# Terrorism and Social Media

An International Conference

**Swansea University Bay Campus**
**25th - 26th June 2019**

# Abstracts and Key Takeaways

**#TASMConf**
**Swansea University**
**25-26 June 2019**

**Contents page**

## Keynote Speakers

"Challenges Ahead: Advancing the Study of Terrorism, Extremism and Social Media"
*J.M.Berger (VOX-Pol Research Fellow, Swansea University)*

**Key Takeaways:**

- Terrorism and extremism are two overlapping but distinct fields of inquiry; they are not the same field
- Political expediency and failure of definition conflates these tracks, inhibiting research and policy advancement

"Tackling terrorist content online through a human rights-based approach"
Krisztina Huszti-Orban (Senior Legal Advisor to the United Nations Special Rapporteur on Counterterrorism and Human Rights)

## Breakout Sessions

[*Italicised* names are speakers; non-italicised names are non-speaking co-authors]

### Panel 1A: Inter-group competition and scapegoating

"Sovereign but Not Alone: An Examination of Competition and Cooperation Among American Sovereign Citizens Online"
*Matthew M. Sweeney (University of Massachusetts Lowell)*
@MMSweeney1109
The Sovereign Citizen Movement has emerged as a preeminent threat to law enforcement officers and members of the general public in the United States. From 2000 to 2017, Sovereign Citizens were responsible for the deaths of 21 law enforcement officers and 37 civilians, and for the injuries of 25 officers and 50 civilians. Due to the disconnected nature of such a movement, online platforms have become essential to the spread of its' ideas. However, even with the violence associated with them, empirical and primary source research is almost nonexistent. This study will examine the online interactions between Sovereign Citizen websites, paying attention to the level to which Sovereigns cooperate or compete with one another. The question this work will answer is, do Sovereign Citizen websites compete or cooperate with one another? Also, how does this competition or cooperation impact tactical choice and ideological cohesion? The data for this study is a sample of over 70 American Sovereign websites identified through a two-step process; open source keyword-based searches and hyperlink connections between websites. This work hypothesizes that competition between websites will result in greater tactical diversity and lower ideological cohesion.

"Islamic State's Hashtag War: Terrorism and the Jewish Community"
*Representative from the Community Security Trust*
Focusing on an Islamic State (IS) social media campaign, this presentation will track the origin and journey of a violent antisemitic IS Twitter hashtag urging attacks against Jews globally by using the hashtags #attack_theJew/#slaughter_theJew. The presentation will set out how Islamic State's online strategy involved capitalising on an existing Twitter campaign urging attacks against Jews, and propelled it on to a global stage, stamping its authority and ownership over the campaign by appropriating violent and explicit imagery, videos and phrases that it shared amongst its global network. The presentation will set out how the IS campaign dwarfed the original local Twitter campaign and pointed towards the ability of IS to capitalise on real world events, surpass the politics and barriers of local groups and utilise social media to reach a global audience.

"Blame Game: Responses to Militant Jihadist Terrorism in the Extreme Right Digital Milieu"
*Benjamin Lee (Lancaster University)*
@nebulon82
There is a well-established assumption in terrorism studies that violence by militant jihadists 'feeds' the extreme right. However, empirical evidence suggests that the reality of any connections between different forms of extremism is nuanced and dynamic. This paper attempts to better understand how extreme right web spaces react to militant jihadist terrorism using a granular qualitative study of posts made in three extreme right web spaces in the aftermath of three terrorist attacks by militant jihadists in the UK in 2017. The results show common themes between ideologically distinct web spaces. The assignation of blame, identification with victims, and the proposed solutions, all suggest that within the extreme right milieu terrorist violence is interpreted in the light of pre-existing worldviews rather than as a stimulus for new ideas. This work furthers understanding of reciprocal radicalisation and highlights the importance of the transnational extreme right as it exists digitally, a space conceptualised in this paper as the extreme right digital milieu.

**Panel 1B: The online/offline nexus**

"Radical and extremist use of social media in a conflict between Russian Federation and Ukraine"
*Viktor Pushkar (National University of Kyiv)*
Generic theoretical approach is proposed for the social media use in an interstate conflict, including the state, the non-state actors and the proxy actors' involvement. The other part is based on field data, mostly not sufficiently systematic before 2014, and more systematic since 2014 when Ukraine was officially recognized a target of Russian informational special operations. The subject requires interdisciplinary approach, including anthropology, psychology and applied linguistics, leading to creation of mathematical model(s). Most existing works known to us are limited to analysis of texts in English and Russian. However, the important part of relevant narrative is bilingual or available exclusively in Ukrainian. Typical linguistic patterns indicate the agents of influence who received similar instructions. Even limiting the research to Facebook only, we should adapt existing analysis tools to bilingual texts. Regarding the popular concept of information weaponization, we consider the normative influence, operating the specific kind of information which is not explicitly harmful by itself but prepares the target audiences for radical or extremist messages acceptance. Normative influence targets the large group culture and identity, causing full or particular identification with aggressor. The large-scale operations are usually supplemented by boutique informational influences targeting the small groups.

"Affect and Online Extremism: Reflections from the UK's Radical Right"
*Elizabeth Pearson (Swansea University)*
@lizzypearson
Much attention is paid by both policy-makers and academics to the ways in which the internet is important to radicalisation. Most research has focused on online 'Jihadist' extremism, engaging an 'outside-in' analysis of the text, pictures and links shared by extremists, and exploring the organisational approach of groups. How 'extreme' members of radical networks describe, understand and reflect on this material is less well explored. This article turns to the British radical right scene, and illustrates the ways in which people active in the EDL, Britain First and the counter-Jihad, understand their online activity. It is based on semi-structured interviews carried out between May 2016 and February 2018, with both male and female participants, leaders and grassroots activists who combat what they believe is the Islamisation of the UK, Europe and the West. The paper explores: participants' affective engagement with social media communities; the mechanisms of online activity; and the tensions apparent in online participation. It suggests the increasingly false dichotomy of online versus offline approaches to radicalisation, and reveals the ways in gender and affect factor in participation in this 'extreme' community.

**Key Takeaways**

- Online and offline aren't distinct. They are increasingly entwined
- Emotion matters in radical movements. It's more about 'heart-washing' than brain-washing

"Boots on the Ground? Online and Offline Identities of the Extreme Right"
*Bradley J. Galloway (University of the Fraser Valley)*, Ryan Scrivens (Concordia University), Barbara Perry (University of Ontario Institute of Technology), Garth Davies (Simon Fraser University) and Richard Frank (Simon Fraser University)
@bjgalloway1717 & @R_Scrivens
Right-wing extremists, amongst other extremists, continue to exploit the power of the Internet by connecting with like-minded others from around the globe and developing a sense of identity both on- and offline. A growing body of literature has been dedicated to exploring this phenomenon, with an interest in how the on- and offline identities of these adherents overlap. Overlooked in these discussions, however, has been an insider's perspective of how adherents' online identities emerge in the offline realm. Drawing from the insights of a former right-wing extremist who was an online recruiter for over 10 years, paired with an open-source analysis of the content found in a popular online space of the extreme right, we explore how the on- and offline identities of right-wing

extremists connect by differentiating between those who are violent and non-violent extremists. The findings reveal that, while both factions share similar ideological beliefs and a victim mentality, each camp uses distinct strategies to mobilize the movement both on- and offline – tactics that are largely dictated by gurus in the sample.

**Panel: 1C Non-English language propaganda**

"Monitoring a periphery of extremism - Education of disintegration in Online Dawah Videos on German YouTube"
*Till J Baaken (Modus; Centre for Applied Research on Deradicalisation)* and Friedhelm Hartwig (Modus; Centre for Applied Research on Deradicalisation)
@tillbaaken & @modus_zad
Epic stories, *anāshīd* and the friendly Imam from next door – Online Dawah videos are as diverse as the people watching them. These videos do not specifically endorse violence, but can serve as a gateway to interpretations of Islam, which open young people to exploration of more radical interpretations of the religion and in the worst case, towards a path of violence. Defining a periphery is one of the major challenges in the triad of freedom of religion, preventing radicalisation early on, and monitoring content by academics. Exemplified by the scene in Germany it will be discussed how a periphery of extremism engages with its audience using different forms of output online. An analysis of YouTube videos shows a wide array of content disseminated from a multitude of channels. After having examined YouTube using the method of First impression Screening (FIS) a qualitative thematic approach brings to light the hot topics, narratives, actors, and trends in this periphery. Peripheral actors show a high level of professionalism, flexibility, and creativity in reacting to the questions and needs of individuals looking for spiritual or life guidance. On the other hand, more traditional means like the singing of *anāshīd* as well as storytelling are employed to influence the target group emotionally. Additionally, leading German activists are well embedded in the dynamic transnational network of worldwide Salafi and Wahhabi content production such as the translation of lectures, books, sermons, videos, and images. First findings of the project in the form of a typology of different videos as well as the major trends and actors will presented

**Key Takeaways**

- The periphery of Islamist extremism use framing techniques to try and align the worldview of the viewers with their own. Using diagnostic and prognostic framing the producers of legal content on YouTube use narratives of a Salafist-Wahhabist interpretation of Islam and hence can act as a gateway for some viewers to more extremist views.
- The network of the channels on YouTube forms an echo chamber that so far has not been penetrated by counter narratives. Several channels fulfil a function of a gateway to the periphery content, knowingly or unknowingly. Some of these actors may be strong allies in countering extremist narratives.
- The Islamist echo chamber on YouTube is enforced by the recommendation "Up next" algorithm. Counter narratives must try to penetrate this algorithm to have any real impact; otherwise, the target group will not be reached on the platform.
- Deleting channels in the periphery of extremism has the opposite of the intended effect. Content reappears on smaller channels and the deleted actor gains popularity.

"User-generated, pro-Islamic State media in tertiary languages: Bushra and Georgian-language propaganda"
*Bennett Clifford (George Washington University Program on Extremism)*
@_bCliff
At their peak of production, Islamic State (IS) media divisions produced and translated content into a litany of world languages, providing a worldwide, multilingual base of supporters with accessible content. "Top-down" production and dissemination of Islamic State media products in a handful of official languages—namely Arabic and English—continues to receive a lion's share of scholarly analysis on the topic, sometimes at the expense of exploring unofficial media and media in less

common languages. As a test case of how individual bases of supporters respond to the lack of officially-produced IS media in their native languages, this study analyzes a corpus of over 200 images produced by the media outlet "Bushra" (Omen) and disseminated via its Telegram channel. Analysis of this case shows that producers of tertiary language propaganda oftentimes have more leeway to blend top-down messaging with local issues and grievances. If successful, unofficial distributors can and do play a role in convincing IS central media outlets to produce official content in tertiary languages. This example of bottom-up diffusion of localized, unofficial content is highly significant for future efforts to understand the interplay between official and unofficial jihadi media

**Panel 1D: ISIS Media Communication**

"Radical Islamist English-Language Online Magazines: AQ & IS Approaches, Interactions with Perpetrators, and Futures"
*Pamela Ligouri Bunker (TRENDS Research & Advisory) and Robert J. Bunker (Safe Communities Institute (SCI) at the USC Price School of Public Policy)*
@DocBunker
The presentation will provide an overview of a multi-year research project conducted for SSI, US Army War College resulting in the publication of two books [one published; *Radical Islamist English-Language Online Magazines* and one forthcoming; *The Islamic State English-Language Online Magazine Rumiyah (Rome)*]. It will begin with an overview of the two-linked projects and explain the place of English-language online magazines within the larger context of Radical Islamist social media. It will then give an overview of Al Qaeda and Islamic State approaches to their English-language online magazines (as well as eBooks), noting the differing strategic approaches. Selected interactions between perpetrators of terrorist incidents directed against the West and IS/*Rumiyah* magazine will then be discussed related to the time frame of this magazine's publication (Sept 2016-Aug 2017). These interactions focus on perpetrator self-identification as an IS operative, known associations, contraband IS materials, and the use of magazine TTPs as well as magazine/greater IS declared links (such as the 'Soldier of the Khilafah' designation) back to the perpetrator. The final section of the presentation will discuss the future of radical Islamist English-language online magazine use and the benefits a magazine format has for cohesive narrative articulation versus other social media approaches.

"The Modern Phoenix: Documenting the Insurgent Campaign of the ISI (2008-2013)"
*Craig Whiteside (US Naval War College)*, Max Baker, Fatih Celeney, Anas Ellalame, Alex Newhouse and Ian Rice
@CraigAWhiteside

"Transmitting the Caliphates, Real and Imagined"
*Haroro Ingram (George Washington University Program on Extremism), Jade Parker (Columbia University), Craig Whiteside (US Naval War College),* Audrey Alexander (George Washington University Program on Extremism) and Daniele Raineri (Il Foglio).
@haroro_ingram, @cyberAOR, @CraigAWhiteside, @Aud_Alexander & @DanieleRaineri
The Islamic State media department has morphed into a world class media enterprise with a sizable presence in local markets, concrete influence over its global media affiliates, and an expansive online presence. This research paper builds on a previous history of the media department to trace its efforts since 2016 to survive a sustained counter-terrorism campaign designed to reduce its impact on global populations. The focus of the paper is to answer questions on the organizational design, technology, and leadership of the department. Using primary source material, the research highlights the careful line Islamic State media officials walk in controlling content while still maximizing its distribution to consumers.

**Panel 2A: Strategies for online counterterrorism**

"Mass surveillance on Social Media: Will 2018 be a turning point in the European Court of Human Rights' case law?"

*Katia Bousliman (Université Grenoble-Alpes)*
@bouslika
"It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime" said the European Court of Human Right in the highly expected decision *Big Brother Watch v. United Kingdom* in September 2018. This ruling, added to the *Centrüm for Rattsiva v. Sweden* case in June 2018, shows that the European Court of Human Rights accepted that States can adopt mass surveillance policies in the name of the fight against terrorism. This presentation will present how the European Court of Human Rights slightly overturned its jurisprudence in mass surveillance and what will be the consequences for mass surveillance on Social Media.

"Tackling Online Extremism through Takedowns: A Critical Analysis of the NetzDG"
*Reem Ahmed (University of Hamburg)*
@RAhmed105
Up until recently, the EU and its Member States have largely relied on a series of 'soft' law obligations and voluntary cooperation from hosting platforms to aid them in the fight against illegal terrorist content and hate speech. A turning point in this shift from 'soft' to 'hard' law was the introduction of the German Network Enforcement Act (Netzwerkdurchsetzungsgesetz – NetzDG), which places financial burdens on social media companies for 'consistently' failing to remove content that violates any of the 22 statutory offences identified in the German criminal code. The NetzDG came into full force in January 2018, and since then, the UK and EU have put forward similar proposals in the form of the Online Harms White Paper and the proposal for a Regulation on preventing the dissemination of terrorist content online, respectively. Given the significant developments in Internet regulation across Europe, this presentation reflects on the first 18 months since the NetzDG came into force. Using transparency reports from Google, Facebook, and Twitter, as well as relevant case law, I examine whether there is any evidence to suggest that social media companies affected by the law are 'over-blocking' reported content and to what extent freedom of speech is being upheld and safeguarded by the German courts. Finally, I outline and compare the proposals put forward by the EU and UK alongside the NetzDG.

**Key Takeaways**

- The future of takedowns: increased reliance on "hard" laws, which warrant the removal of illegal and potentially legal content on multiple hosting platforms with stricter time limits
- Relying on formal laws, rather than a variety of Community Standards/Guidelines from different platforms, would not only add clarity and transparency to the process of takedowns, but also reduce the risk of extremists exploiting these very inconsistencies in Internet governance

"'I Speak for the Trees': #PineTreeTwitter from Eco-fascism to Xenofeminism."
*Brian T Hughes (American University)*
@mrbrianhughes
As the threat of ecological collapse looms ever-larger, and crises of social dislocation and cultural instability continue to proliferate, the face of eco-extremism is changing. Environmental radicalism—a largely leftwing movement during the 1990s and 2000s—has taken an increasing turn away from its onetime association with the politics of liberation. In its place, misanthropy, anti-egalitarianism, and even racist mysticism are coming to define the moral and ideological core of certain eco-extremists. This range reflects a spectrum of ideological tendencies which do not easily conform to existing operational definitions of left- and right-wing. So-called "pine-tree twitter" (named for the pine tree emojis often incorporated into user profiles) is a publicly-accessible space in which these new eco-extremists express themselves. This paper presents an overview of the rhetorical habits, ideological postures, and moral concerns of these emerging extremist groups. In doing so, it hopes to contribute to a developing groundwork for the study of this potentially significant new vector of extremism.

**Key Takeaways**

- The global climate crisis may lead to a dissolution and reorganization of ideological commitments among extremists.
- We are today seeing the emergence of such new ideological commitments, in the form of an eco-extremism that does not easily track with the conventional left-right/authoritarian-egalitarian political axis.

**Panel 2B: Telegram**

"From Telegram to Twitter: The Lifecycle of Daesh Propaganda Material"
*Mohammed Al Darwish (M&C Saatchi World Services)*
The paper examines the ways through which Daesh official media channels and "fanboys" utilise Telegram to disseminate propaganda material. The paper charts Daesh's efforts to push its content past Telegram into Twitter and the role "fanboys" play in promoting that content. Therefore, it lists the typical life-cycle of sharing a propaganda material: from Daesh channels announcing the imminent release of a propaganda material, to fanboys urging each other to prepare to "invade" Twitter by supplying already activated Twitter accounts and passwords, to finally Daesh releasing the content and fanboys' uploading it on multiple social media and content sharing platforms. As such, the paper looks at some of the ways Daesh sympathisers have been using popular online storage websites to multiply the content online along with their use and calls for popular hashtags to be used when sharing Daesh material on Twitter.

**Key Takeaways**

- Daesh are involved in a coordinated and sophisticated campaign of hashtags and @reply hijacking
- Analysis has shown that Telegram accounts provide activated accounts for Daesh supporters to disseminate material on Twitter
- Telegram accounts instruct Daesh about dissemination strategy, trending hashtags and potential target profiles

"ISIS Culture on Telegram"
*Chelsea Daymon (American University)*
@cldaymon
Culture is an instrumental element in understanding the ecosystem and functions of a group. Culture provides unity, identity, and belonging, while helping to define shared patterns among members. Definitions of culture vary; however, it can be agreed that culture helps shape the customs, beliefs, and social behaviors of individuals, making it a powerful component for understanding groups. Despite its loss of territory, supporters of the Islamic State of Iraq and al-Sham (ISIS) are still active on the encrypted messaging platform Telegram. Official and semi-official channels continue to disseminate breaking news announcements, magazines, videos, photo reports, and other informational products, while pro-ISIS chats expand on these by offering a hybrid version of jihadi culture found in the online environment. There are cultural similarities between the online and offline environments, while there are also differences. Understanding jihadi culture in the online setting, is of vital importance since terror groups are utilizing platform like Telegram at an unprecedented rate. One could even argue that with its loss of territory, online jihadi culture, helps sustain ISIS in the long-term ensuring a continuation of ideas, support, and mobilization, which future groups will learn from.
"Investigating the digital caliphate on Telegram platform through the digital ethnography: from jihadi multi-level propaganda to a multi-actor service network"
*Nicolò Giuseppe Spagna (Catholic University of Sacred Heart in Milan)*
The study analyses the pro-IS digital movement on Telegram platform through the digital ethnography approach. This study is a small part of a more extensive ethnographic research on Telegram in which the process used to collect information has involved a covert participant observation within the digital platform that took nearly two years. The proactive monitoring has

permitted to capture how jihadist movement protects its virtual network. Indeed trust-building process, based on the linguistic-religious and the cooptation system, has emerged as relevant in this respect. This study also focused on one of the main extensive service provided in the digital caliphate – lone-actor terrorism instructional materials – underlining a new rising trend of remote-controlled terrorism called "Terrorism on Demand". It has been also observed that the jihadi extremists consider Telegram platform not a simple messaging application, but an extension of the caliphate – a jihadist service provider - that provides several services to users. Telegram platform plays a key role in communication amongst IS supporters generating an ecosystem based on a multi-actor service network. Finally some considerations have been made in relation to the use of covert participant observation as a precious tool to penetrate and gain a better understanding of terrorist digital communities that would not be otherwise possible to study

**Key Takeaways**

- "Terrorism on Demand" summarizes a new model of an underground remote warfare that has been observed on pro-IS Telegram net through digital ethnography.
- Digital caliphate on Telegram acts as a multi-actor service network. Multiple actors work as interconnected networks providing services in a collaborative way. Social informal control helps to protect pro-IS Telegram net, increasing also its resilience.
- Keeping one-step ahead of terrorists requires an understanding of their social habits by exploiting their social vulnerabilities. Digital ethnography is a powerful tool to collect interpretational keys in this way.
- "Think like a terrorist" is a practical way to face terroristic issues. Evolution of terrorism is fast. It's time to question our methods and tools in order to develop efficient counter-terror measures.

## Panel 2C: South and South-East Asia

"Myanmar's Media-Savvy Monks: How Buddhist Extremists Harness Social Media to Incite Anti-Muslim Violence"

*Teresa Barros-Bailey (Moonshot CVE) and Franz Josef Berger (Moonshot CVE)*
@tbarrosbailey & @franz_j_berger

The violent extremism of Buddhist ultranationalists poses an imminent threat to ethno-religious minorities in South and Southeast Asia. In Myanmar, the 969 Movement and its leader, Ashin Wirathu, known as the "Buddhist bin Laden", have traditionally used 'mainstream' platforms such as Facebook as a conduit through which to spread alluring disinformation myths and hate speech about ethno-religious minority groups, particularly Muslims. Facebook came under fire in early 2018 for the actions of these extremist monks, who were using the platform to spread hate and encourage violence towards the Rohingya Muslim minority. Since then, Buddhist violent extremists in Myanmar have faced expulsion from the mainstream platforms they have until now relied on to aid their cause. This paper explores how Buddhist violent extremists have historically harnessed the power of social media to incite anti-Muslim violence in Myanmar, and how they have responded to the increasingly aggressive policies of the same social media platforms. We will present new primary data, gathered using Moonshot CVE's proprietary technological tools, to shed some light on the social media activities of Buddhist extremists and their audience in Myanmar. In doing so, we aim to determine whether suspensions of accounts have been successful in purging Buddhist violent extremist material in Myanmar, or whether they have simply pushed content onto other platforms.

**Key Takeaways**

- 38% of Myanmar's population have joined Facebook since 2011. Buddhist extremists have capitalised on this golden opportunity by deliberately spreading anti-Muslim hate further and faster than ever before.
- If Islamic State is paying attention to Buddhist violent extremism, then we should be too.

"Evaluating local efforts in Mindanao to confront Islamic State East Asia 'influence operations'"
*Haroro J. Ingram (George Washington University Program on Extremism)*
@haroro_ingram
In the aftermath of the Maute-Hapilon led siege of Marawi, Philippines in 2017, local civil society groups mobilized to confront Islamic State East Asia (ISEA) 'influence operations' across Mindanao. The case of Islamic State East Asia in the Philippines offers important insights into the interaction of top-down (e.g. Islamic State outreach to the region) and bottom-up (e.g. local actor outreach to Islamic State) forces and its implications for how local civil society combats these threats. Drawing on the findings of an 18-month study, this paper analyses the campaign, message, roll-out and evaluation design of two civil society run campaigns that fused offline and online efforts to confront violent extremist influences in their local areas. It then presents the 'reach' and 'impact' evaluation results for each campaign and identifies key 'lessons' for scholars and practitioners.

**Key Takeaways**

- It can often be difficult to convince western C/PVE practitioners and scholars that strategic communications, i.e. persuasive communication towards a strategic goal, is an important tool for countering and preventing violent extremism. We have had no such difficulties in Mindanao. It says a lot, I think, that those who witness violent extremism largely through a computer screen thousands of kilometres from any actual threat should flippantly dismiss the importance of persuasive communication while those whose lives depend upon it being effective for their survival embrace it.
- Effective training must achieve more than just the understanding of our strategic communications methodology and an ability to practically apply it. Shaping the mentality of individuals and the culture of teams is equally important. Our strategic communications workshops emphasise the importance of being persuasive, methodical and evidence-based. This requires competency in the method but also the right mentality and culture.
- In less than two years our team have rolled-out strategic communications training to over 525 P/CVE and peace advocates across Mindanao. We have a comprehensive system of 'learning impact', 'retention' and 'application' evaluations to monitor the effectiveness of our C/PVE strategic communications capacity building effort. As you can see from these 'learning impact' results, 5-10 times as many workshop participants are able to answer basic competency questions accurately after receiving our strategic communications method. This highlights both a severe deficit in basic competencies amongst C/PVE and peace advocates in Mindanao but also the effectiveness of the training.

"Indonesian online extremism: latest trends and techniques"
*Mark Wilson (Jane's by IHS Markit)*
@M_DubU
Following a spate of terror attacks in May 2018, the Indonesian authorities renewed their online crackdown on Islamist extremism. However, open source research and social media monitoring indicates this crackdown has been only partially effective, with online Indonesian militants still able to spread their messages on various social media platforms and websites. This briefing will explore the ecosystem of Indonesian online extremism, looking at how militants operate online and how they are indirectly supported by a range of pro-jihad websites and organisations.

**Key Takeaways**

- The Indonesian online extremist community is made up of three parts: Online jihadists, pro-jihad websites and NGOs that mask their support for jihad through humanitarian work
- Telegram will for now remain the key platform for Indonesian supporters of Islamic State, but this may change, with Indonesians beginning to experiment with decentralised social media networks like Minds.

- The longer-term threat may come from media outlets aligned with Jemaah Islamiyah, which while not overtly calling for violence, are building support for jihad through online religious outreach activities.

**Panel 2D: Engagement with online extremist content**

"Vulnerable or just having a laugh? Diverse youth responses to online violent extremism"
*Lise Waldek (Macquarie University) and Julian Droogan (Macquarie University)*
This paper presents findings drawn from empirical research conducted as part of an Australian Research Council (ARC) Discovery Grant into youth perceptions and engagements with online violent extremist materials. To date, the majority of research into online violent extremism conceived of the audience as passive and vulnerable, primed for radicalisation by virtue of cursory traits such as demographics or religious belief. Drawing from literature in the field of media studies that positions the audience as an active agent in the communication process, this paper prioritizes the voices of youth audiences (12 – 17). It explores the diverse responses to violent extremist content, and ways young people demonstrate resilience to exposure. The paper maps the findings from a survey of 1000 young people from across New South Wales, Australia, conducted in June 2018. The survey findings show that young people identify a range of media types and content as violent and extreme and access this material through a wide variety of platforms. Exposure to this material saw young people experience various emotions from anger through to humour and bragging rights. Responses ranged from sharing the material online, to deleting it and/or reporting it. Prioritizing the voice and experience of the usually silent audience, young people, provides insight into their levels of resilience to violent extremist messaging.

**Key Takeaways**

- Terrorism research into online violent extremism often silences the voice of youth audiences and assumes them to be passive and without agency.
- Young people identified a diverse range of content as violent and extreme.
- Youth audiences reactions to violent extremist content display complex emotions from anger to humour and bragging rights, which may suggest strategies of resilience to violent extremist content.

"Engaging with online extremist material: experimental evidence"
*Zoey Reeve (Newcastle University)*
@ZoeyReeve
Despite calls from governments to clamp down on violent extremist material in the online sphere, in the name of preventing radicalisation and therefore terrorism, research investigating how people engage with extremist material online is surprisingly scarce. The current paper addresses this gap in knowledge with an online experiment. A mock extremist webpage was designed and (student) participants chose how to engage with it. Several social psychological individual-level factors were included in the study. A mortality salience prime (being primed to think of death) was also included. Mortality salience did not influence engagement with the material but may have led to disidentification with the ingroup. Whilst interaction with the material was fairly low, those that did engage tended to indicate preference for hierarchy and dominance in society, stronger identification with the ingroup, higher levels of radicalism, and outgroup hostility. More engagement with the online extremist material was also associated with increased likelihood of explicitly supporting the extremist group. These findings show that indoctrination, socialisation, and ideology are not necessarily required for individuals to engage attitudinally with extremist material. This study is not conducted on the dependent variable, therefore shedding light on individuals who do not engage with extremist material.

**Key Takeaways**

- Most people do not engage with online extremist material, but those who do share certain traits that we would not know about by conducting research on the dependent variable.
- Extremist material can have the effect of promoting disidentification away from an ingroup, meaning that whilst it may promote radicalisation in some people, in most others it has an inhibiting effect.
- Engagement with extremist material online predicts explicit support for extremist groups. In the real world, this type of engagement/support may lead to further exposure to extremist material, and/or attention of recruiters/mobilisers.

"Exposure to Violent Extremist Content on Social Media: An Audience Perspective"
*Muneer Hamaid (Macquarie University)*
This paper examines how young people react to violent extremist content on social media. An analytical framework is adopted combining the Multistep Flow of Communication and Uses and Gratification Media Theories to interpret the agency of social media audiences. Data was collected using an incentivised online survey targeting a sample of Australian university students, which uses both qualitative and quantitative questions to explore a series of research questions:

- Do individuals actively seek online violent extremist content? What drives them to do so?
- What drives individuals whether or not to report violent extremist content to platform administrators?
- What is the extent of prevalence of the echo chambers and temporal compression phenomena?
- What is the extent of normalisation of exposure to violent extremist content in today's online experience?
- What content typology respondents perceive as violent extremist and why?
- What is the breakdown and intensity of the experienced emotive responses?
- How do individuals utilise social media functions and offline actions to react to online violent extremist content?

Early results suggest a relation between gender and the type/intensity of experienced emotive responses. A relation also exists between gender and the prevalence of echo-chamber/temporal compression effects. Overall, respondents cite a perceived lack of effectiveness/action on the platform's part as the most common reason for not reporting violent extremist content. Results also show that audience perception of what constitutes violent extremist content is widely varied.

**Key Takeaways**

- Right wing extremism has overtaken religious extremism as the most prevalent ideological type behind violent extremist content on social media today.
- Men aged between 18-25 are eight times more likely to experience amusement than women in response to viewing violent extremist content on social media.
- Some respondents report that the presence of graphic content warning drove them to consume content they would not otherwise consume.

## Panel 3A: Online terrorist financing

"Public-private collaboration to counter the use of the Internet for terrorist purposes: What can be learnt from efforts on terrorist financing?"
*Florence Keen (RUSI)*
In response to the use of social media and other online communication services for terrorist purposes, communication service providers (CSPs) face growing expectations to proactively detect, remove and/or report terrorist content. The emerging regulatory regime features significant parallels with global efforts to protect the financial system from terrorist financing. Under counter-terrorist financing (CTF) rules, financial institutions must take measures to prevent the use of their services for terrorist purposes and report suspicious activities. Based on a literature review and semi-structured interviews with representatives from both CSPs and the financial sector, this paper reviews how

lessons learnt from the CTF context can inform the response to the online terrorist threat. The paper analyses the unintended consequences of regulations; objectives for public-private collaboration, and the key elements required for a collaborative model.

"Crowdfunding Extremism: How Extremist Groups Use Crowdfunding Platforms"
*Shahed Warreth (Dublin City University)*
@libyenne_
While extremist groups are well financed, little research has been carried out on how they use crowdfunding to finance their causes. This research will explore the advantages and disadvantages crowdfunding poses to such groups, how crowdfunding fits into terrorist financing more widely, and how such campaigns are disseminated on social media.

**Key Takeaways**

- The periphery of Islamist extremism use framing techniques to try and align the worldview of the viewers with their own. Using diagnostic and prognostic framing the producers of legal content on YouTube use narratives of a Salafist-Wahhabist interpretation of Islam and hence can act as a gateway for some viewers to more extremist views.
- The network of the channels on YouTube forms an echo chamber that so far has not been penetrated by counter narratives. Several channels fulfil a function of a gateway to the periphery content, knowingly or unknowingly. Some of these actors may be strong allies in countering extremist narratives.
- The Islamist echo chamber on YouTube is enforced by the recommendation "Up next" algorithm. Counter narratives must try to penetrate this algorithm to have any real impact; otherwise, the target group will not be reached on the platform.
- Deleting channels in the periphery of extremism has the opposite of the intended effect. Content reappears on smaller channels and the deleted actor gains popularity.

"Researching Cryptocurrencies as a Source of Funding for Extremist Activities Online"
*Lorand Bodo (Tech Against Terrorism) and Benjamin Strick (OSINT analyst)*
@LorandBodo & @BenDoBrown
A vast majority of the literature on terrorism financing focuses on large terrorist organisations. Less attention has been given to extremist groups, particularly right-wing extremist entities. Even less is known about how these entities utilise cryptocurrencies to finance their activities. To this end, this study seeks to explore the role of cryptocurrencies in extremist financing to gain a more nuanced understanding of its appeal to right-wing extremist groups, as well as shedding light on the finance mechanisms used, to identify potential disruption-points. The ultimate goal is to develop a robust methodology for researching cryptocurrency-based finance activities employed by extremist entities online and to identify strategies to trace and find sources with start and end points of cryptocurrency financing. To do so, the Daily Stormer is used as a case study, in which various OSINT tools and techniques are employed and evaluated in terms of suitability. This project will cover the surface, deep and dark web to uncover as much as possible of Daily Stormer's cryptocurrency-based finance operations. To our best knowledge, this is the first study that explores cryptocurrencies as a source of funding for right-wing extremist entities and how these finance operations could be countered.

**Key Takeaways**

- The literature around terrorist financing focuses predominantly on Salafi-jihadist organisations
- In particular its methods to raise, store and move funds for financing terrorist activities as well as sustaining the group
- Less attention has been paid to XRW individuals/groups. In fact, "there has been as yet no attempt to understand how these individuals and groups raise funds" (Keatinge, Keen & Izenman, 2019: 12)

- The same is true for studies around XRW's use of bitcoins to finance extremist activities online
- Spreading hate costs money
- To research this topic, a methodology was developed for researching bitcoins as a source of funding for extremist activities online on all levels of the Internet (surface, deep and dark web)
- The two case studies presented have demonstrated the methodology's viability in terms of uncovering relevant information about fundraising activities through bitcoins
- To disrupt these activities, one of the key recommendations for social media and tech companies is to blacklist URLs that lead to donation instructions; blacklist particular BTC addresses as well as hash bitcoin QR codes

**Panel 3B: Gender perspectives**

"The Islamic State's Manipulation of Gender"
*Kiriloi M. Ingram (University of Queensland)*
@KiriloiIngram
This paper analyses how Islamic State's (IS's) propaganda construct, use and prioritise masculine and feminine norms and practices, and explores the interrelationship of both constructed models of gender. Furthermore, it situates these dynamics within IS's broader information operations strategy to mobilise a global audience and subsequently identifies why men, women, and their stipulated gender roles are imperative for IS as an organisation. I argue that IS constructs a Manichean perception of the world between the revered in-group and malevolent out-group. These bifurcated macro identities are subdivided into micro gendered identities, or male and female archetypes. These gender archetypes are used by IS to compel men and women to identify with in-group archetypes, to thus influence the formation of male and female audiences' identities in order to catalyse radicalisation and mobilise support for the in-group (IS). Moreover, there is a distinct symbiotic relationship between the use and prioritisation of male and female archetypes and this interdependence enhances the overall objective of IS's propaganda campaign: to offer audiences an alternative frame through which to understand the world and, to mobilise support for IS.

"Feminism is Killing Western Civilization: 'Manosphere' Logics and Far/Alt-Right Recruiting on YouTube"
*Ashley A. Mattheis (University of North Carolina at Chapel Hill)*
@aamattheis
This paper discusses the Far/Alt-Right use of "Manosphere" logics – ideology drawn from Men's Rights, Pick Up Artist, and Men Going Their Own Way online communities – in *YouTube* videos to mobilize their radicalization efforts specifically through constructions of gender. Here fears of white men losing control over white women's sexuality becomes the basis for promoting white nationalist extremism. These videos specifically leverage the misogynist and anti-feminist logics of the Manosphere to argue that the "real" threat to white men is immigration, globalization, and "Islamic" hatred of the West. Links between feminism and the "Islamic" threat are made through depictions of miscegenation – by choice or through violence – as an outcome of multiculturalism. Importantly, these videos use "flip board" imagery mimicking educational videos which pose extremist rhetoric as "truth" and "fact." I argue this format is persuasive to participants in Manosphere communities for two primary reasons. First, the videos' visual format generates a neutralized and seemingly fact-driven visual narrative. And second, because Manosphere and Far/Alt-Right ideologies share a gendered worldview. Ultimately, the Manosphere offers a useful site of radicalization for the Far/Alt-Right which can be seen in the increasing racialization of misogyny in Manosphere blogs.

"Gender in Online CVE Strategies: Maternalism, Absence and Lessons Learned"
*Elizabeth Pearson (Swansea University) and Morgan-Rose Young (Swansea University)*
@lizzypearson & N/A
That the online space matters in radicalisation to violent extremism is now a given. Authors have outlined how websites enable recruitment, fundraising, the fomenting of us-them identities, and the

distribution of terrorist propaganda. A number of studies, particularly of Daesh, additionally emphasise the ways in which males and females differ online in both behaviours and roles. Women can be more aggressive, taking advantage of online space as free of restrictive offline norms. They are secondary influencers when compared to men, but effective recruiters of other women. While offline projects aimed at Countering Violent Extremism (CVE) are a well-instituted aspect of global efforts to combat terrorism, particularly violent Islamism, online initiatives are a more recent intervention. Many offline CVE projects already focus on women, particularly as peaceful allies able to prevent male radicalisation. This paper explores the gender logic within online CVE strategy, considering the ways in which gender appears and is absent, the effects this produces, and how these might be addressed.

**Key Takeaways**

- Gender matters in violent extremism, so P/CVE has to think about gender
- Online P/CVE is more than just messages about women

**<u>Panel 3C: Smaller Platforms</u>**

"Gabs of Hate: Exploring Alternative Platforms of Hate on Social Media"
*Amarnath Amarasingam (Institute for Strategic Dialogue)*, Derek Silva (Western University), Ryan Scrivens (Concordia University) and Jade Hutchinson (Macquarie University)
Much research has focused on the presence and uptake of hate rhetoric in popular online spaces such as Facebook, Twitter, and Telegram. Much less discussed, however, is how online hate rhetoric is constructed, used, and disseminated throughout and across new, less well-known, social media platforms such as the Gab network. Gab is an alternative to Twitter that was explicitly founded on notions of free speech where users are able to read and write messages of up to 300 characters, referred to as "gabs." Many high-profile right-wing commentators and extremists have taken to Gab, including former Breitbard writer Milo Yiannopolous and Richard Spencer. Indeed, Gab has been described in the popular press as the "Twitter for racists" and a "safe haven" for white nationalists. Drawing on a sample of Gabs that were hosted by the Gab network in Canada, the US, UK, and Australia, we explore the ideological and geographical landscape and presence of extreme-white rhetoric online, critically evaluating the presence and uptake of hate speech, the use of violent rhetoric online, and the similarities and differences of online content between Gab and other social media platforms. Our findings suggest that despite some notable similarities in hate speech on Gab and other, more traditional, social media platforms, the network offers us key insights into how the right mobilizes quickly and promulgates hate speech in emergent online spaces. Appreciating both similarities between Gab and other platforms, as well as key distinctions, will tell us much about groups in these countries adopt new platforms and platform strategies in order to give some insight into craft interventions to counter them.

"Following the whack-a-mole: Britain First's visual strategy from Facebook to Gab"
*Lella Nouri (Swansea University), Nuria Lorenzo-Dus (Swansea University) and Amy-Louise Watkin (Swansea University)*
@ctproject_lella, N/A & @ctproject_ALW
The old adage claims that as soon as something is removed from the internet it pops up somewhere else. On 14 March 2018, Facebook banned Britain First from its platform, reasoning that they had "repeatedly posted content designed to incite animosity and hatred against minority groups" (Guardian, 2018). Subsequent to their removal, they created an official Britain First Gab page in May 2018. So, why have Britain First decided to migrate and post on another open platform? The obvious answer can be linked to the successes the group reaped on Facebook, which are not to be overlooked. However, they lost these followers, due to their removal and ban, so they obviously had a desire to recreate that follower community elsewhere. The key question therefore is: Why Gab? Gab does seem like a smart choice considering their removal from other more mainstream sites such as Twitter (December 2017). Moreover, Gab is more lenient than Facebook or Twitter, with its ethos centred on promoting free-speech and privacy and fighting against censorship. This raises some questions,

though: Could Britain First's use of Gab become as prolific as that of Facebook? What effect may their communicative tactics have in terms of followers' reactions? Would their simple 'like' and 'share' strategy with Facebook posts such as "share if you love England" or "like if you are against animal cruelty" achieve the same results on Gab? In particular, this study explores the effect that Facebook's removal of their official page has had on their visual communication strategy, specifically their choice of images. Our study examines (i) trends in terms of the types of images used and which ones were most successful on Facebook and; (ii) if, and if so, how their use of images has changed with the move to Gab.

"Infinite (8)Chan: Analysing Far-Right Extremist Responses to the Christchurch Attacks"
*Suraj Lakhani (University of Sussex), Maura Conway (Dublin City University)* and Susann Wiedlitzka (University of Sussex)
@surajlakhani, @galwaygrrl & N/A
The live-streamed attacks by Brenton Tarrant in March 2019, in two Christchurch mosques, left 50 dead and many injured. Although Tarrant's video has largely been removed from major social media platforms, the material is openly viewed and shared on other publicly available online spaces. One of these is 8Chan (or Infinite Chan), a website that allows anyone to create their own anonymous multi-content 'imageboards'. In fact, shortly before the mass shootings, Tarrant posted a live-stream Facebook link on 8chan. The space was also used to spread and praise Tarrant's manifesto. However, to date, little research has been undertaken on the platform. This paper will discuss key findings from an exploratory piece of research on 8Chan, undertaken in the aftermath of the New Zealand attacks. Preliminary research findings have indicated the presence of online 'communities of support' for Tarrant's actions, which could, hypothetically, be used as part of narratives for future acts of violent extremism. The research also demonstrated the existence of subcultural threads, whereby, similar to arguments on jihadi-cool, there are various existential attractions towards involvement with far-right extremism. Finally, the findings indicate that rather than displaying sympathy towards the victims of the attacks, certain posters victimised the victims.

## Panel 3D: Africa

"Boko Haram's Online Presence: An Overview"
*Bulama Bukarti (Tony Blair Institute for Global Change)* and Mubaraz Ahmed (Tony Blair Institute for Global Change)
@bulamabukarti & @MubarazAhmed
The study of terrorist groups' use of the internet has largely neglected the online presence of Boko Haram, whose internet-based activity stretches back to 2010, while the group's militant activities have burgeoned beyond Nigeria and spread across the Lake Chad Basin. This paper seeks to draw the attention of academics and policymakers to the vast plethora of Boko Haram content that remains available online, in spite of international efforts to tackle terrorist groups' exploitation of the internet. It will present an overview of the evolution of Boko Haram's online activity, looking at how the group has used social media platforms for recruitment and propaganda purposes, the role of mainstream media outlets in amplifying the group's messaging, and identifying the significant ideological features of the group's propaganda. The paper will also examine the online activity of Boko Haram's different factions, exploring the types of content they are producing, the platforms they are using, and delving deeper into the output of the factions, in particular looking at how online activity fits with the group's broader strategy and objectives. Concomitantly, it will assess the current level of response from governments, tech companies and civil society organisations to the group's online activities.

### Key Takeaways

- Boko Haram's online presence remains a blind spot despite the group's robust virtual presence that stretches back to 2011.

- Although the group does not currently have official online account(s), there are several channels hosting its contents as it leverages messaging apps to coordinate with members and with ISIS.
- The study of terrorists' use of the internet must be broadened to incorporate a greater focus on the sub-Saharan African context.
- Media outlets must bear greater responsibility for reproducing often uncontextualized and unredacted Boko Haram propaganda.
- Tech companies should ensure greater consistency in the application of community guidelines across all geographic and linguistic contexts.

"Ansar al-Sharia in Tunisia's Facebook Mobilization"
*Aaron Y. Zelin (Washington Institute for Near East Policy and Brandeis University)*
@azelin
The 2011-2013 time frame at the outset of the Arab uprisings and before the reemergence of the Islamic State is an overlooked period in the literature on jihadi media usage, strategy, and mobilization. While most historic groups aligned with al-Qaeda remained glued to password-protected forums and subsequently adopted Twitter and Telegram in 2013-2015 for official media distribution, new 'Ansar al-Sharia' groups that were founded after the uprisings began to use Facebook. One case in particular is unique: Ansar al-Sharia in Tunisia (AST). AST was not based in a war zone, but in a transitioning democracy. AST was not using terrorist tactics, but attempting to conduct dawa and social service activities. AST was not a group operating as minority Muslims within society as European jihadi dawa groups had been previously. It was very much a social movement, but unlike most social movements that attempted to garner more rights and justice within society, AST was attempting to build a theocracy and shadow state. Therefore, it is not an easily compare case amongst historic jihadi groups either within the broader Middle East conflict zones or homegrown movements in the West. As a consequence, AST's Facebook campaign had a different type of relationship to members of its group, the broader Tunisian public, as well as the global jihadi community. It allowed for different types of connections and interactions not possible with a clandestine group, one closed off to the dark corners of the Internet, or not open to society. This provided different dynamics for recruitment, mobilization, and interaction locally, which helped to strengthen bonds and connect individuals amongst current and new members of the organization that was not previously possible or has really been seen since within the jihadi milieu.

"Propaganda or Not? The Persistence of the 'Al-Qaeda Narrative' in Boko Haram Studies"
*Jacob Zenn (Georgetown University)*
@BokoWatch
It has often been assumed that the public messages of Al-Qaeda and Boko Haram about each other from as early as Usama Bin Laden's first mention of Nigeria in 2003 were bluster to exaggerate both groups' international and expansionist credentials. However, the emergence of primary source documents of the private correspondences between these groups now reveals that most of their public messaging, in fact, corroborated what the groups were actually doing behind-the-scenes. Why would al-Qaeda telegraph the financial and training support it was providing to Boko Haram when it could tip off intelligence agencies to their activities? This article theorizes that al-Qaeda understood that intelligence agencies were already tracking their activities and its public messaging served two specific purposes: first, to alert al-Qaeda and Boko Haram members not involved in leadership decision-making about al-Qaeda's forthcoming support; and, second, to confirm to leaders who were "in the know" that such support was bound by a public oath of commitment. The article contributes to the literature on al-Qaeda and Boko Haram and weighs in on the debate about whether primary sources from al-Qaeda and Boko Haram that are now published online are "propaganda" and academically unreliable or not. The articles also contributes to providing methods that analysts can use to distinguish between "aspirational messaging," which is a form of propaganda, and "operational messaging," which reflects actual operational activities.

**Key Takeaways**

- Boko Haram "cinematography" revealing clues about which factions are taking control at this current time of leadership shifts
- Primary sources emerging from AQ on social media revealing new clues about Boko Haram's origins that require further investigation.

**Panel 3E: Online ISIS propaganda and radicalisation**

"Between the 'camp of falsehood' and the 'camp of truth': exploitation of propaganda devices in the *Dabiq* online magazine"
*Miron Lakomy (University of Silesia)*
The paper discusses results of a research project which aims to identify the most important propaganda methods exploited in the former flagship magazine of Daesh - *Dabiq*. The content analysis was based on the Institute for Propaganda Analysis' concept of propaganda devices. It consisted of seven devices: name-calling, glittering generalities, transfer, testimonial, plain folks, card-stacking, and bandwagon. The research project adopted both qualitative and quantitative approaches. This paper argues that name-calling and glittering generalities, based on the use of "bad names" and "virtue words," were among the most frequently used, in order to create a black and white vision of the world, composed of only two groups: the camp of truth (i.e. IS) and the camp of falsehood (infidels *en masse*). Transfer, which is defined as the use of the authority of someone widely respected, was also commonly exploited in all issues of *Dabiq*. It was manifested by frequent references to the Quran, Allah's commands, the Prophet's and Sahabah's actions (being "role-models"), as well as to Islamic scholars. This was done to present IS as the only "true" embodiment of the caliphate. Bandwagon, based on the use of the "follow the crowd" logic, was usually manifested by suggestions that masses of Muslims support IS and celebrate its victories. Card-stacking, defined as obvious lies, as well as testimonials, were noticeable, but much less frequent. Finally, the rarest and least important device was plain folks, whereas the *mujahidin* in the magazine were predominantly presented as unique and extraordinary Muslims.

**Key Takeaways**

- Dabiq stigmatized enemies of Daesh and presented them in a degrading way, akin to Nazi propaganda on "Untermenschen" in the Second World War
- It created an artificial black-and-white vision of the world, composed of the "camp of falsehood" and the "camp of iman"
- It conveyed a simple message: either you support the Islamic State, or you belong to the "camp of kufr," effectively becoming a target

"The online behaviours of Islamic State actors in America (2013-2018)"
*Joe Whittaker (Swansea University)*
@CTProject_JW
There is a considerable degree of ambiguity in Terrorism Studies and counter-terrorism practice surrounding the phrase "online radicalisation" – both in relation to the process of radicalisation itself, as well as how the Internet's role can shape it. This research adds to the dearth of empirical data by analysing the online behaviours of over 200 Islamic State terrorist actors in America, discerning their pathways into their eventual activity and assessing the role of the Internet in that pathway. Data were collected via open-sources including criminal justice documents, journalistic sources, government reports, and academic literature. Following on from the work of Gill et al. (2015), it disaggregates a number of behaviours that can be described as aspects of "online radicalisation" and offers a number of descriptive statistics and multivariate tests to offer insight on the role of the Internet in contemporary trajectories into terrorism.

"On Understanding Online Radicalism: A Case Study on ISIS Propaganda"
*Mariam Nouh (University of Oxford)*, Jason R.C. Nurse (University of Kent) and Michael Goldsmith (University of Oxford)
@Mary_n0, @jasonnurse & N/A
The Internet and Online Social Networks in particular have changed the way that terrorist and extremist groups can influence and radicalize people. Recent reports show that the mode of operation of these groups starts by exposing a wide audience to extremist material online, before migrating them to less open online platforms for further radicalization. Thus, identifying radical content online is crucial to be able to limit their reach and the spread of the extremist narrative. In this study, we identify several markers including textual, psychological, and behavioural, that together allow for the classification of radical content. We adopt a data-mining approach to computationally analyse extremist propaganda, determine a textual model of radical content, and create a psychological profile of known radicals. Our results show that radical users do exhibit distinguishable psychological properties. These properties can be utilized as signals for detecting radicalization activities. We believe that this approach will have significant implications on improving the existing efforts on detecting evidence of online radicalism and combat extremist narrative and recruitment campaigns.

**Key Takeaways**

- Using computational methods to analyze Dabiq propaganda reveals hidden signals that can be used for automatic detection of ISIS supporters.
- The main drive for the ISIS group as conveyed by the analysis of 14 Dabiq issues is power, which is expected since they aim to recruit and attract individuals.
- Propaganda published in Dabiq shows confidence and formal logical thinking style. Adopting this style of writing for the propaganda material may reflect why they have been successful in their recruitment campaigns.
- Analysis show that the dichotomy mentality of us-vs-them is reflected in the Dabiq articles. With high focus on the 3rd person pronouns (they, she, he) as opposed to less focus on the use of 1st person pronouns (i, we).
- The use of the second person pronoun (you) is higher compared with other pronouns. This shows that the strategy of these magazines in putting the focus and emphasis on the reader.

## Panel 4A: Threat Assessment

"Analysis of written online content as part of structured behavioral risk analysis in the field of religiously motivated terrorism"
*Dominik Irani (Bavarian State Criminal Police Office)*
With the rising numbers of individuals who have been identified as being high risk cases or potential high-risk cases in the field of jihadism and the unfolding of the Syrian conflict, threat and risk management in these cases have become ever-increasing challenges for security services. The first step of risk management is risk assessment. There are numerous screening tools in operation as a first step of risk-assessment. In identified high-risk cases an individual risk assessment is conducted as a second step. Risk assessment is based to large extents on the analysis of an individual's behavior and especially recurring behavioral patterns. With nowadays increasingly blurred lines between offline and online behavior and a significant shift from face-to-face interaction towards virtual group dynamics, the data that serves as a basis for the analysis tend to include an increasing amount of online content and communication between individuals. From the analysis of this written online content and communication important conclusions can be draw concerning an individual's communicative behavior towards others and in groups, the role an individual tends to take within groups and the emotional state of the individual while communicating. While deductions regarding the risk an individual might pose or represent cannot be drawn solely from virtual written content, it seems to be an important piece of information to achieve a larger and more detailed picture of an identified high-risk individual.

"Understanding linguistic trajectories of YouTube's alt-right"
*Isabelle van der Vegt (UCL)*, Maximilian Mozes (UCL), Paul Gill (UCL) and Bennett Kleinberg (UCL)
@isabellevdv, @maximilianmozes, @paulgill_ucl & @benkleinberg
In recent years, alt-right movements have significantly grown online. Simultaneously, the world has been faced with terror attacks motivated by white supremacist ideologies. Online, these ideologies are widespread; YouTube has been referred to as a breeding ground for the alt-right. Reports have shown YouTube is rife with alternative "influencers", who behave not much differently than other popular YouTubers, besides the dangerous ideas they spread and the violent acts they potentially inspire. This study utilises a dataset of almost 60,000 YouTube video transcripts, extracted from known alt-right and left-progressive channels. We uniquely examine alt-right language use on a large scale and compare it to language use on more mainstream channels. A fully automated analysis of the video transcripts is performed to understand the linguistic trajectories throughout the videos and the potential differences between the two groups. We are interested in whether certain exogenous events have an effect on the linguistic trajectories in both groups. We investigate whether the deadly violence in Charlottesville (August 2017) is accompanied by differential linguistic patterns in alt-right and progressive videos. By doing so, we hope to gain a deeper understanding of the online alt-right community and potentially aid in finding ways to combat their dangerous message

"Identifying trajectories of Islamophobia amongst followers of the BNP on Twitter"
*Bertie Vidgen (Alan Turing Institute & University of Oxford)*, Taha Yasseri (Alan Turing Institute & University of Oxford), Helen Margetts (Alan Turing Institute & University of Oxford)
@bertievidgen, @TahaYasseri & @HelenMargetts
This paper examines Islamophobic hate speech amongst all Twitter followers of the BNP, a UK far right policy party (after cleaning, n = 6,406), over one year (2017-2018). We label the content of all their tweets (n = 5.51 million) using an Islamophobia detection classifier which distinguishes between 'Weak' forms of Islamophobia, which are primarily subtle and nuanced, and 'Strong' forms of Islamophobia, which are primarily overt and aggressive. We find that the majority of Islamophobic tweets are Weak rather than Strong (10.8% compared with 5.3%). We then use this labelling to assign users to one of six trajectories of Islamophobia, identified inductively using latent Markov modelling. These trajectories are: Never (n = 1,843), Casual (n = 2,028), Extreme (n = 976), Escalating (n = 382), De-escalating (n = 313) and minor de-escalating (n = 864). This model can then predict the aggregate number of users who engage in different strengths of Islamophobia over time. This research challenges the longstanding view that far right Twitter users comprise 'walls of hate'. Rather, the far right is highly heterogeneous, with users exhibiting markedly different behavioural trajectories.

## **Panel 4B: Understanding the Radical Right**

"You Will Not Replace Us: Hate Speech and Extremism Among Sovereign Citizens and the Alt Right in the United States"
*Michael Waltman (University of North Carolina at Chapel Hill)*
I propose to study hateful discourse produced by Sovereign Citizens and the "Alt Right" on social media platforms in the United States. Hate speech often leads their targets along a path that radicalizes them by (a) constructing a valued ingroup as significant, (b) constructing outgroups in stigmatized and stereotypical terms, (c) constructing the stigmatized outgroup as a threat to the ingroup, and (d) invites the ingroup to take pleasure in the marginalization, suffering, or killing of outgroup members. Sovereigns and the Alt Right are chosen because: (a) they represent the most recently emerging manifestations of hate and terror groups in the United States, (b) they are groups actively engaged in violence against individuals and institutions in the U.S., and (c) they share a certain "kinship" in that they blend nationalism with hatred of outgroups and the Federal Government as an ideological foundation for their terror and extremism. This discourse will be mined from YouTube, social media outlets, and Web Pages these groups employ to communicate their beliefs and activities. The final report of this project will illustrate how Sovereigns and the Alt Right use hateful discourse to radicalize their followers and promote violence against their enemies.

"Virtual Tug of War: A Socio-Technical Analysis of Online Alt-Right and Alt-Left Propaganda"
*Ashton Kingdon (University of Southampton)*
@AshKingdon
Social Media is one of humanity's most liberating innovations, yet has become a virtual forecourt for extremists who seek to radicalise, recruit, and disseminate propaganda, effectively transforming this technology into a vessel for hatred and violence. The research presented here combines the academic disciplines of Criminology and Computer Science to explore the socio-technical aspects of both left and right-wing online radicalisation, giving equal weight to both the influence of technology and the subcultural elements of its users. Methodologically, this paper centres on a comparative semiotic content analysis of propaganda images, in order to explore the ways in which extremists from contrasting sides of the political spectrum utilise the technology of social media to sow the seeds of dissonance, reinforce existing prejudice and target those who feel marginalised or hold an existing grievance. Utilising evidence collected from Twitter, YouTube and 4Chan, this paper argues that the burgeoning ideological divide within contemporary society, is not solely based upon societal and political upheaval, but also the ability of social media platforms to create and promote ideological echo chambers, which, in turn, accentuates the need for increased algorithmic transparency and accountability. Ultimately, this paper argues that when it comes to extremism the technology of social media is inherently neither good, nor bad, but it is not neutral either, and whilst machine learning algorithms can lead people further down a radicalisation rabbit hole, these technological mechanisms cannot be considered in isolation from the subcultural elements that surround the users of this technology.

**Key Takeaways**

- The power of the image within extremist propaganda cannot be ignored! We need more Visual Criminology to examine the subcultural elements of radicalisation
- AI has led to the creation and promotion of ideological Echo Chambers that accentuate the increased need for Algorithmic Accountability and the development of Responsible AI
- AI will always be embedded within a socio-technical context, to successfully counter extremism we need to combine the best of Human Intelligence and Machine Intelligence

"Like, Share, Hate: Exploring Australian and Canadian Far-Right Extremism on Facebook"
*Jade Hutchinson (Macquarie University)*, Amarnath Amarasingam (Institute for Strategic Dialogue), Derek Silva (Western University) and Ryan Scrivens (Concordia University)
@JadeHutch00, @AmarAmarasingam, @derekcrim & @R_Scrivens
As two nations that share cultural, political, and economic synergies, Canada and Australia have experienced an uptick in right-wing extremist activity as of late, from organized hate rallies in urban centres to a growing presence on social media platforms such as Facebook. Common sentiment that has been shared across these movements is a need to defend national and Western identity and culture from what adherents argue is the twin threat of unchecked immigration and the proliferation of Islam. Recent studies have described this ideological narrative as that of the 'new radical right', particularly in an Australian context. Little, however, is known about how this ideological shift is being experienced in a Canadian context. Drawing on a sample of Facebook pages that were hosted by Australian and Canadian right-wing extremist groups, we explore the ideological landscape and presence of both extreme-right factions online, evaluating the popularity of the group pages, the content that they post, who is targeted and how the use of violence is negotiated, and the socio-cultural similarities and differences of the online content. The results suggest that, although the Australian and Canadian extreme-right movements share broad commonalities, unique distinctions exist between the two. Understanding these distinctions will tell us much about how right-wing groups in these countries may evolve going forward and provide some insight into how to counter them.

**Panel 4C: The technology underpinning social media**

"The Technology Powering GIFCT's Industry Efforts"
*Lakshmi Mounika Bodapati (Facebook)*
In 2017, the UN General Assembly released a statement that "Terrorist use of the internet to incite, inspire, and direct terrorist and violent extremist acts is one of the most pressing issues the global community faces." Not only did they explicitly call out that it was specifically their use of the Internet, but they went on to say that it required a global response – a global response where not only governments but also *social media companies* had a part to play. Tech companies already have teams of people to address this problem and protect their own users. But what if we as an industry worked together to make the entire Internet safer? What can companies do to help each other? This talk focuses on the technical platform called ThreatExchange we built for the Global Internet Forum to Counter Terrorism (GIFCT). We will explore examples of problems like harmful content that actually lives on another platform (a Facebook post that's actually a share of a reddit post URL, a tweet on Twitter that's actually a YouTube video, etc) and harmful photos/videos that are uploaded to multiple platforms. I'll dive into two specific initiatives, hash-sharing and URL-sharing, that aim to address these problems, and talk about how this data sharing fits into Facebook's approach to dealing with this kind of abuse to not only make its own platform safer but the whole Internet as well.

"The Effects of Social Media Personalisation Algorithms and Extremist Content"
*Fabio Votta (Stuttgart University), ashton Looney (Swansea University),* Joe Whittaker (Swansea University) and Alastair Reed (Swansea University)
@favstats; @_Sean_Looney_, @CTProject_JW & @reed_alastair
Social media platforms and the algorithms that drive them are now an inescapable part of contemporary life. They are responsible for the content that users see in their feeds; the content they are recommended; and the products that they are advertised. Despite this, little is known about their operational workings or their effects on users. This is even more the case with regards to extremist content and their role in trajectories towards terrorism. In this research we offer an exploratory analysis of three social media – YouTube, Reddit, and Gab – platforms' recommender systems when put into contact with far-right extremist content. We find evidence that only one platform – YouTube – indicates a prioritisation of extremist material by the recommender system. We offer a number of interpretations of the results and give a number of policy recommendations.

**Key Takeaways**

- There is a paucity of research studying the effects of personalisation algorithms on extremist content. We set out to ask: Do algorithms promote extremist material once a user begins to interact with such content?
- Our research design analyzes frequency & order of extreme content on YouTube. We find that after YouTube users engage with such content they are more likely to be recommended more. Extreme content is also found to be higher ranked after interaction.
- We recommend the following policies to tackle the issues revealed in our study:
  1. Removing Problematic Content from Recommendations
  2. Ensuring Video Recommendations are from Quality Sources
  3. Greater Transparency on how Algorithms prioritize & recommend Content

"What Does the Study of Platforms' Affordances Tell Us About the Workings of Contemporary Online Extremism and Terrorism?"
*Sam Jackson (University at Albany) and Maura Conway (Dublin City University)*
@sjacks26 & @galwaygrrl
Over the past several years, a substantial body of research has developed investigating extremism and terrorism online. Despite this, scholars have not yet begun to investigate how the functionalities of different online platforms affect online extremism and terrorism. Social media research has long pointed out that platform affordances (such as synchronicity vs. asynchronicity, anonymity, and whether multimedia like images or videos can be used) directly shape what users do on those

platforms. As they shape what users can do, affordances also constrain the purposes that platforms can serve. For example, some platforms (like Telegram) that offer greater privacy and security might serve as tools for coordinating illegal activity, but these platforms are less likely to be useful as initial recruitment sites. In this paper, we set out an agenda to systematically investigate the relationships between platforms, affordances, and online extremism and terrorism. We present early findings about the different purposes (for example, recruitment, operational planning, trolling, and ideological indoctrination) for which extremists associated with different ideologies and active in different parts of the world use different platforms (such as Twitter, Telegram, and forums), analyzing how the features of each platform affect how extremists use it

**Key Takeaways**

- Extremists use different platforms for different purposes.
- The affordances of different platforms shape and constrain what purposes each platform can be used for.
- Cultures and norms among users are just as important as technical features in shaping how platforms are used.

**<u>Panel 4D: Islamic State media output</u>**

"Determining the 'Stateness' of Islamic State According to their Video Propaganda"
*Moign Khawaja (Dublin City University)*
The birth and existence of the "Islamic State" generated a lot of international controversy, both in terms of its "Islamic" identity and its functioning as a "State." While the Islamic aspect of IS has been highly debated, the state aspect needs to be challenged. IS supporters argue their state had its own borders, government institutions, army, and a powerful media, just like any other modern state. They also insist that almost all modern states came into existence out of terrorism and it is not just unique to IS. Many experts agree that the most accepted requirements for determining the existence, hence legitimacy, of a state in international law is the following criteria stipulated in the 1933 Montevideo Convention on the Rights and Duties of States: i) a permanent population, ii) a defined territory, iii) an effective government, and iv) a capacity to enter into relations with other states. Taking these criteria into account, can the "Islamic State" be recognised as a sovereign international state? Did the "Islamic State" manage to fulfil the statehood conditions expected from any modern state? My research aims two following objectives (i) address IS statehood claims by contrasting their propaganda videos which showcased its claims of running an effective government, depicted lifestyle of the population living within its territory, with established norms, theories and conventions of international law and diplomacy (ii) how IS effectively used social media to project its claims of statehood.

"The Islamic State Reader: Strategic communications lessons from Islamic State's Fall & Rise & Fall, 2007-18"
*Haroro Ingram (George Washington University Program on Extremism), Craig Whiteside (US Naval War College) and Charlie Winter (King's College London)*
@haroro_ingram, @CraigAWhiteside & @charliewinter
Despite the flood of research that has emerged since the establishment of its so-called "caliphate" in 2014, persistent myths continue to shape public understanding of the movement now known as the Islamic State. Going beyond the descriptive and the sensationalist, our co-authored book *The Islamic State Reader* presents milestone doctrinal texts and media releases from Islamic State to trace the group's path from failed pseudo-state in Iraq to standard-bearer of the global jihad. In this paper we draw on this study to identify 'lessons' for not only understanding the group's approach to propaganda, especially its use of the Internet, but its implications for practitioners across civil society, public and private sectors responsible for combating the group's 'influence operations'.

**Key Takeaways:**

- You can't fake being serious about strategic communications. Everything we know about the Islamic State movement – from its origins in the late-1990s to today – demonstrates how seriously they take persuasive communications as not only a psychological and strategic tool but a tactical and operational one as well."
- "The most effective strategic communications campaign the West has ever launched related to the Islamic State movement is the one it has run on itself. The self-soothing myths and misconceptions that still persist to this day – despite all the blood, ink, money and treasure that has been spilled – is testimony to the effectiveness of that campaign. Returning to primary source materials, ensuring that not only are they accessible to scholars and practitioners but they have the methods to appropriately analyse them, will be crucial to improving both research and practice."
- "The ISIS Reader features milestone speeches and texts appearing in 15 chapters divided across four historical periods. It begins with al-Zarqawi's early speeches in the 1990s and ends with al-Baghdadi's 2019 address. This book not only seeks to tell the story of the Islamic State movement's rise and fall and rise and fall through its own words but demonstrate the importance of primary sources for improving our understanding and designing more effective strategies to confront violent extremism.

"Tackling terrorists' use of the internet: practical measures to support smaller platforms"
*Adam Hadley (Tech Against Terrorism)*
@techvsterrorism
This presentation provides an overview of Tech Against Terrorism's work with the website Jihadology, to implement a password requirement to access the most egregious content.

**<u>Panel 5A: Strategic communications</u>**

"Beyond Prevention: The Role of Strategic Communication across the four pillars of the CT Strategy"
*Alastair Reed (Swansea University) and Andrew Glazzard (RUSI)*
@reed_alastair & N/A
The role of strategic communications in Counter-terrorism and Countering Violent Extremism policy has been brought increasingly in focus following the recent rise to prominence of the Islamic State and their expert exploitation of extremist propaganda. Whilst much work has been done in this area, too date, strategic communications has so far largely been employed only to counter recruitment and radicalisation to extremist groups. This paper argues, that strategic communications has so far been underutilised in the fight against terrorism, and has far wider application across a holistic counter-terrorism strategy. The paper provides an analyses across the four pillars of the UK CT-Strategy, of Prevent, Protect, Pursue and Prepare, demonstrating where the application of strategic communications approaches can enhance the effectiveness of current CT policies.

"Online Counter-Narratives in East Africa: Successes and Challenges"
*Sara Zeiger (Hedayah)*
@sarazeiger & @Hedayah_CVE
Despite the relatively low internet access in most East African countries, the use of online and social media spaces for recruiting young people to join Al-Shabaab has the potential to grow in the coming years. This paper will investigate the use of counter-narratives in East Africa to prevent violent extremism in the online space. The paper will leverage the existing East Africa collection in Hedayah's Counter-Narrative Library, and draw out some recommendations for current and future online counter-narratives for the region. In addition, it will provide some preliminary analysis through 3 case studies of online counter-narratives in East Africa in terms of their effectiveness.

**Key Takeaways:**

- Despite currently low internet and social media access in East Africa, rapidly growing access presents a challenge for future CVE and countering radicalization and recruitment online
- Civil society in East Africa are beginning to use social media to develop counter-narratives to violent extremism—the more successful ones involve youth in their own solutions and content creation
- There is limited information about the actual impact of the campaigns in terms of influencing cognitive or behavioral change

"Countering violent extremist narratives online: lessons from offline countering violent extremism"
*Talene Bilazarian (University of Oxford)*
@tbilazar
The literature examining use of online counter-narratives to divert potential extremists from a path of violence highlights the importance of messenger credibility, interactive approaches, and the shaping of broader network contexts. However, counter-narrative efforts have often failed to integrate these insights fully into their digital campaigns. After reviewing several prominent counter-narrative initiatives in the United Kingdom and the United States, this article highlights lessons from offline efforts to counter violent extremism (CVE) that can be used to inform counter-narrative efforts online. First, CVE efforts benefit from using a networked approach where a range of individuals highly connected in their respective social networks are used to disseminate counter-narratives. Second, interactive, interpersonal messaging techniques help to remove obstacles to participation in CVE efforts. Third, counter-extremism messages and narratives are often better received when they relate to broader community concerns and priorities, rather than focusing exclusively on terrorism or violent extremism. Common challenges faced by both offline and online CVE are outlined, and the important synergies between these efforts examined.

**Panel 5B: Evaluating extremist online narratives and counter-narratives**

"Are they any different? Comparative analysis of propaganda by alt-right and jihadi extremists"
*Weeda Mehran (Georgia State University), Stephen Herron (Queen's University Belfast)*, Maura Conway (Dublin City University), Tony Lemieux (Georgia State University) and Ben Miller (Emory University)
@WeedaMehran, N/A, @galwaygrrl, @aflemieux & N/A
The Internet has been used as a safe venue for promoting political action, forging affiliations and propagating strategies by various groups taken from ultra-right movements to jihadi extremists. There is an extensive body of literature on how jihadi extremist and alt-right groups use the Internet to communicate with their supporters, disseminate their propaganda and promote their ideologies. Less is known about what sets the discourse of these seemingly different groups apart? What are the shared and different linguistic patterns used among the white supremacists and the jihadists? In this paper, we conduct a semiotic comparative analysis of online propaganda material by alt-right groups such as the American Renaissance, the Daily Stormer, Frontpage Magazine, Jihad Watch, Heritage and Destiny, Gates of Vienna, Knights of Templar International, and the propaganda by ISIS, Al Qaeda, the Taliban and Tahrik-e Taliban-e Pakistan. Our data corpus consists of more than 150,000 sentences collected from English online magazines and statements. We have applied an Information, Motivation, Behaviour Skills (IMB) framework to analyse differences between alt-right and jihadi extremist groups. The IMB model stipulates that social and cognitive factors such as knowledge, attitudes, and social norms influence the willingness to learn skills and change behavior. The paper highlights the similarities and differences of these groups' narratives particularly in relations to social, cognitive and psychological processes and drives such as achievement, power, rewards and risks.

"This is the picture Reddit Admins don't want you to see: Alt-right antagonism on mainstream social media"
*Sam Bernard (University of Sussex)*
@sgb_lite
In this paper, I will examine the playfully antagonistic relationship that many alt-right communities maintain with the mainstream platforms that sustain them. Using Reddit's The_Donald as a case study, I will explore how these spaces provide something of a border zone between the alt-right and the mainstream, facilitating the rise of personalities, humour and talking points from the depths of the Internet to wider significance. The_Donald's prominence on Reddit is central to its influence, but much of its visibility comes through deliberate attempts to irritate, troll, and otherwise antagonise the site's wider community and administrators. Users on The_Donald adopt an ambivalent, playful style of ritualised participation that makes full and effective use of Reddit as a platform for recruitment and coordination whilst continually evading an outright ban from the site – even as other, similar communities are routinely removed. This case study sheds new light on how communities like The_Donald are able to effectively utilise popular online platforms like Reddit in spite of - and perhaps partially because of - attempts by site administrators to curb their influence.

"@UKAgainstDaesh: Winning a Digital War?"
*Anna Kruglova (Queen's University Belfast)*
@Anna13058990
The question of ISIS online propaganda has been widely discussed by scholars. Significantly less attention is dedicated to attempts to counter this propaganda. While there are some works that look at the UK efforts to find an effective digital response to ISIS they normally just compare UK and US Twitter accounts but do not assess their effectiveness in relation to ISIS themselves. At the same time, since both ISIS-associated and UK-led accounts are essentially aimed at getting followers and effective delivery of their message to followers, all general criteria of successful social media marketing (followers engagement, consistency of posting, tags usage, finding the niche the balance of posting of original materials and retweeting and replying, conversational tone, right timing, visualisation, finding the style) can be applied to assess both sides' online strategy. The goal of this research is, therefore, to assess both ISIS and UK-led accounts against those criteria and make the conclusion about the effectiveness of their social marketing strategies. The general argument of this research is that the UK marketing strategy is much less effective than the one of ISIS even after the group's defeat. From its very creation, the UK's account suffered from several serious issues which have not changed over time. They are the following: 1) Boring content; 2) Very official style; 3) Lack of interactivity; 4) Lack of attractive visual representation; 5) The content targets Western audience rather than Muslims; 6) The strategy is not adapting to changes in ISIS-led social media

## **Panel 5C: Capabilities**

"The Roles of 'Old' and 'New' Media Tools and Technologies in the Facilitation of Violent Extremism and Terrorism"
*Maura Conway (Dublin City University)* and Ryan Scrivens (Concordia University)
@galwaygrrl & @R_Scrivens
We describe and discuss the roles of media tools and technologies in the facilitation of violent extremism and terrorism. Rather than focusing on how media report on terrorism, we investigate how extremist and terrorist groups and movements themselves have exploited various "traditional" and "new" media tools, from print to digital, outlining the significance that they have had on extremists' ability to mark territory, intimidate some audiences, connect with other sympathetic audiences, radicalise, and even recruit. We find that violent extremists and terrorists of all stripes have, over time, used every means at their disposal to forward their communicative goals. Also worth noting is that 'old' media tools are not extinct and whilst 'new' media play a prominent role in contemporary extremism and terrorism, 'old' tools—everything from murals to magazines—continue to be utilised in tandem with the former.

"Is Twitter a Gateway to Terrorist Propaganda? A Study of Outlinks Contained in *Rumiyah*-Mentioning Tweets"

*Stuart Macdonald (Swansea University)*, Daniel Grinnell (Cardiff University), Anina Kinzel (Swansea University) and Nuria Lorenzo-Dus (Swansea University)
@CTProject_SM, N/A, @CTProject_AK & N/A

This presentation focuses on the attempts by the so-called Islamic State (IS) to use Twitter to disseminate its online magazine, *Rumiyah*. Our previous work on this topic found that IS disseminator accounts were mostly young, had very few followers (sometimes none at all) and received few retweets. They were, in effect, throwaway accounts that were used to try and signpost users to copies of *Rumiyah* on other platforms. In this study, we build upon this previous work by examining this strategy in greater detail and evaluating its effectiveness. The dataset for the study consisted of a total of 11520 tweets that both mentioned the term 'Rumiyah' and contained an outlink. These tweets contained a total of 892 distinct outlinks. The presentation will detail the hostnames that were most commonly contained in these outlinks and the types of content that the outlinks led to, before examining in greater detail the 381 outlinks that led to a full-copy PDF of *Rumiyah*. Based on these findings, the presentation will conclude by evaluating Twitter's attempts to prevent its platform being used as a gateway to jihadist propaganda and identifying challenges facing policymakers seeking to suppress such content.

**Key Takeaways**

- Botnet activity plays a significant role in efforts to disseminate IS propaganda. GIFCT members should accordingly develop shared automated systems that use behavioural cues to block terrorist content.
- The large number of file sharing sites and smaller platforms in the study's dataset of tweets that both mentioned Rumiyah and contained an outlink shows the importance of expanding membership of the GIFCT.

"The 'Resistance' Online: Understanding Hezbollah's Presence on Twitter and Related Out-linking Practices"

*Alexander Corbeil (Concordia University) and Joshua Gillmore (security contractor)*
@alex_corbeil & @joshuagillmore

This research project aims to systematically analyze the presence of Hezbollah and its supporters on Twitter using their public communications with other accounts. By giving insight into Hezbollah's activity on Twitter and exploring out-linking practices to other social media platforms and web-based services, this research will contribute to the limited body of knowledge on Hezbollah's use of the online space. Research will employ mixed methods using Twitter's free to access application programming interface (API), scripting, and social network analysis. This approach will allow for the segmentation of Hezbollah's Twitter networks to explore how distinct groups of users contribute to the organization's strategic objectives through their interactions, shared content and out-linking practices. The "Resistance" Online will highlight the continued importance of Twitter to Hezbollah's political and military wings, showing how the organization and its supporters frame and regulate online conversations. In so doing, it will explore the specificities of Hezbollah's online activity. The project will also act as a case study of how certain terrorist organizations operate in a relatively permissive online environment and raise questions about how social media companies regulate their platforms.

**Key Takeaways:**

- Automated community detection and sampling methods are effective in identifying hard-to-reach communities, in this case Hezbollah members and the organization's supporters.
- Hezbollah members and supporters operate in a relatively permissive environment on Twitter, which may be due to exemptions to the platform's terrorism and violent extremism policy for groups whose representatives have been elected to public office through democratic elections.

- Users who are purportedly members of Hezbollah's military wing share common identifiers that are useful for communicating and for researchers, determining, in-group membership.

**Panel 5D: Computer-assisted methods and studies**

"On the methodology of application of the stochastic methods of analysis of big data from social networks to control of indicators of the violent behaviour"
*Viktor Pushkar (National Academy of Sciences of Ukraine)*, Yuriy V. Kostyuchenko (National Academy of Sciences of Ukraine), Maxim Yuschenko (National Academy of Sciences of Ukraine) and Olga Malysheva (National Academy of Sciences of Ukraine)
@YuriyKostyuche1
The task of analysis of separate aspects of group behavior and identification of indicators of violent, and especially, terroristic activity is describing. To this task solving the social networks data analyzed as the big data have been utilized. Taking into account an adaptive nature of studied community behavior, a stochastic approach to collection, filtration, regularization and analysis of multi-language data has been proposed. On the base of the proposed approach the number of algorithms was developed aimed to classification, clustering and analysis of data. Few important tasks might be solved using the developed algorithms. For example, after application of this algorithm groups with violent behavior could be identified. Using the proposed approach the available statistics could be integrated with data from varied sources and correctly divided to different network groups: local support community, international support groups, network propagandists, and illegal armed group's members. As the result of application of the classification algorithms we obtain a dataset with all records that meet the condition we specified. For example, distribution of members of community "foreign participant of illegal armed groups" with age, sex, social status, accessory, spatial and temporal marks inside the general community of members of illegal armed groups' combatants. It is important to note, that using described algorithms, it is possible to obtain regularized spatial-temporal distributions of investigating parameters over the whole observation period with rectified reliability and controlled uncertainty. Proposed algorithms were applied for the number of cases of conflict studies in Ukraine and Syria in 2014-2017.

"What about the private sector? A closer look at how private organizations employ social media analysis to detect the terrorist threat"
*Gianluca Riglietti (PANTA RAY) and Kamal Muhammad (The Business Continuity Institute)*
@GianlucaRigliet & N/A
Terrorist organizations are making an increasing use of social media to plan attacks, recruit new members and spread their ideas. Some of them even went as far as to form a dedicated cyber unit, as in the case of the Islamic State's United Cyber Caliphate. As a response, governments are dedicating resources to monitor the terrorists' presence on social media. While these efforts are useful and necessary, they can still fail to cover the full spectrum of the threat. Security agencies stress the importance of community involvement in the detection of the terrorist threat, with initiatives such as the UK's ACT. Following this principle, it seems interesting to explore how private organizations can provide an extra layer of security, both for themselves and the community, by employing modern detection tools such as social media analysis. This is particularly significant as terrorism remains one of the main threats to organizations and terrorist groups become more sophisticated with the use of technology. Hence, this presentation will aim to show a series of case studies of how private organizations adopted social media analysis to understand the online sentiment regarding this specific threat. This will be done by asking organizations and experts that have been actively involved in the analysis to share their experiences. A content analysis of the case studies will then lead to an examination of the methodology and the significance of the results achieved by the organizations included in this study.

**Key Takeaways**

- Social media platforms play a key role in the gathering and sharing of information during a crisis. Several private organizations rely on them.

- One of the future challenges for social media platforms will be to step up and make their services more reliable during a terrorist incident.
- It is key that organizations learn how to filter through the social media noise during a terrorist attack to gather valuable intelligence.

"Cross-domain perspectives on online hate speech"
*Tom de Smedt (University of Antwerp) and Sylvia Jaki (University of Hildesheim)*
@tom_de_smedt & @sylviajaki
Recent years have witnessed a surge of hate speech on social media and hate crimes that are perceived to be related, such as ISIS terrorist attacks, the recent extremist riots in Chemnitz, and the male supremacist Toronto van attack in April 2018. Using the latest advancements in Machine Learning and Natural Language Processing, it is possible to identify hateful content online in real-time. For example, we have developed systems to detect jihadism, extremism, racism, and misogyny, by harnessing stylistic cues in (anonymous) authors' writing style. Such techniques are known in academia as stylometry, and in law enforcement as forensic linguistics. While the aforementioned domains are vastly different, there are striking similarities in the way in which all instigators employ language. In this talk, we offer a comprehensible overview of the language technology we have developed, and we discuss legal and ethical implications, in particular pertaining to the grey area between an angry personal opinion and defamation and incitement.

**Panel 6A: Cyber and influence operations**

"Spiders and Flies: The Use of Cyberwarfare in the online war against ISIS"
*Daniel Cohen (The Interdisciplinary Center (IDC) Herzliya)*
One analogy for the actors arrayed on the virtual battlefield is the comparison between spiders and flies. Modern non-state actors, such as terror organizations, are reminiscent of flies – a constant nuisance carrying disease wherever they go. They are inherently flexible, operating across borders and without standard constraints. In contrast, government agencies – virtual spiders – spin their webs in strategic locations and patiently await their prey. In the world of cyber space, collaborative efforts are difficult, and it is even more difficult to collaborate in the fight against ideological terrorism. A unique recent case study illuminates the challenges faced by the U.S state department and Pentagon with the conducting of influence operations campaigns and cyber warfare attacks against the ISIS since 2015. This online campaign demonstrated the extent to which a relatively weak non-state actor – ISIS – can project power and cause damage on a global scale. The paper will examine strategies and operational activity of this unique case study that illustrates an approach whereby cyber and influence operations are conducted as two distinct offensives against a singular opponent.

"Are jihadists losing control online?"
*Peter King (Independent consultant)*
The presentation will look at the state of play of jihadist groups' efforts to regulate the online behaviour of their supporters within their networks on social media platforms, focusing mainly on Arabic-language networks on Telegram. Specifically, it will look at Islamic State group (IS)'s attempts to prevent its supporters from engaging in any discussions online and how these appear to have failed. The presentation will discuss the disruption of networks, both in the past and today, and the impact this has had on jihadist groups' ability to control debate and keep supporters in check. It will also investigate the impact of perceived infiltration activity by intelligence agencies, both in shifting the focus of supporters' online energies and undermining trust. It will compare examples of alleged infiltration of online networks in the past with more recent allegations. Specifically, it will look at multiple allegations since late 2017 that intelligence agencies have been operating networks of online activists posing as Islamic State (IS) supporters with the aim of undermining the group and challenging it ideologically. Some have been linked with CVE efforts in the West

"Trends in ISIS's systemic exploitation of the web and social media"
*Laurence Bindner (The JOS Project)* and Raphael Gluck (The JOS Project)
@LoBindner & @Einfal
The latest trends in ISIS online activities may be compared to its military and insurgency operations on the field. During a first stage, as ISIS controlled a territory, a young generation of jihadists openly took possession of parts of the digital space with an "occupation" of the web, so to speak. During a second stage, following ISIS' military setbacks, the group morphed back into an insurgency, increasingly operating underground. A similar phenomenon seems to have taken place online, where ISIS opted for more operational security and partially migrated to encrypted apps such as Telegram. Lastly, as ISIS continues to carry out hit and run operations on the field, the group shows particular resilience and endurance in its media jihad. How does ISIS deploy tactics to circumvent censorship on major platforms? How do they use the web in a systemic approach to keep disseminating their content? How do they segment between platforms according to the types of online activities? What is ISIS' overall digital strategy, both to spread of propaganda and from an operational capacity (in a defensive and offensive perspective)? This paper expands on several articles written by the authors, in particular "Wilayat internet: ISIS resilience across the internet and social media" focusing on the whack-a-mole game played by cyber jihadists on social media, and on the analysis of the dissemination extent and longevity across the web for jihadist materials.

## Key Takeaways

- Similarly as ISIS morphed from a proto-State and territorial domination to an insurgency, it online activities migrated from public facing social media to more clandestine platforms
- ISIS is emulating in the digital sphere some of the features of a "guerrilla" style warfare: harassment, tactical mobility, appearing & disappearing, show of force.
- ISIS faces 2 dilemmas to keep its online influence: 1/ the need for digital security is disrupting exposure & reach, 2/ the need for anonymity is weakening brand authenticity.
- As ISIS is attempting a decentralization strategy with the announcement of new Wilayat, the group is also decentralizing its online reach: translation projects, fragmentation of propaganda to multiple platforms, more active unofficial media foundations.

**Panel 6B: Videos and videogames**

"Critical Analysis of Taliban's Videos: Intermodal Competition, Reinforcement and Conformity"
*Weeda Mehran (Georgia State University)* and Tony Lemieux (Georgia State University)
@WeedaMehran & @aflemieux
The Taliban banned watching TV and taking photos when in power, however, after being ousted in 2001, the group has harnessed the power of stories, images, videos and anasheed to promote its propaganda campaign. There is a prolific literature on the Taliban and their propaganda material. The focus of these studies has by and large been analysing online texts, night letters and magazines, while Taliban's videos has relatively remained under-studied. The Taliban has produced volumes of videos that depict "mujahidin's battles", the Emirate's "governance" activities and training camps to mention the most prominent themes. In this paper, we analyse more than 100 Taliban videos through a multimodal/multi-semiotic critical analysis lens. This method allows us to bring into light some of the inter-modal dynamics such as reinforcement, redundancy, competition or lack of it between visual, text and audio semiotics. Taking a critical approach, the paper also discusses what is put on display and how these intermodal dynamics influence those displays.

"Call of Jihad: The gamification of violent extremism"
*Nick Robinson (University of Leeds),* Maxime Bérubé (Université de Montréal), Imogen Richards (Deakin University) and Joe Whittaker (Swansea University)
N/A, N/A, @imogen_richards & @CTProject_JW
This presentation reviews the literature on gamification and violent extremism and describes how videogames and videogame representations are deployed on new and social media by jihadist organisations. For several years, 'gamification', (including elements of competition, rules of play, and point scoring), has had a discernible impact in a variety of contexts. This has been so in many online, non-gaming environments, especially when this type of engagement is facilitated by the affordances

of new and social media architecture, and when the audience is receptive to gamified modes of communication (Hamari, Koivisto, & Sarsa, 2014). A review of the extant literature tells us that organisations within the global jihadist movement (GJM) are increasingly featuring gamification, and gaming-related music and imagery, in their online propaganda. This intensification of activity is in part due to the 21st century diversification of the actors involved in the production of jihadist communications, and also to the evolution of new information and communication technologies that render extremist communications widely accessible. Gaming, gamification, and its social media correlates can be broadly conceptualised as 'influence techniques', which have likewise been extant in far-right propaganda and that of regional jihadist organisations such as Hezbollah. Gamification on the part of the GJM and in particular 'Islamic State', has been comparatively recent.

"Grading the Quality of ISIS Videos: Assessing Changes in Technical Sophistication of Digital Video Propaganda Across Time"
*Cori E. Dauber (University of North Carolina at Chapel Hill) and Mark D. Robinson (University of North Carolina at Chapel Hill)*
@CoriDauber & N/A
Our methodology for the grading of jihadist video propaganda makes it possible to compare the relative quality of videos in a quantitative way. One potential application of this method is the development of specific "aesthetic fingerprints," unique styles that could allow us to identify (and therefore trace) the Islamic State or AQ Hitchcock, Spielberg, or J.J. Abrams. We have continued to apply our method to videos of multiple groups, and the stark difference in rates of change across groups presents an opportunity. While HTS, or Al-Shabab, may try to imitate the qualitative successes of IS, their videos have improved gradually over a long period of time. Boko Haram, though, produced material that did not appear to change at all – until a sudden jump in quality resembling that of typical IS, complete with markers of typical IS output, apparently overnight. This suggests that individual media makers can be identified and traced. As they move, their unique aesthetic "fingerprints" will be carried with them. IS documents released by the CTC reveal a media checklist that makes the group's quality standards clear.

**Key Takeaways**

- The "Terrorism & Tech" discussion needs to include the creation as well as the distribution of propaganda

**<u>Panel 6C: Regulatory strategies</u>**

"CYTREC's response to the U.K. Government's *Online Harms* white paper"
*Patrick Bishop (Swansea University)*
@CYTREC_
This presentation will offer an overview of the U.K. Government's recent white paper on online harms and outline the responses that CYTREC will submit to the consultation questions.

"The Social Regulation of Social Media: Terrorist and Extremist Content"
*Amy-Louise Watkin (Swansea University)*
@CTP_ALW
Social media companies are under pressure to meet social regulatory demands concerning terrorist and extremist content. Social regulation is concerned with a broad range of non-economic issues whereby private organizations are seen to hold regulatory responsibility for serving public interests, promoting human rights, and overall general societal good. The majority of social regulation research has been developed in three areas: occupational health and safety, consumer protection, and environmental protection. Given the current demands, this research argues that social regulation research should be extended and applied to another area: the regulation of terrorist and extremist content on social media. This research identifies the current regulatory measures in place in the already established areas of social regulation and examines what we can learn and apply to the regulation of this content on social media. However, this research is not looking at what can be

applied generally, but, individual platforms specifically. Companies that fall under the term 'social media' differ in many characteristics and, therefore, a uniform approach may not necessarily be the most effective. This is a cross-platform study analysing Facebook, Twitter, YouTube/Google, Microsoft and Gab. Preliminary analysis of data collected from the platforms rules/community standards, 'about us' pages, blogs, and other publicly available documents will be presented. This research aims to gain a deeper understanding of the companies on an individual level in order to aid the argument of more tailored social regulation.

"Enough already! Why and how we are placing too much emphasis on social media companies to tackle terrorist use of the internet, and what to do about it"
*Hugo Rosemont (ADS Group; King's College London)*
@HugoRosemont
A consensus has emerged that social media platforms and tech companies including Twitter, Facebook, Google, along with many others, 'must do more' to eradicate the scourge of online extremism. Whilst the tendency to pressure these global giants to take responsibility for policing the internet is understandable, not least as they 'own' the networks on or through which offending communication or material is transmitted, the emphasis to date on 'outsourcing' counter-terrorism policy in this way is misconceived. This paper argues that the urge to press companies to 'do more' to remove extremism content has not been accompanied by the emergence of a sustainable policy framework that enables genuine public-private collaboration - an essential element for success in this space - nor have appropriate mechanisms of accountability yet been established. Having established a picture of the UK Government's over-emphasis on companies to tackle online extremism, the paper draws on research from other areas of security privatisation to offer options for manageable reform. The development of stronger public-private partnerships is a prerequisite of success in addressing online extremism and the state must now take ownership for its own role in counter-terrorism policy in the digital space.

**Key Takeaways**

- Governments and tech companies remain frustrated with each other around how to tackle terrorism online. More open and honest discussion on the balance of responsibilities is now needed.
- Effective public-private security cooperation doesn't happen on its own. We need to foster a much better understanding across the divide of each other's political and commercial constraints.
- Regulation of tech companies on security and CT issues is coming and is well overdue. This can facilitate a sustainable framework for cooperation but, as ever, beware the unintended consequences.

**Panel 6D: Methods and ethics**

"Deep Learning methods to detect radical online content"
*Berta Biescas (Insikt Intelligence)*
@insiktintel
Insikt Intelligence has developed a methodology to automatically detect terrorist-content text using supervised learning based on deep learning methodology. Word2Vec algorithm is used for the creation of the word embedding models. This algorithm is integrated in a python script with the Gensim library. Word2vec models are shallow, two-layer neural networks that are trained to reconstruct linguistic contexts of words. Word2vec takes as its input a large corpus of text and produces a vector space, typically of several hundred dimensions, with each unique word in the corpus being assigned a corresponding vector in the space. Word vectors are positioned in the vector space such that words that share common contexts in the corpus are located in close proximity to one another in the space. The main parameters of the word embeddings are: number of occurrences, size of the layers and the training algorithm. These parameters have been tested to find the most suitable ones as well as the best balance between accuracy and computing time. With this method, the

classifier has achieved a 75% of accuracy in English, and 80% in Arabic, classifying tweets in 6 degrees of suspiciousness. Besides that, we are working in a method of language alignment to take advantage of the English model for creating classifiers for other languages

**Key Takeaways**

- Deep learning methods can be used to detect radical online content
- The Inviso Intelligence Platform is a unique tool for the real-time detection of Jihadist radicals on social media platforms, embracing the latest technologies in order to understand jihadist terrorists' online activity locally and globally

"I lied but it was only for the good of society': The ethics of deceptive CVE"
*Lise Waldek (Macquarie University) and Julian Droogan (Macquarie University)*
This paper contributes to the literature exploring the ethics and justification of deception in Countering Violent Extremist programs. Identifying and addressing these ethical challenges is critical given the continued emphasis from academia and government on the production of effective and transparent CVE evaluation. Drawing on a case study from a government funded anti-far-right CVE program in Australia, the paper argues the ethical limitations of deception used in the program limit its overall effectiveness as a tool for online deradicalisation. The paper provides space for critical reflection on the ethical issues that arise for those managing these programs and working on their evaluation. The paper will first outline the program under investigation: a social media platform, designed to emulate far-right forums that exist to discuss and disseminate extremist content, so to attract vulnerable individuals and engage them in one-on-one dialogue for the purposes of deradicalisation. It will then present the findings of the evaluation, which was undertaken by the authors, and explore the limits posed by deceptive practice in CVE. Drawing on the work by Guillemin and Gillan (2004) on micro-ethics, the paper identifies a growing requirement for reflexive ethical capabilities in academic communities in order to facilitate engagement in evaluations of complex CVE programs.

**Key Takeaways**

- Robust evaluation frameworks and reflexive ethical processes are critical for CVE evaluation particularly where deradicalisation programs incorporate elements of deception.
- Evaluation and reflexive ethical processes raise important questions about the impact and effect on all those involved in the element of deception.
- The effectiveness of online deception for purposes of behavioural change is incredibly difficult to assess without access to oversight (online and offline) of any given 'deceived' individual.

"Grounded Theory: A Methodology with Much to Offer in Terrorism and Social Media Research"
*Orla Lehane (Dublin City University)*
@orr_laa
Drawing on a classic grounded theory study of grassroots CVE practitioners, this paper argues that grounded theory is a methodology that could, and should, be used further in the area of terrorism and social media research. Within terrorism studies there has been considerable criticism of the lack of systematic research methods (Freilich and LaFree, 2016: 571) and Dolnik (2013:1) notes that while the field has witnessed a significant increase in academic output over the last decade, comparatively little attention 'has been devoted to attempts to systematically develop the quality of the terrorism studies discipline itself.' This paper begins by outlining grounded theory, in its different forms, using specific examples from the case study in question. The advantages of grounded theory are discussed, along with the challenges it poses, particularly for novice researchers and those working in areas wherein grounded theory is not typically employed in research. Finally, this paper explores the various types of data that can be used within a grounded theory study. Here it is argued that, given the flexibility to follow up leads, while adhering to the inbuilt rigour in the methodology, and consider a variety of data types, including images, online materials, quantitative data, (online) ethnographies, and

more. As such, there are a variety of ways that grounded theory research can contribute to understandings around various issues within the realm of terrorism and social media. A series of examples will be used here to identify more specific areas that might benefit from the use of grounded theory.

**Key Takeaways**

- We need to consider different/alternative methods and approaches to progress research in the area. Grounded theory is not commonly used in this field, but offers potential to approach things in a different way and to draw on ideas from other fields