Global Network
on Extremism & Technology

GNET Research Workshop Summaries

Prepared by:
The International Centre for the Study of Radicalisation (ICSR),
Department of War Studies, King's College London, WC2R 2LS, London, United Kingdom

New Wave of Right-Wing Terrorism?

The Peace Research Institute Frankfurt

1 June 2020

This workshop opened with a presentation that summarised the main findings and recommendations of a recent study by an author team from IFSH and PRIF[1]. Starting with a brief overview of the main insights on developments and narratives of transnational right-wing terrorism, the focus was then on the (self-) regulatory space of coping with digital hate culture and digital networks of right-wing extremists.

Three core themes arose from this presentation and the ensuing discussion:

1. **The challenge of leaving takedown decisions on extremist content to tech companies:** The participants noted that one of the central challenges to content moderation is that extremist content is a moving target: opinions, trends, 'disguises' of right-wing ideas are constantly changing. Moreover, online behaviour only gives a brief insight into the actual people behind the posts – offline behaviour might differ; but judging the online content, the motives and context of those who post, is of great importance too.
2. **The ethics of online intervention:** From the tech company side, it was stressed that clear categories from states are very welcome to be able to identify problematic content within a given jurisdiction. Legal regulations vary between countries and indicators/subcultural signals change rapidly. Since there is no ideal solution, transparency about processes and legal concepts is key. Representatives from tech companies stated that they strive for transparency about their definitions of hate speech, terrorism, community standards and so on. However, there are obvious deficiencies in the regulatory area. States should not only provide legal guidelines, but also have their own sufficient capacities of technical expertise and analytical skills to develop and update those guidelines and to judge the cases before them.
3. **The complexity of categorisation:** The complexity of categorising the vast amounts of extremist content came to the fore in a discussion on the varying challenges of monitoring diverse sources of content. It was explained, for instance, that a nudity policy is relatively easy to follow because it is, under many jurisdictions and cultures, more obviously straightforward to define. The grey zones for extremist content are larger. While organisations such as al-Qaeda and Islamic State have a clear set of symbols and terminology, this does not apply to a lot of the newly emerging and constantly evolving extremist communities and loosely coupled transnational networks; platforms need to operate on binary factors (is it extremist content? yes or no); extremists apply tactics to mitigate the policies. As such, tech companies are involved in a never-ending game of catching-up to follow the evolving content being posted.

[1] The introduction was based on a chapter that has been published in the German Peace Report in June 2020

The Global Internet Forum on Counter Terrorism:

Balancing Online Content Moderation and the Rule of Law Program on Extremism

27 August 2020

This workshop included nine panelists, who discussed how we can better combat online violent extremist and terrorist content. The presenters exchanged ideas on the resources that are currently available and what needs to be improved in order to counter the dynamic, opportunistic and adaptable nature of violent extremists online.

Three core themes arose from these presentations:

1. **The goals of multi-stakeholder platforms:** The presenters discussed the role of multi-stakeholder platforms, such as the GIFCT, in combatting online content. The GIFCT was described as a unique platform that brings the tech sector, social media and governments together to work on online problems ranging from terrorism and extremism to broader issues. A presenter highlighted that the GIFCT has shared over 300 hashes and over 20,000 compromised URLs in the past few years. One presenter noted that stakeholders need to be more aggressive at stating their objective and their concrete/technical ways on how to achieve their goal. In order to optimise the work that the GIFCT conducts, it should set a precedent for ways to deal with online threats, encourage companies to think differently and view the various member platforms as many united nations in order to identify standards and norms to which everyone can operate.
2. **Creating policy and best practices:** One presenter stated that companies need to change their policies to be adaptable and resilient in the face of challenges as they arrive, instead of being worried and preoccupied with shutting them down completely. A second presenter added that it's important to create pillars of work that would help both big and small tech companies. There are three main pillars: (i) joint-tech innovation; (ii) knowledge sharing; and (iii) conducting research and partnering. Joint-tech innovation looks at sharing tools and knowledge from a programming perspective. It involves a hash database to gather the digital fingerprint of images and videos. Knowledge sharing is sharing a network of knowledge with those involved in GIFCT. Finally, the pillar of conducting research and partnering is based around funding a research institute in order to identify where best practices can be shared and how others can be supported. However, one presenter pointed out that when it comes to the hash-sharing database, it can be difficult for smaller platforms as it augments the power and biases of the bigger platforms.
3. **Shift in focus:** The presenters discussed how the model for the GIFCT started with child sexual abuse material and evolved into a focus on terrorist content, hate speech and general problematic content. The child sexual abuse material was much easier to classify as problematic content, as not all terrorist content is necessarily explicitly concerning.

Online Agitators, Extremists and Counter-Messaging in Indonesia

The Centre of Excellence for National Security

25 August 2020

This workshop opened with four presentations that all highlighted current developments regarding the use of social media by violent extremists, potentially subversive Islamists, and agitators on both sides of Indonesia's increasingly polarised political debate. This led into a discussion of fresh experiments to offer alternative narratives and amplify constructive messaging, particularly among young Indonesian influencers.

Four core themes arose from these presentations.

1. **Improvement in content moderation:** Social media companies have become better at shadow-banning users and removing violent extremist content with artificial intelligence tools. As in other parts of the world, the pro-Islamic State (IS) Telegram ecosystem in Indonesia has been decimated in the past couple of years. New groups continue to pop up regularly but are also taken down relatively quickly. Whereas Telegram groups of IS supporters in Indonesia used to comprise over a thousand users, the average size in August 2020 was around 200 users before a group would be discovered and blocked. Another notable development is that content previously spread from node to network – individuals were able to post or broadcast to thousands of people on Facebook, for example – but now sharing is more node to node within, for instance small WhatsApp groups of close associates. Nonetheless, WhatsApp accounts have become vulnerable to penetration in Indonesia and users regularly migrate to new platforms with similar functions.

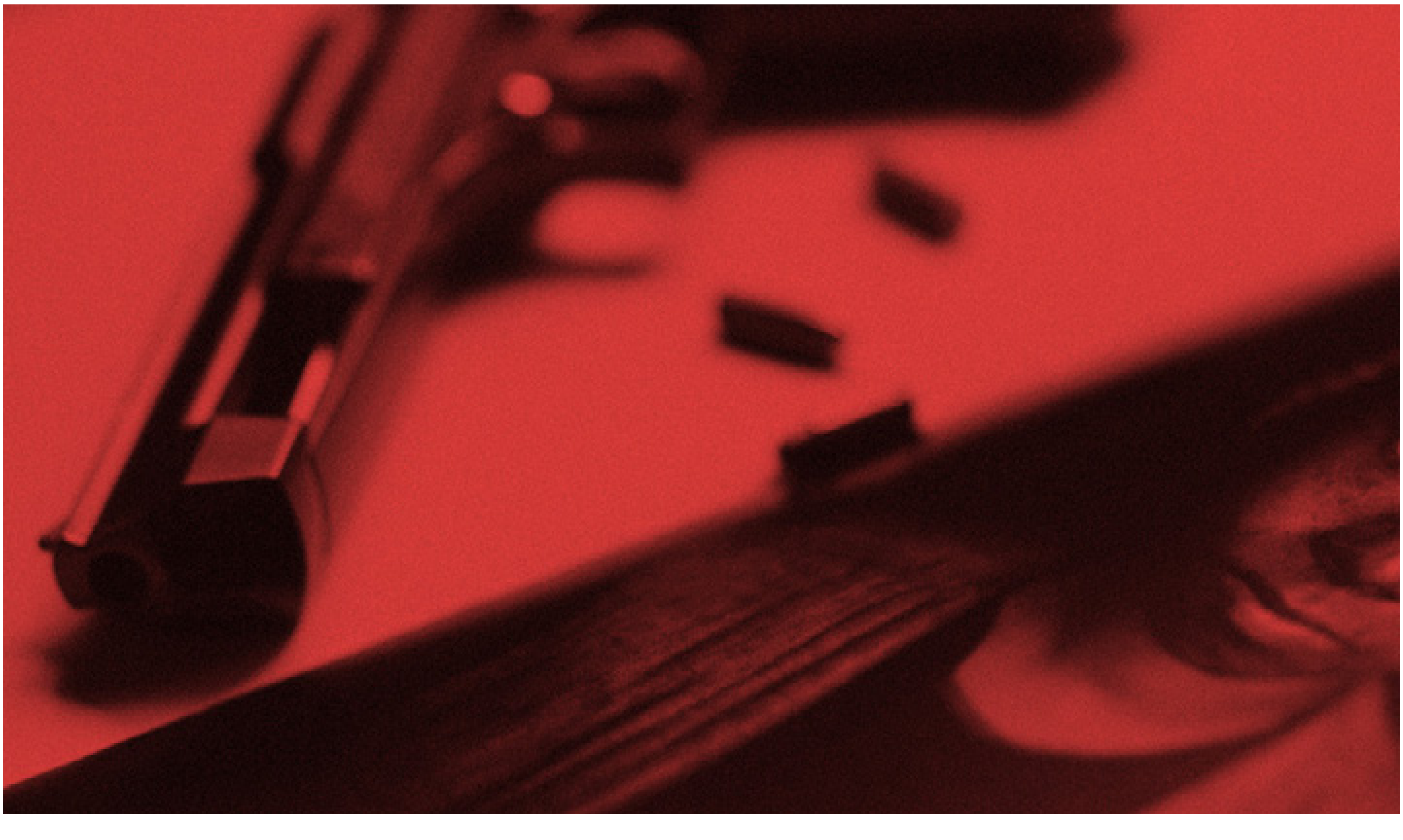
2. **The current activities of the Muslim Cyber Army:** The Muslim Cyber Army (MCA) emerged during the 'anti-Ahok' rallies in November and December 2016, during which Islamists demanded the Jakarta gubernatorial candidate be charged under blasphemy legislation. Supporters were urged to use whatever digital skills they possessed to wage an online war against their perceived enemies. MCA's leadership operates in secret by coordinating on such platforms as WhatsApp and Zello (a push-to-talk app that facilitates private communication). More open social media sites allow the movement to reach new audiences and reinforce social and political positions through filter-bubbles and echo chambers, exacerbating the political polarisation emerging in recent years.

3. **The PCVE website ruangobrol.id:** Having assisted with the reintegration of former prisoners convicted of terrorism offences for several years, activists behind Ruangobrol set up the online platform ruangobrol.id to create and promote alternative narratives for young Indonesians confronted with violent extremism. The idea was to train ten ustadz and ten former combatants in media communications and encourage them to become 'credible voices' who could unveil the realities of violent extremism. One year ago, Ruangobrol started a pilot programme aimed at engaging people who seemed set to spiral towards violent extremism. The programme identifies individuals on Facebook

and classifies them into different levels of radicalism, before attempting to interact with them through post comments and chat. The ultimate aim is to link people with suitable mentors offline, but the programme has so far encountered difficulty building the requisite trust.

Additional problems include Ruangabrol's undercover accounts facing takedown measures from Facebook content moderators; the savviness of users adept at identifying suspicious accounts; and the potential security risk of meeting people offline before revealing their true intentions.

4. **Gender:** Over the past ten to fifteen years, social media has provided new space for women in Indonesia to express themselves. More recently, online extremist propaganda has been manipulating gender issues, injustices and marginalisation, while claiming to offer pathways to empowerment. Search for Common Ground Indonesia (SFCG) has developed a programme called Generating Indonesian Resilience and Leadership Skills, known as GIRLS, which is focused on facilitating opportunities for young women. SFCG conducts social media analysis to target its messaging appropriately and currently work with 'micro influencers', or social media accounts with around 1,000 followers on Twitter or Instagram.



Online disinformation in the age of COVID-19

Program on Extremism

23 September 2020

This workshop included nine panellists who are all involved in efforts to combat and study online disinformation in the information environment wrought on by the coronavirus pandemic. The workshop's goal was to foster a meaningful exchange of ideas that reflected on lessons learned over the last several months and to identify paths forward as well as future needs across a range of stakeholders. The panellists were given the following three questions: (i) How has the coronavirus pandemic impacted the subjects of your area of expertise, especially in the online space, and what are likely to be the long-term implications? (ii) How is propaganda and disinformation transferring from the online to the offline space, especially related to COVID-19? And (iii) How do you see the contest between illiberal and democratic norms in cyberspace playing out? In what ways has COVID-19 shaped these dynamics?

Four core themes arose from these presentations:

1. **Extremists are seizing and co-opting emotions:** A panellist discussed the power of emotions, which play a critical role in government responses, public trust and other social processes. She highlighted that the trauma and frustration wrought by the current environment have major psychological and physiological implications, adding that extremist groups are seizing on compassion and co-opting it into their strategic messaging.
2. **Boost in online numbers:** There has been a boost in online membership of armed militia and white nationalist groups, which initially centred their discussions around Second Amendment issues but have repurposed their collective focus in the pandemic-era to 're-open' protests. One panellist also noted a surge in antisemitic and anti-China racist tropes spreading online. A second panellist warned that the rise in viral online traffic (especially related to apocalyptic and cross-ideology material) may be correlated with an increased probability that individuals will act on their searches, including possibly by resorting to violence in the current environment.
3. **Narratives:** One panellist noted that groups are seizing on political unrest in the streets to frame the narrative of their ideological goals, and that the amplification and reinforcement of these narratives in online echo chambers has given rise to what she terms 'contagious fascism'. A second panellist added that offline behaviour tends to follow the source of whatever conspiracy theory individuals believed; for example, the targeting of 5G masts believed to be the source of illness and death rather than the 'fake' coronavirus. Adding to this, a panellist noted increased efforts across ideologies to use conspiracy theories and current events related to the pandemic to amplify existing tensions in their strategic messaging. Along those lines, anti-vaccination conspiracies in particular seem to be gaining popularity across groups, and general distrust of the concept of a coronavirus vaccine may have serious real-life implications.

4. **Reaction of groups on different ideological leanings:** One panellist found that groups of different ideological leanings are reacting differently to the pandemic and seizing on different coronavirus-related news and events for their own purposes. White supremacists, for example, reacted to news that black and brown Americans were at higher risk of mortality from the coronavirus by talking of ways to specifically target people of colour. Anti-government extremists, meanwhile, have reacted to conspiracies related to government control and Second Amendment issues. A second panellist noted that non-governing violent Islamist groups, such as al-Qaeda and Islamic State, have focused their attention on, first, noting the pandemic is a ramification of unbelief and, second, encouraging their followers to carry out personal hygiene as laid out in hadiths. However, governing violent Islamist groups, such as Hamas and Hezbollah, have focused their efforts on demonstrating their effective governance and handling of the coronavirus crisis while deflecting any criticism and blaming it on those that oppose their rule.

Legal Framework for Countering Violent Extremism Content Online

Policy Center for the New South

8 October 2020

This workshop opened with four presentations highlighting how national and legal frameworks for countering violent extremist content in the MENA region and Africa are diverse and all face different challenges. The first presenter emphasised that there is a shortage in terms of legal frameworks in Mali to tackle extremist activities online and the risk of misuse of these law to crackdown on individual liberties is present.

The second presenter explained that in Tunisia the problem of terrorism both online and offline is being strongly addressed given the history of the country suffering from multiple terrorist attacks. The coronavirus pandemic has created the risk, due to a large number of unemployed youths, of an increase in recruitment.

The third presenter's research was focused on the importance of data privacy in Kenya. The computer crime and misuse act was passed in 2018 and specifically provided for cyber-terrorism as an offense. This act is exclusive to Kenya as surrounding countries, such as Uganda, do not have this emphasis on cyber-terrorism.

The final presenter introduced the legal frameworks in Morocco and explained how law enforcement agencies in the country react.

In Mali, the fight against terrorism is conducted on multiple fronts by military personnel, law enforcement specialists and intelligence analysts. One of the issues raised was the lack of training in terms of tackling online content and the lack of resources in terms of technological equipment. Another challenge, especially in the northern part of the country, is that many of the terrorist groups run their own websites. However, the control of Internet activity is not a real priority in Mali, as the country is more focused on activities on the ground.

Tunisia is debating a bill on the protection of the police force, and part of this bill addresses violent extremist content online. The participants debated whether the state role in combatting violent extremist measures should be confined to positive measures like education and providing counter narratives rather than enforcing sanctions on online activities.

In Kenya, young people are being recruited and radicalised online, and recent investigations show that the latest attacks in Nairobi were tied to online recruitment strategies. Another challenge is the mistrust of state security operators by the community. If security officers were to be given the power to collect data, it raises the question of freedom of speech and corruption of data.

In Morocco, there is a debate around how to assess online content, by which criteria and by whom. In terms of legal frameworks, there is a question of who is in charge of online counter-terrorism. Again, respecting the democratic component of governance is essential.

Additionally, there is an imbalance between north and south in terms of intelligence infrastructure and cooperation.

Three core themes arose from these presentations:

1. **The collective response is paramount in terms of tackling cyber-terrorism:** On the regional level, ECOWAS is trying to interact, and the fifteen country are proposing to harmonise the legal frameworks in spite of the difficulties in terms of language and legal culture.
2. **Legal frameworks:** The issue of encompassing what is extremist online content in terms of legal frameworks is also essential to further enhance enforcement. Public–private partnerships can be very useful.
3. **Training:** Training can be a very useful area of international cooperation in terms of educating teachers, imams and professionals on the online realm and how it is used by extremist groups.

The Intersection of State-Sponsored Disinformation and Online Extremist Content

The Lowy Institute | 15 October 2020

This workshop opened with four presentations that focused on how extremists spread online disinformation which forms part of a known, state-sponsored disinformation campaign, and where combatting online extremism overlaps with combatting online disinformation campaigns.

The first presenter offered an assessment of the relationship between state-sponsored disinformation and extremist narratives. He stated that far-right and far-left groups are more susceptible to engaging with and being targeted by foreign disinformation campaigns than jihadist actors.

The second presenter pointed out that the policy responses to online extremist content have made progress in ways that policy responses to disinformation have stalled. This is because of the acknowledgement of the threat: the threat of online extremist content has been comprehended in ways that that of disinformation has not been, particularly in the United States.

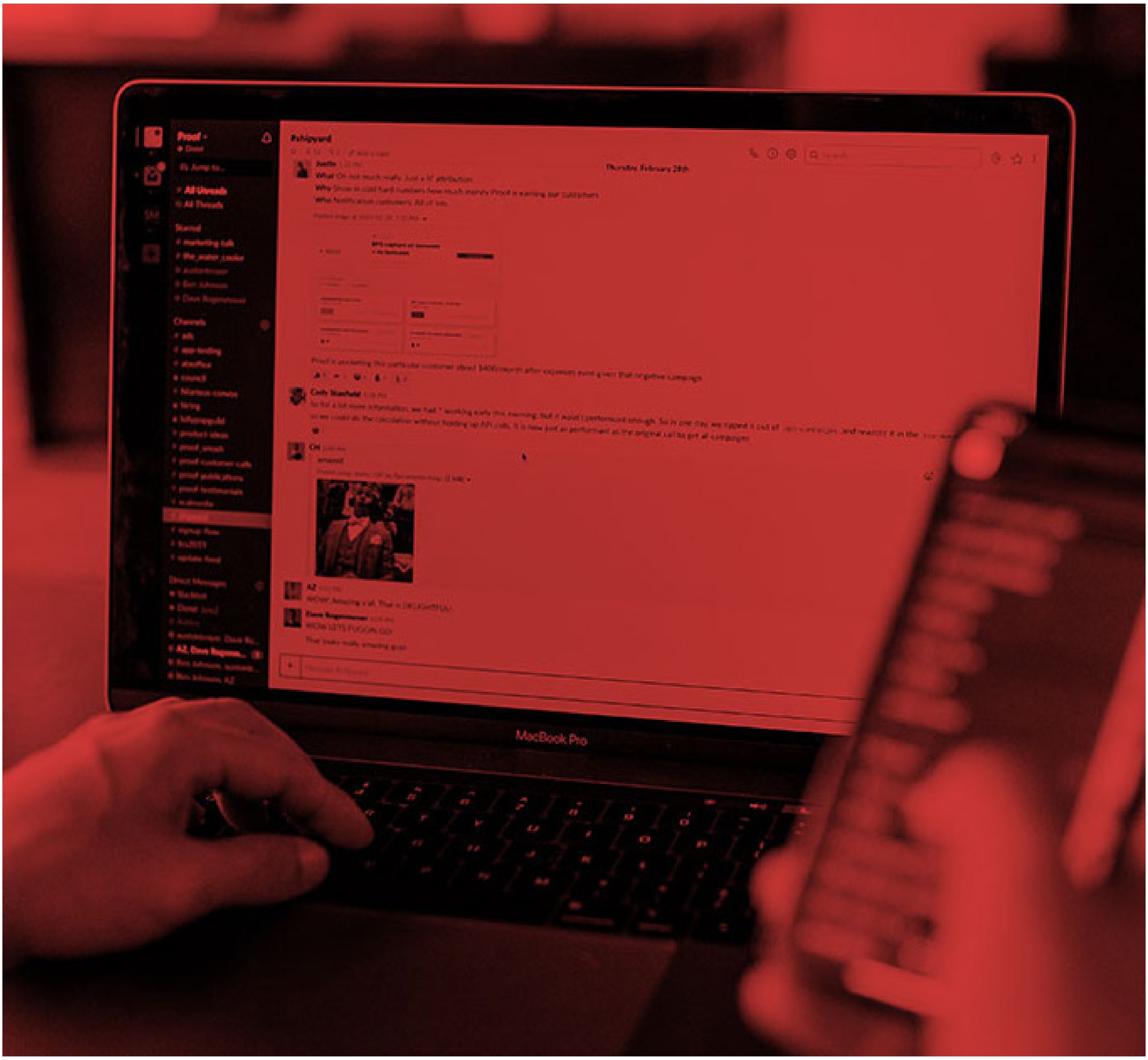
The third presenter gave a brief on his work examining disinformation spread online around the Australian bushfires and its spread via bot-like activity, which was then also spread by far-right groups online.

The final presenter discussed online racism and hate targeting ethnic Chinese individuals, as well as the intersection of far-right and neo-Nazi groups online with anti-China actors.

Three core themes arose from this workshop:

1. **Russia:** One of the presenters noted that he had observed the amplification of messages of extremist movements by hostile states such as Russia, as a tool to disrupt liberal Western societies. Furthermore, the Russian social media platform VK is now a viable alternative platform for the far right. With this in mind, the presenter emphasised the need for platform providers to do more in this space and the demand for more robust public/private partnerships as well as government responsibility regarding public awareness and education around disinformation.
2. **Policy responses to extremism vs responses to disinformation:** We do not have the same consensus regarding social media platforms' role in spreading state-sponsored disinformation as we do for its role in spreading online extremist content. Regarding disinformation campaigns, cooperation between law enforcement and tech platforms is more begrudging and limited. Cooperation on extremist content is more robust, as evidenced by GIFCT's existence. However, the coronavirus pandemic may have shifted considerations, as social media platforms have more understanding that disinformation spread online has resulted in real-world harm and offline violence.

3. **The nexus between neo-nazi groups and anti-Chinese actors:** Far-right protesters protesting lockdown and coronavirus restriction measures in Australia have been strongly connected to anti-Chinese Communist Party (CCP) and anti-China narratives. Furthermore, far-right groups have also been promoting propaganda of Falun Gong both online and off, which is also anti-CCP.



Researching Social Media and Data Protection Challenges

The Peace Research Institute Frankfurt

26 October 2020

This workshop opened with three presentations that summarised the main challenges faced by researchers in the violent extremism field. The presentations considered the issues from both ethical and legal standpoints, as well as from the perspective of tech companies.

Three core themes arose from these presentations and the ensuing discussion:

1. **Consent:** A key distinction must be made between research involving data from subjects who have consented to the use of their data and research involving data that is collected and analysed without the consent of data subjects. Under particular circumstances, research is possible without informed consent (for example, when information about the research would jeopardise the research). However, there is a need to anonymise personal data, making it completely unidentifiable including getting rid of IP addresses and so on. Because consent is particularly difficult to achieve in extremism studies, researchers need to work with legal basis (balance research interest with protection of the individual; article 6) and be especially aware of the special protection of political and religious opinions (article 9).
2. **Flagging extremist material:** Although researchers should flag extremist content, they want to see how it unfolds and how others interact with it. Relatedly, many researchers wonder which material should be flagged, and how they should go about it. There exists a lot of 'grey content' that isn't illegal but is potentially dangerous. The participants discussed how to make researchers in the field more aware of the online tools for reporting content at their disposal. Facebook, for instance, offers training on all of its tools and the changes it makes (for example, to privacy settings) to its stakeholders.
3. **Accessing flagged material:** Accessing old extremist content on Facebook may be difficult, because the platform has only a 90-day waiting period before the content is deleted from Facebook servers. Storing deleted content has legal and ethical connotations, even though it can be very practical: as there are more than two billion pieces of content uploaded every day, there is not enough data storage capacity to store everything. Although violent extremist content cannot be stored legally, content may be hashed and put in a database so it is automatically flagged if it comes up elsewhere. The participants agreed that this is a potential discussion to have with Tech Against Terrorism: who should host deleted content?

Academic Freedom in the Violent Extremism Space

International Centre for the Study of Radicalisation

18 November 2020

This workshop looked at the issue of academic freedom in relation to studying terrorist content, specifically whether researchers should post screenshots and related contentious material on social media. The discussion opened with the question of whether it is a researcher's responsibility to circulate violent extremist content on social media platforms, such as Twitter, in order to bring it to the attention of tech companies and practitioners. Some of the workshop participants expressed concern about individuals who believe that no content should be circulated, as they stated that academics need to circulate as much information as possible in order to change the conversation.

Three core themes arose from this workshop:

1. **Sharing content that contains personally identifiable information (PII):** The workshop participants discussed the importance of practicing self-protection when sharing violent extremist content. In the past, some researchers have accidentally tweeted out Telegram handles leading back to the original creator. From a tech perspective, the greatest concern is when a researcher posts violent extremist content without removing or blurring out the PII, inadvertently leading others to the source of the content, such as a far-right extremist who hasn't been banned or a core terrorist text.
2. **Sharing harmful content without amplifying it:** One participant stated that one of the biggest obstacles is the question of how to publish violent extremist content without amplifying it. However, it was noted that most academics and researchers don't have huge followings on social media platforms – the bigger issue was media organisations that release this type of content. A participant voiced her concern around the responsibility of determining whether content is illegal harmful content or legal harmful content falling to organisations such as the GIFCT.
3. **Academics vs journalists:** The participants highlighted that there is an important difference between academics and journalists in this field, as academics are not offered the same protection as journalists. When journalists are considered as a separate case in this discussion, there is a risk of forgetting academic research when developing new policies; however, the lines are increasingly blurred in many contexts between journalists and academics. A participant noted that when any solutions around posting violent extremist material are formed, particular caution should be taken to ensure that we aren't doing something that protects one group while doing a disservice to another.

The Online Presence of Australian Far-Right Extremism

The Lowy Institute

25 November 2020

This workshop opened with three presentations that focused on the narratives spread by Australian far-right extremists on the Internet and social media, as well as how extremists in Australia engage with the broader global far-right extremist community. The first presenter shared their recently released study, which analysed data from a number of social media sites (Twitter, Gab, Reddit, 4chan and 8chan). This study was focused on far-right actors in New South Wales. Their research identified two connected levels of risk in the use of the Internet by far-right extremists: (i) The shifting of the Overton window – the acceptable level of social and political discourse; and (ii) The difficulty in identifying potential violent actors or indicators that online rhetoric will lead to offline harm.

The second presenter shared his recent research project that found that far-right and male supremacist groups have become a growing threat in Australia and that, as a recruitment mechanism, they target men by appealing to their sense of manhood and masculinity.

The third presenter discussed far-right and far-left ecosystems and examined how they discuss each other and how the narratives about the other shape the online activity of these groups.

Two core themes arose from this workshop:

1. **The transnationalisation of far-right extremism:** The presenters identified how transnationally connected the Australian community is to other far-right communities in the United States, North America and Europe. This is indicative of how social networking sites have contributed to the transnationalisation of far-right extremism and the post-organisational structure of extremism more broadly. They also identified a number of themes and frames within online far-right communities in Australia that also intersected with the international far-right community: 'White identity under threat', 'Trumpism' and 'deep state conspiracies'. On what they identified as 'low risk platforms' – mainstream social media sites that have more established content moderation mechanisms – these narratives are engaged with in ways that purposefully skirt content moderation. On 'high risk platforms' such as Gab, themes are framed more explicitly and with a willingness to explore the need for violent action.
2. **The far-right's messaging against the far-left:** In 2020, the coronavirus pandemic provided ample opportunity for the far right to push its narratives against perceived enemies on the left online. The analysis of messaging this year also found that it framed groups on the left as 'anti-capitalist, anti-liberal and violent' and individuals as 'un-Australian, anti-white hypocrites', over-educated 'dole bludgers', precious cowards and violent thugs. Furthermore, in the months of June and July 2020 during the global protests against racial inequality and the BLM movement, the far right's discussion of the left increased exponentially and this period led to increased antagonistic mobilisation online.

Everyday Encounters with Extremism: Locations, Effects and Challenges

Cyber Threats Research Centre

25 November 2020

This workshop opened with three presentations. The first presenter used a critical focus group approach to analyse militarisation and gaming, and explained that gamers routinely saw graphically unpleasant pornography, which they regarded as part of wider cultural 'playground' practices. Furthermore, every single one of the gamer groups in this study had one person who had joined the military, which was not expected.

The second presenter's research was focused on gender and anti-feminism in men's far-right groups and also social media conspiracy theories. She described QAnon as a current focus of concern, as it has connections to the far right yet is more commonplace than a lot of far-right extremist groups. The presenter added that the links between the military and far-right extremist groups point to linkage in the everyday and extreme spaces.

The third presenter currently studies Stormfront, the violent neo-Nazi message board, and conducts interviews with former far-right extremists. In his presentation, he explored whether gaming or other cultures have more influence on extremists than propaganda.

Five core themes arose from these presentations.

1. **Everyday violence as a cathartic environment:** The presentations raised the question of whether immersion in violent culture could be protective against radicalising materials, rather than enabling radicalisation. One participants noted that although it is interesting that these communities can have protective factors, this is at odds with widespread takedown policy. A question arose about whether we should be putting resources into removing content – which is difficult, due to the volume – if it's protective or cathartic, or whether this is a permissive environment for violence. It was noted that there are differences between violence and non-violent propaganda: leaving the latter up means that we are potentially enabling extreme groups to indulge in particular forms of messaging. One participant noted that she had seen widespread tolerance of IS posts on Facebook, even in networks where many people disagreed with the posts. Young people are more resilient than might be assumed.
2. **Gender:** One panellist noted the ways that gender came into focus groups who reflected on past exposure to extremist and violent content: focus group participants were nostalgic, using terms like "boys will be boys" and exploring violence as a rite of passage. It was "just a thing people did".
3. **People who post every day:** One panellist noted a number of posters did post every day on Stormfront. They were not the most extreme posters, and many of their posts were what he called 'gateway' extremism material. A panellist suggested that when looking at gateway material, it is important to understand it's often an amplification of mainstream narratives.

4. **Removal of everyday extremism:** It was noted that although takedown efforts do work, it's impossible to remove all problematic content. The point was made that if we can see this material, we know what is being discussed and we know what we're dealing with. A tech platform representative noted that it is challenging defining what is a violent extremist group according to their policies, particularly in regard to the far right. Groups and movements are very savvy in terms of testing this and knowing how far they can go before they cross the line.

5. **Future areas of work:** One participant noted that we need to look at the ecology and affordances of different platforms. Another participant pointed out that thinking of new and innovative ways to connect online and offline extremism will give us better insight into the impacts of these communities and more of a measure of the role of the Internet in violent extremism.

The Fusion of Offline and Online Interventions against Extremism in the Philippines

The Centre of Excellence for National Security | 16 December 2020

This workshop opened with four presentations that all discussed interventions made by civil society and non-government organisations for preventing/countering violent extremism (PCVE) in the Philippines. There was consensus among speakers that while online interactions facilitate radicalisation and recruitment, offline interactions remain the most important factor behind violent extremism in Mindanao.

Four core themes arose from these presentations.

1. **The use of 'hope-based' narratives in Mindanao:** In the Philippines, especially among residents of rural and/or conflict-affected areas (CAAs) in Mindanao, Facebook is synonymous with and practically indistinguishable from the internet. The coronavirus pandemic has amplified pre-existing issues such as the dearth of government services provided to CAAs in Mindanao. Jihadist propaganda has seized on the narrative that the government has left communities in Mindanao to fend for themselves. In response, the Asia Foundation has pushed for the implementation of digital literacy campaigns to be spearheaded by local government units (LGUs). LGUs are trained to go beyond counter-narratives or 'fear-based' communications, which highlight the threat posed by violent extremists. Instead, there is emphasis on 'hope-based' communications that highlight solutions and cooperation between LGUs and CAAs.
2. **Cross-platform PCVE messaging:** Social media can become an echo chamber, with violent extremist organisations often structuring their narratives into something akin to a monologue. In response, Equal Access International (EAI) promotes dialogue among the youth in Mindanao to disseminate the messages of diversity and inclusion. Recognising the patchy nature of Internet connectivity in Mindanao, EAI utilises cross-platform messaging. This includes broadcasting content on the radio and establishing transistor radio operators' groups to reach communities. On the digital side, EAI runs 'tech camps' to train youth leaders in skills needed for online/social media content creation and distribution.
3. **Data collection to identify vulnerable communities:** impl.Project differentiated itself from other PCVE-related organisations in the Philippines by its emphasis on 'last-mile' data collection. Ongoing studies by impl.Project reveal that membership in violent extremist organisations, particularly in the provinces Maguindanao and Lanao del Sur, are often motivated by socio-economic deprivation or resistance to the predatory practices of local government officials. Across Mindanao, impl.Project staff were able to conduct wide-ranging surveys. Locally hired staff using technology developed by impl.Project engaged with 25,000 respondents, compiling what was quite possibly the largest database of CAA residents in Central Mindanao. Based on impl.Project data, the lack of livelihood opportunities is the primary driver for recruitment into violent extremist organisations.

4. **Public backlash:** PCVE by the Armed Forces of the Philippines (AFP) over social media suggests continuity with offline counter-insurgency propaganda. A look at Facebook pages associated with the AFP highlights the ad-hoc fusion of offline and online efforts – aviators would share videos of leaflet drops, while civil relations personnel would livestream AM radio broadcasts. However, there is a wholesale replication of counter-insurgency themes. Content made targeting communist insurgents were misapplied to jihadist-inspired groups. Aesthetically, content that can be attributed to pro-government sources takes on a trolling character, as seen in botched attempts at image/photo manipulation and falsely 'red-tagging' famous celebrities as communist sympathisers. There is also rampant misunderstanding among military personnel regarding social media platform usage policies. Some military and law enforcement personnel used their own personal social media accounts to report inappropriate content or to organise mass reporting. Such initiatives, however well intentioned, can be miscategorised as 'brigading' or a form of coordinated, inauthentic behaviour by platforms such as Facebook.

Big Data, Counter-Terrorism and Transparency

The International Centre for Counter-Terrorism

25 January 2021

This workshop opened with a presentation on the relation between artificial intelligence and transparency and the related legal issues and concerns. The presenter explored transparency as a cornerstone principle of democratic systems, one that is interconnected with the necessary accountability of public powers. She explained that these cornerstone principles can sometimes be limited in the name of national security. This balancing, however, must meet certain conditions (such as necessity and proportionality) that the presenter concretely developed.

The presenter then addressed the issue of lack of transparency in artificial intelligence (AI) more specifically. She explored the difficulty to ensure transparency activities (security practices) that build on big data. The presentation revolved around several questions relating to the design of the algorithmic system. These questions each raise serious legal issues that were developed in the presentation, such as (i) how was the algorithmic system designed? (ii) what and how was the data collected? (iii) is there enough data to ensure trustworthiness and effectiveness of AI systems? (iv) how or under what criteria is the input data transformed into the legal output? And (v) to what extent do decisions to delete online content derive from the suggestions of the algorithm alone?

Three core themes arose from this presentation:

1. **The shift from data to meta data is seen as problematic:** Meta data contains exit data, itself containing information about, for instance, geographical locations, which can be used to identify the personal address of individuals, thus defeating the anonymous nature of the data and leading to privacy concerns and GDPR implications.
2. **Difficulties when applying AI to large datasets:** The participants discussed the findings of a project on the 'digital jihadists', in the framework of which within a month of research they were able to find 400 domains online being used by jihadists. Participants asked why, despite concerted efforts, AI is not efficient enough to detect such information. Is AI useful only when lots of data are available? Problems arise through a lack or fragmentation of data, the dark net and torrents where it is difficult to apply AI, or the difficulty of gathering large amount of data.
3. **Private companies:** When AI systems are (co-)implemented by not only law enforcement agencies but also private companies, there are issues of state sovereignty being reshaped; of separation of powers; and of private companies becoming quasi-judicial bodies when formulating judgements on persons using their platforms (and enforcing decisions that have consequences).

Far-Right Responses to the U.S. Capitol Attack

The International Centre for the Study of Radicalisation

10 February 2021

This workshop opened with four presentations looking at the far right's online responses to the 6 January insurrection at the U.S. Capitol. The first presenter looked at the far right's use of the application MeWe, explaining that the platform does not moderate its content as strictly as bigger networking platforms.

The second presenter highlighted three technological affordances offered by communications technology to extremists online. These affordances are the hyperlink structure of the Internet, power law dynamics and network effects, and algorithmic automation.

The third presenter discussed why deplatforming the far right is more challenging than deplatforming Islamic State.

The final presenter commented on how the previous three presentations highlighted the transnational aspect of the problem and questioned when the whole discussion becomes a terms of service issue.

Three core themes arose from this workshop:

1. **Smaller platforms vs bigger platforms:** The first presenter observed that far-right MeWe users targeted a smaller audience than they would on a bigger platform. She gave the example of a group for a specific militia in a specific town in the United States, such as a QAnon group for Philadelphia residents. The participants discussed whether individuals feel safer conversing in smaller groups and on smaller platforms such as MeWe. However, Telegram remains a favoured option for members of these groups, as they believe their content is safer there.
2. **The growth of online networks:** As online networks grow, their value to users increases. For example, Telegram has become a rich network of extremism and as more users flock to the platform, its value as a communication tool increases, which further encourages potential users to create accounts. On platforms such as Facebook and YouTube, networks grow through hyperlinking, which allows for the connection of disparate groups, and through algorithmic automation. The participants discussed how these problems cannot be solved from an engineering perspective, and there is a need to search for solutions in areas such as public education and inoculation against extremist narratives.
3. **The challenges of deplatforming:** The issue of why deplatforming the far right is more challenging than deplatforming Islamic State was broken down into five key points: (i) There is a category error in the question, as Islamic State is a group while the far right is an ideology and/or scene; (ii) The far right has more support globally than Islamic State ever did; (iii) Most of the online companies/ platforms we discuss are American companies, so according to many users this is a First Amendment or constitutional issue; (iv) Many companies have issues around deplatforming, particularly due to the potential loss of revenue; (v) We need to define the far right and its parameters more clearly in order to disrupt online activity. One of the presenters commented on how much far-right content is not illegal, so it can be challenging to determine what is legal or illegal in different countries, especially when it comes to smaller, less moderated platforms.

The Gamification of Extremism

The Peace Research Institute Frankfurt

22 March 2021

This workshop opened with two presentations. The first presenter discussed gamification, which can broadly be defined as the use of game elements in non-game contexts. She explained that there are four core mechanisms of gamification: entertainment, positive reinforcement, social relatedness and competition.

The second presenter focused on single-actor terrorism and the role of online forums in the radicalisation process. She identified three distinct form of gamification: (i) belonging, recruitment and racialisation; (ii) propaganda; and (iii) gamification of terrorism. The presenter also explained how forums can become an anonymous 'digital home' and an escape from feelings of isolation, while also desensitising subjects and separating emotions from the real world. In order to help prevent radicalisation through online forums, she explained that we must address root causes (for example, how the playworld distances users' emotions from the real world), limit exposure (for example, through moderation in games), digital literacy (for example, for educators), avoid heroic status of shooters (for example, in mainstream media), and detect leakages (for example, when someone mentions violent intentions).

Four core themes arose from these presentations and the ensuing discussion:

1. **The link between playing video games and violent behaviour:** Though often discussed, no direct link has been found between playing violent video games and violent behaviour. Furthermore, there is no single game type that can be associated with extremism and radicalisation. Nonetheless, risk mitigation is important: for example, establishing guidelines for companies to ban far-right behaviour on platforms and in games.
2. **Gamification and memefication as a concerning trend in gaming:** The imitation of an attack through memes has a propaganda aspect and can encourage real-life violence, create a sense of urgency and can radicalise an online audience.
3. **Involvement in certain online communities as a potential indicator for radicalisation:** Extremists are often isolated or were kicked out from other social networks, leading them to join increasingly more extreme forums. However, some terrorists (such as Tarrant) also pulled back from forums and gaming to organise their attack.
4. **The need to understand why certain platforms are chosen by extremists:** It is important to determine whether a platform is being used by extremists to communicate with each other or to game. Furthermore, more research is needed to explore the role of gaming in other potentially violent subcultures: for example, how gaming platforms are used and exploited by such groups as incels.

Extremism in Australia: The Nexus between Terrorism and Technology

Cyber Security Cooperative Research Centre

31 March 2021

This workshop opened with two presentations that delved into an increasingly pertinent topic for Australia: the growing spectre of extremism and terrorism facilitated via online and technological means. The first presenter explained how Australian terrorist cohorts are defined by the ubiquity of family links: family is the key enabler among Australian terror cells, rather than technology, though the latter does play a central role in the communication and distribution of propaganda materials. He added that there is a direct causal link between watching content and carrying out acts, as it fortifies potential actors, like a 'virtual glass of whiskey'.

The second presenter discussed the Internet's role in the radicalisation of far-right actors. She stated that the Internet rapidly radicalises individuals as it acts as an echo chamber. Echo chambers facilitate and accelerate the rate of radicalisation but usually there has to be pre-existing social ties, at least initially. The presenter established various typologies that demonstrate the interface between online content and individuals, noting that the progression is not linear. These typologies are: (i) the 'seeker' – a person who goes online to ask basic questions about their religion, cognitively open to receiving new information; (ii) the 'lurker' – a person who frequents more and more narrow information sources and begins to 'stack them up' around ideological themes and formulate identities on social media; (iii) the 'inquirer' – a person who begins to demonstrate political aggression in posts, the blaming of others, or skewing towards extremist content; (iv) the 'advocate' – a person who begins to engage in trolling, demonstrate confrontational behaviour and make declarations; and (v) the 'activator' – a person who has conducted or commissioned a violent act, often construed as an altruistic act.

Three core themes arose from these presentations.

1. **Family:** Both presenters noted the significant role played by family in drawing Australian extremists 'into the fold', downplaying the impact of technology and media in these initial phases. One participant asked whether any comparative analysis had been conducted on extremist communities in other countries (answer: not yet), noting that it would be interesting to understand how unique these conditions are to Australia, as it would inform local policy responses.
2. **Designing positive intervention programmes:** A discussion emerged around what types of positive intervention programmes can be designed to prevent the progression towards actual physical expression of violent extremist views, and whether or not particular forms of extremism matter in the Australian context when talking about intervention strategies.
3. **The Internet's role:** Apart from the negative impacts raised during the discussion about how the Internet has facilitated extremism, what is its role in mitigating these behaviours?

Challenges Faced by Women Researchers in the Violent Extremism and Tech Field

The International Centre for the Study of Radicalisation | 7 April 2021

This workshop was held to commemorate International Women's Day and it opened with three presentations. The first presenter began by remarking that for the first time in the terrorism field, researchers were beginning to take ethics more seriously and to conduct research on safety issues and concerns. She noted that it can be difficult to remain completely detached from the content a researcher studies if one's identity is constantly targeted by an online community. The researcher may feel under attack with no way of escaping it.

The second presenter shared findings from a survey conducted on the online harms to researchers in the terrorism and extremism field. More women than men are affected by broader cultural issues. For example, both men and women identified problems with 'macho' culture, with men saying that it's easier for women to discuss the difficulties they are experiencing, and with women saying they don't want to admit that they are both experts and victims.

The third presenter discussed online safety measures currently in place of which most researchers aren't aware. She explained that the GIFCT is bringing together open access resources from all member companies and creating a document to make researchers more aware of how to flag harmful content.

Three core themes arose from these presentations:

1. **The need for tailored guidelines:** There is a need for more research on this subject, especially when it comes to women's safety in this field. All of the participants agreed that it would be important to create a charter of guidance that includes coping mechanisms, tips and resources. When creating this charter, it is important to keep in mind that researcher safety issues aren't uniform and that the risks which may arise depend on certain identity markers, such as being a woman.
2. **Different concerns arise when changing research topics:** The presenters noted the difficulty researchers may experience when shifting from one research topic or area to another. For example, a researcher may become adjusted to one type of content, such as jihadist material, and then shift to far-right material, assuming that the shift in content would not have an impact on them. However, different content resonates differently with individuals.
3. **Online visibility:** Online research enables women's research in ways that offline research may endanger them. However, being visible online may make a woman a target for extremist actors. When women put something out into the public domain, they may receive negative or harmful comments about feminism and other topics that detract from their research achievements. This may cause women to reflect on how male researchers would not have received the same sort of commentary and encourage them to self-curate as a risk mitigation strategy in order to avoid this type of commentary. For this reason, women put more pressure on themselves and on how they present themselves online, including on social media.

Studying Online Radical Islamism in France after the Fall of IS

The Middle East and the Mediterranean Chair of Excellence of the Ecole Normale Supérieure | 28 April 2021

The workshop opened with three presentations that discussed the methods and means to conduct research on jihadism and radical Islamism in the digital age. Each presentation lasted 10 minutes and a 30 minute Q&A session followed. The discussion emphasized the necessity of creating new types of research departments, gathering top data scientists and field researchers, to develop the full potential of research in the digital age. It also addressed the benefits and limits of online tools to understand offline political dynamics and how these new approaches could pave the way for European and international partnership, with both universities and tech. The event was private, conducted online, under Chatham House rules, with no public advertisement.

Four core themes arose from these presentations:

1. **Big Data and the question of data sets:** The notion of Big Data refers to a somewhat blurred reality. It is often understood as a set of data too vast to be analysed by a personal computer unit. The expansion of storage and computing facilities have allowed for an unprecedented collection of social data. However, these records fall increasingly outside the scope of any institutional control, in contrast to social statistics that emerged to serve state interests, notably in the two following domains: demographic measurements in population census (1801 in France), and "moral statistics" (among which are crime statistics, which were first conceptualised in France in 1824). Contemporary social data, meanwhile, is more fragmented, more partial and often more precise. We often identify such data as the digital footprint that users leave behind, more or less voluntarily, on digital services. Data of this type require the development of new means of studying social issues, if not new social sciences altogether.
2. **Social Sciences in the Digital Age – opening up new fields of research at the crossroads of quantitative and qualitative methods:** The objective of this project, initiated two years ago by Dr. Hugo Micheron (Princeton / ENS), is to develop a new research unit in Paris, at the crossroad of quantitative and qualitative research in political and religious sociology. The aim is to create a pool of researchers who would be trained in mathematical methods applied to digital technology and data analysis, while also possessing knowledge from the traditional methods of qualitative social sciences (interviews, understanding of the "real-life" field, familiarity with concepts and references of Islamology and philology). The genesis of this project stems from a simple observation based on the current state of studies of jihadism: many tech companies or laboratories have the technical means to organise large-scale research using digital tools, but do not know how to make the most of or analyse the wealth of data captured due to a lack of sufficient expertise on these specific issues. Conversely, some Parisian research departments retain significant qualitative expertise (Arabic speakers, knowledge of ideological references and universes

of meaning) but ignore the full scope of possibilities that basic data processing tools offer. To decompartmentalise the two worlds, a team of engineers and field researchers from Sciences Po, the ENS and the CNRS has been set up and two joint projects have been launched.

3. **Archiving radicalisation occurring on the web:** The first joint project consists in the elaboration of a database (or archive) that compiles the entire intellectual and doctrinal production of French-speaking radical Islamist movements. Such a database previously did not exist, even in fragmented form. This implies archiving content of a heterogeneous nature (texts, audio recordings, videos), filed according to specific metadata (texts, audio recordings, videos), organised on the basis of specific metadata (author, distribution platform, date of issue, target audience, replication, degree of virality). The automatic transcription of audio content makes it possible to compare the content of the texts with the recordings, which was previously difficult to achieve without considerable manpower. The data structure thus produced will take the form of a high-dimensional matrix, which can be studied as a whole or by block, using the most advanced methods available to date. The fact that this type of initiative did not exist in France up until now indicates the extent to which universities and institutions are lagging behind in the digital era, but also the importance of further work in this direction.
4. **Analysing Islamism through the prism of Big Data:** The second project of this partnership is led by a team from the Interdisciplinary Research Centre of Université de Paris and aims to map the ideological re-compositions taking place in jihadist spheres on social networks. Studies on quantitative data produced by radical Islamist movements are garnering interest in the wake of social network analysis. Yet these studies face three limitations:

    i) The use of social networks is either specific and restricted (Twitter) or highly asymmetric (Facebook).

    ii) The content that can be observed on social networks represents only a partial and distorted facet of global social interactions; it is produced by narrow but active communities of authorities, influencers and followers.

    iii) These networks represent ideal venues to test the appeal of specific slogans, to approve new ones and discard others. However, they rarely host structured debates or content creation (although the promotion of content created elsewhere is intense).

For the time being, the work focuses on French-speaking Islamism, but it is possible to envision possible expansions and comparisons, in partnership with other international research organisations, allowing for the study of English, Arab or even Turkish spheres of these social groups.

Right Wing Extremism: East and West

The Centre of Excellence for National Security

5 May 2021

This workshop opened with four presentations that discussed the context and current trajectories of right-wing extremist movements in different countries. Ideologies historically associated with white supremacy may find fertile ground in parts of Asia, where minority identities are contested, and manifestations concurrently resonate and vary from the West. Intolerance and the pervasiveness of echo chambers online may be creating a diffused movement across continents, with opportunities for mimicking tactics and (re)appropriating narratives.

Three key themes emerged from these presentations:

1. **Definitions are required, but are complex and fluid:** The US government employs the term 'Racially or Ethnically Motivated Violent Extremism' (REMVE), which encompasses individuals or groups who promote or conduct violence in the name of defending a perceived ethnic identity, which can be cultural, racial or religious. This broad terminology is not connected to the political spectrum and can encompass many actors around the world. It could apply, for example, to Hindutva attacks on minorities or extremist Israeli settler violence against Palestinians.

   Counterintuitive intersections complicate a fragmented movement. Some far-right groups in the USA claim that they are the 'true multiculturalists', as they seek to preserve cultures by both separation and avoiding dilution. One common strategy is known as the 'greening of hate', whereby white supremacists claim that immigration degrades the environment, often citing the Native American experience as a cautionary tale of what can happen if people don't defend their land.

2. **Online exchange galvanises offline activity, and vice versa:** The vast majority of far-right terrorism is not committed by people attributed to specific groups. Most develop their views through 'self-radicalising networks' online, inspired by group propaganda without necessarily becoming card-carrying members themselves. Narratives typically involve combined sentiments of precariousness and entitlement.

   Over the past fifteen years, symbols of the far-right iconography (in clothing brands, for example) have been recoded to evade legal restrictions and have also transformed and evolved into content for global meme culture. Other concepts have developed among online subcultures and are now commonly seen on flags and clothing at real-world events and violent rallies, further connecting online and offline spaces. Irony and humour are commonly employed to provide the protection of plausible deniability.

3. **Transnational links are facilitated by history and online connectivity, but tempered by context:** Hindutva ideology in India was initially influenced by Italian Fascism and German Nazism during the inter-war period of the 20th century. Its recent resurgence over the past decade maintains links with the West, as witnessed in 2019 when far-right members of the European Parliament visited Jammu and Kashmir. The Hindu diaspora has played quite a pivotal role in supporting Hindu nationalism online since the 1990s. Many overseas Hindutva advocates were employed in the IT sector and had the skills required to access resources and establish online communities.

   Buddhist nationalist rhetoric in Myanmar has appropriated Hindutva memes, but differences in strategic direction probably outweigh any cross-pollination of ideas. The organisation Ma Ba Tha has also established links with other Buddhist nationalist groups such as Bodu Bala Sena in Sri Lanka, and to a lesser extent with comparable groups in Thailand. However, the legislative setting in Sri Lanka and contrasting colonial experiences in Thailand present contextual differences that make it difficult to align agendas.

Online Intervention Programmes Addressing Right Wing Extremism

The Lowy Institute

27 May 2021

This workshop opened with three presentations that focused on online intervention programmes aimed at addressing the rise in right-wing extremism that is facilitated and enabled by computer-mediated communications.

The first presenter briefed the workshop on the work of online intervention programmes that work with partner NGOs to redirect individuals to psychological or social offline support and resources. Through analysis of online searches and behaviours of individuals engaging with extremist content, particularly right-wing and violent conspiratorial content, the presenter found that individuals who were accessing or interested in violent extremist content also had psychological or social needs that required addressing. Their data analysis has found that the coronavirus pandemic, government restrictions and stay-athome directives have significantly increased engagement with far-right extremist content online.

The second presenter discussed online intervention programmes grounded in inoculation theory. Inoculation theory was explained and specific programmes based on inoculation theory were discussed. Inoculation messaging consists of a message of forewarning, a refutational pre-emption and micro-doses of the misleading message. Inoculation has proven to be replicable across cultures and subject areas.

The third presenter discussed recent research that attempted to measure behavioural change and sentiment shifts. The research examined two approaches for measuring theories of change in online audiences exposed to counter-narratives that went beyond basic reach and engagement metrics. The research demonstrated that, contrary to some concerns, counter-narratives do not have unintended consequence of entrenching extremist beliefs. The research has also found that online intervention programmes aimed at directing those individuals who conduct passive online content searches with extremist indicators to offline trained outreach professionals have shown the greatest potential to address engagement with online extremist content.

Three core themes arose from this workshop:

1. **Addressing psychological or social needs:** The limitations of deplatforming, content moderation and presenting counter or alternative narratives emerged as a key theme in these discussions. There is a lot of borderline content that is not targeted for takedown or online activity that cannot be a basis for deplatforming (such as Google searches). Instead, the evidence supports the notion that online intervention programmes need to address individuals' psychological or social needs, especially those that were driving engagement with online extremist and other harmful content. Using search traffic data is very valuable for understanding the scale of engagement with extremist content. There

were discussions around the ethics and privacy considerations of using online search data for redirection efforts to offline service providers.

2. **Inoculation is proving to be an effective means to counter disinformation and extremist narratives:** The application of inoculation theory, as applied to disinformation and violent extremist content, is proving to be effective means of countering violent extremist narratives. There should be efforts to replicate and scale inoculation programming, similar to efforts now underway (such as "Campaign Toolkit") that allow individuals and groups to set up their own counter-hate programmes following a set template or toolkit.
3. **Online redirection programmes do often lead to offline engagement with disengagement resources or programmes:** Focusing on behavioural metrics rather than extremist narratives per se is a more effective means of understanding extremism and creating effective online intervention programmes. Online intervention programmes that direct individuals to offline resources and assistance instead of counter-narrative content could be more effective means to combat extremism.

Extremism in 2021, January 6 and Beyond

Program on Extremism

2 June 2021

This workshop included 11 panellists who are all scholars or practitioners examining best practices for combating violent extremism and understanding the far right. These panellists work to understand the individuals and rationale behind the violence and the forms that domestic extremist violence takes. The workshop's focus was on the state of domestic extremism following the 6 January 2021 riot at the US Capitol; its goal was to foster relevant dialogue and identify key areas of focus and gaps in the field for future research. The panellists were asked to discuss what the academic community has learned about right-wing extremism and accelerationism since 6 January, the landscape of the transnational far right today and the nature of online networks that continue to operate.

Five core themes arose from the presentation.

1. **The important role of the individual:** One panellist noted the importance of individual rationale for participation and the shortcomings that arise from assigning broad labels to these individuals. Lumping people together under group labels without acknowledging this nuance impacts law enforcement's ability to prevent and respond. In domestic extremism, individuals are rarely beholden to a singular group; if a group dissolved tomorrow, many of the members would simply migrate to a different group. It is most helpful to think of them as part of a larger movement and avoid labels. Another panellist agreed that groups do not matter, except in the context of recruitment and mobilisation. Instead of looking at networks, we should focus on tracking named entities interacting in the extremism world.
2. **Comparing jihadism to domestic extremism:** There was some debate over the value of comparing Islamic extremism to domestic extremism. One panellist argued that comparison to jihadist groups is beneficial for recognising the blinders that emerged when studying jihadist groups in the past and applying those lessons to current issues. The panellists discussed the mainstreaming of political violence and debated the challenges posed by the USA needing to look inward, at their friends as neighbours, within the discussion of extremism. A panellist cautioned against equating the ideologies and noted that neither the groups nor the individuals function in the same way. Equating the two forms of extremism without nuance could lead to over-reactions or unfit practices.
3. **Participation versus Membership:** The panellists spoke at length about the challenge of assessing extremist behaviour through the use of data predicated on court records, when every case is inherently a positive variable. It is very difficult to compare violent versus nonviolent extremists in their posting behaviours, actions and affiliations, as there is simply not the data available. Acquiring a better understanding of this would require gaining access to these groups and getting a sense of why people join these movements, what their intentions are and if they are willing to engage in violence. Research is needed to understand whether individuals are acting as keyboard warriors or as potential credible online threats. Two panellists brought up the importance of a gendered lens when trying

to understand participation versus involvement without active mobilisation. They argued that there is a need not just to look at when women do participate, but also why women don't participate. Understanding ideologically aligned individuals versus violent actors is necessary to predict accurately who is a credible threat.

4. **The Role of Violence:** One panelist noted that ambient conditions for violence are also inherently violent. It is incredibly stressful to live under the constant threat of white or male supremacist violence; physical acts of violence are not the only form that violence takes. Consequently, our conception of what constitutes violence widens. For example, both a gunman shooting people and the memes glorifying violence have varying degrees of violent impact. Participation is not just picking up a gun, but a lot of participation is preparation and support for violence.
5. **Gamification:** The role of gamification in the domestic extremism space was raised primarily in connection to QAnon, but also in other groups. A panellist with expertise in this space referred to QAnon as "The ultimate reality game" and noted its ability to move keyboard warriors to commit offline action. In a game, the entire epic story is not laid out all at once; instead, users go through challenges, make decisions and receive clues in order to find out the whole story. QAnon is structured in a very similar fashion in order to keep followers engaged and participating. This type of gamification allows individuals to be engaged and part of the in-group. Many extremist groups use this application to recruit, engage and mobilise potential extremists.