicalisation)
- Lucy Calledine (Government Affairs and Public Policy, YouTube)

This workshop will discuss the tooling, hybrid moderation tactics, and artificial intelligence used by tech platforms in their efforts to counter terrorism and violent extremism online. Technical approaches for preventing terrorist use of the internet (PTUI) can be company specific, furthered by partnerships companies have with NGOs or through cross-platform collaborative infrastructure. This workshop will highlight a variety of tooling-focused approaches and give insight into cross-platform and cross-sector methodologies available for PTUI practitioners.

GIFCT and TAT both manage and provide different structures and technical capacities to tech companies in order to further efforts in PTUI. GIFCT will discuss the evolution and expansion of the Hash Sharing Database that it manages for member companies to share signals across platforms in a way that does not violate privacy or human rights. TAT will discuss how the Terrorist Content Analytics Platform (TCAP) operates to track, verify, and analyse terrorist content across the internet, enabling it to flag terrorist content directly to affected platforms for review and removal.

To frame these tooling approaches GNET will provide a broad review of some of the primary adversarial shifts its global network is seeing for how terrorists and violent extremists are evading basic detection tactics to avoid being blocked or banned from platforms. YouTube, as the 2021 Chair of GIFCT, will discuss where tooling needs are specific to a given platform versus where cross-platform signal is increasingly important and what this looks like for triaging between tools and human review.

To workshop with the audience, the Q&A will look to engage the audience by teasing out areas for tooling development, what adversarial shifts mean for technical approaches, and how to ensure tooling solutions are not at the cost of other fundamental human rights such as privacy or free speech.