EVENT SUMMARY AND CEP POLICY RECOMMENDATIONS

CEP webinar supported by the Federal Foreign Office of Germany on Nov. 10, 2021:
"The misuse of online services by transnational right-wing extremist and terrorist networks: threats, regulatory countermeasures, and challenges"

Dr. Hans-Jakob Schindler, Alexander Ritzmann, and Marco Macori

Counter Extremism Project (CEP) Germany

COUNTER EXTREMISM PROJECT

Table of Contents

EVENT CONCEPT

Transnational right-wing extremist and terrorist groups and networks have developed specific online ecosystems that are an integral part of their operations. In addition to meetings and gatherings in geographic network hubs, the online sphere plays a crucial role in the transnational functionality of the movement. This is particularly the case during the current COVID-19 pandemic. Within this unorganized collective, individuals and groups feel connected by shared values, actions, and perceived enemies. However, since the overall movement is leaderless and characterized by a variety of organizational models and structures as well as networks of loosely connected individuals, the online ecosystem mirrors this variation and is characterized by an array of online nodes and different sub-milieus and distinct online communities, employing a wide range of strategies and tactics.

In recent years, a range of stakeholders within the tech industry have made efforts to counter the misuse of their services. The Christchurch Call for Action and the development of the Global Internet Forum to Counter Terrorism's (GIFCT) Content Incident Protocol demonstrate this. However, significant failures, such as the failure to quickly contain the spread of the Christchurch attack video or effectively moderate online communities prior to the attack on the U.S. Capitol in January 2021 continue to occur regularly.

Therefore, in addition to voluntary industry initiatives, government regulation is playing an indispensable role by requiring greater transparency, setting standards for moderation, creating legal clarity, and providing commercial incentives through penalty systems, which enable companies to strengthen their defensive mechanisms against misuse by extremist and terrorist actors. In this regard, new legal developments such as the amendments of the German Network Enforcement Act (NetzDG) in 2020 and 2021, the passing of the Terrorism Content Online (TCO) Regulation of the European Union, as well as the ongoing negotiations concerning the future Digital Services Act (DSA) of the European Union and Section 230 of the Communications Decency Act (CDA) in U.S. Congress are crucial developments.

This webinar explored the current situation and regulatory developments and discussed the various challenges encountered by governments and industry in countering this threat. It was the second event in a virtual event series during which the Counter Extremism Project (CEP), supported by the Federal Foreign Office of Germany, examines the various challenges emanating from the transnational right-wing extremist and terrorist movement.

EVENT AGENDA

Moderator
Dr. Hans-Jakob Schindler
Senior Director, Counter Extremism Project (CEP)

Introductory remarks
Gabriele Scheel
Head of Division "International Cooperation against Terrorism, Drug Trafficking, Organized Crime and Corruption", Federal Foreign Office of Germany

Part 1: Methods of misuse
Jacob Davey
Head of Research & Policy of Far-right and Hate Movements, Institute for Strategic Dialogue (ISD)

Alexander Ritzmann
Senior Advisor, Counter Extremism Project (CEP)

Part 2: Developing regulatory framework, challenges and role of industry
Amb. Henri Verdier
Ambassador for Digital Affairs, Ministry for Europe and Foreign Affairs of France

Derek I. Schmeck
Senior Policy Advisor, Bureau of Counterterrorism, U.S. Department of State

Yolanda Gallego-Casilda Grau
Head of Unit "Prevention of Radicalization", DG Migration & Home Affairs, European Union

Dr. Erin Saltman
Director of Programming, Global Internet Forum to Counter Terrorism (GIFCT)

EVENT VIDEO RECORDING

Please find the available video recordings here (playlist):
https://www.youtube.com/playlist?list=PLMgGq1NecSpapvZ8IORDgcfGpz1ettg5H

SUMMARY OF PRESENTATIONS

Introductory remarks

Gabriele Scheel

Head of Division "International Cooperation against Terrorism, Drug Trafficking, Organized Crime and Corruption", Federal Foreign Office of Germany

Violent right-wing extremist and terrorist networks continue to be one of the most significant security threats in Germany. As a consequence, Germany has put into force a comprehensive legislative package, including specifically tailored updates to the already existing the NetzDG law, to fight the misuse of online services by right-wing extremist and terrorist networks. Online extremism has seen a significant increase during the COVID-19 pandemic, requiring continuing action. Right-wing extremist and terrorist networks cannot be fought only on the national level alone. Their growing transnational connections require a multilateral approach to combat this threat.

Part 1: Methods of misuse

Jacob Davey

Head of Research & Policy of Far-right and Hate Movements, Institute for Strategic Dialogue (ISD)

Over the past five years ISD has built a wide-ranging global repository of right-wing extremist activity across the United States, Canada, the United Kingdom, Australia, New Zealand, Germany, and France. This dataset contains more than 25,000,000 messages sent by over 20,000 accounts, pages, groups, and channels since 2019.

The threat we face – a fringe insurgency:

Over the past decade, we have seen a wholesale transformation of the extreme right ecosystem and threat. This is intrinsically linked to online mobilization. What were primarily localized nationally oriented groups have transformed into large scale, tech savvy movements with an international reach that are able to translate online mobilization into effective offline action. The threat has become increasingly hybridized: there is an increasing intersectionality between disinformation, conspiracy theories, targeted hate, harassment, and violent extremism. This is further amplified by covert and overt information operations conducted by malign state actors as well as algorithmic amplification of hateful and extreme messaging on social media platforms.

This online coordination has significantly impacted the extreme right wing:

- An increasingly empowered and violent set of extreme right-wing actors;
- Mainstreaming of extremism, with extremist movements enlarging their sphere of influence, reaching a significantly expanded audience;

- A transnational dynamic, where extreme right-wing movements adopt shared cultural, ideological, and tactical tropes and coordinate across borders to advance their worldview;
- The emergence of post-organizational terrorism and mobilization to violence where activity does not emanate just from organized groups, but from loose (often online) communities and individual actors.

Funding:

ISD analyzed the digital footprint of 17 extreme right-wing groups in Germany, examining their use of 20 different funding mechanisms. The study found 79 instances of these groups using online mechanisms. 12 of the platforms used by these groups had outlined in their terms of service that they prohibit the use of their services by hate groups. This demonstrates that there are gaps both within the policy framework of these platforms as well as in their policy enforcement mechanisms. These results correspond to similar trends observed in the United States, where extremists used a wide range of platforms despite the fact that these platforms had policies outlining that they would not allow extremists to use their services.

Gaming:

ISD also analyzed four platforms with close ties to gaming communities: Twitch, Dlive, Steam, and Discord. This study found that these hosted a wide range of extreme right-wing communities, including supporters of proscribed neo-Nazi organizations. The average age of users on extreme right Discord servers was 15 years. The analysis found limited evidence that gaming was being used as part of a concerted strategy to radicalize and recruit new individuals. Instead, ISD's analysis suggests that in online spaces populated by the extreme right, gaming acts as a means of bringing already radicalized people together.

Alexander Ritzmann

Senior Advisor, Counter Extremism Project (CEP)

Major findings of new CEP research and analysis on the extreme right-wing infrastructure on Facebook, Instagram, YouTube, and Twitter in Germany:

Through an in-depth mapping exercise, this CEP research and analysis project produced an inventory of the most relevant actors of right-wing extremism in Germany. Based on criteria such as the number and relevance of activities (e.g., concerts, festivals, martial arts events, rallies, orientation towards violence, propaganda activities, as well as national and transnational networking), a total of 100 individuals, organizations, music labels, bands, fashion brands and companies were identified as (in many cases violence-oriented) key right-wing extremist actors.

A large proportion of these key actors in the various German right-wing extremist milieus are still present on Facebook, Instagram, YouTube, and Twitter. However, generally, they no longer carry out illegal activities there. For the most part, they also do not violate the respective companies' general terms and conditions or community standards with regards to hate speech or similar offences in order to avoid being permanently blocked from the platforms.

These far-right extremists are now pursuing a strategy of "extreme normalization" on major social media outlets. Nonetheless, they remain the same key right-wing extremist actors who form the basis of Germany's transnational right-wing extremist scenes through festivals, fashion brands and mixed martial arts tournaments.

Beyond their activities on major social media and video-sharing platforms, these key actors remain architects as well as advocates of dangerous conspiracy myths and narratives of group-based misanthropy that increase the likelihood of violence and terrorism.

Since many right-wing extremist key actors explicitly pursue economic interests, they use social media to promote their merchandise stores, martial arts associations, music labels, bands, and survivalist (or prepper) organizations and to reach new customers and to recruit new followers and members.

On smaller platforms, messenger services and offline, they show their true colors. Through their actions there, they build the foundation for the (transnational) right-wing extremist milieu in Germany.

Of the total 100 identified (violence-oriented) far-right key actors:

Facebook: 54 profiles can be assigned to 41 key actors, with a total of 267,743 subscribers/friends. Of these 54 profiles, 39 have explicit economic purposes.

Instagram: 37 profiles can be assigned to 34 key actors, with a total of 82,957 followers. Of these 37 profiles, 24 have explicit economic purposes.

YouTube: 33 profiles can be assigned to 27 actors, with a total of 82,160 subscribers. Of these 33 profiles, 15 have explicit economic purposes. The total number views for all videos is 9,594,861.

Twitter: 17 profiles of 16 actors were identified with a total of 6,818 followers. Of these 17 profiles, 9 have explicit economic purposes.

While a large part of known (violence-oriented) German far-right movement-entrepreneurs are present and active on Facebook, Instagram, YouTube, and – to a much lesser extent – Twitter, big tech is to some extent engaged in countering hate speech, extremism, and terrorism on their platforms. However, established policy dialogues that focus on the self-regulation of this industry as well as workshops with civil society groups are usually limited to harmful or illegal behavior on the platforms themselves. As our research shows, however, key German (violence-oriented) right-wing extremist actors have adapted their strategies for propaganda, recruitment and funding to avoid being banned from popular social media platforms.

Concerns regarding an excessive limitation of freedom of expression through content moderation and the enforcement of terms of service by the platforms need to be discussed. This fundamental right is, however, designed to protect against government censorship and oppression and does not apply in a commercial relationship between companies and consumers/users.

The question of whether users can legally compel social media platforms to enforce their own community standards and delete profiles of, for example (violence-oriented) extremist actors

or hate organizations, is a complicated legal issue and requires further exploration. If this would be established as a legal obligation, this would break new legal ground in Germany. It seems obvious, however, that if community standards promise a somewhat “safe space" to users, this promise should be honored and activities of violence-oriented extremists, in particular commercial operations which fuel their violence, are highly problematic.

Part 2: Developing regulatory framework, challenges, role of industry

Amb. Henri Verdier

Ambassador for Digital Affairs, Ministry for Europe and Foreign Affairs of France

It is important to note that the internet of the 1990s and early 2000s was characterized by open and neutral platforms that had an overwhelming positive effect on society. This has changed and the online sphere is now dominated by social networks which are centralized, closed, not neutral, and cause harm. There is a coherent, continuous spectrum of threats ranging from misinformation to terrorist activities. One central issue is algorithmic amplification. Therefore, algorithms of social media platforms require regulation. Online terrorist content has become an intrinsic part of any terrorist operation in order to achieve maximum impact. This was tragically demonstrated by the life-streaming of the Christchurch attack.

As a consequence, the Christchurch Call for Action was developed as an essential step in terms of countermeasures. The GIFCT database of hashes is one positive outcome of this action another is the incident crisis protocol, which was already tested but require continuous development. Positive is also that this multi-stakeholder approach is growing as far as participants is concerned, which includes governments and civil society organizations. However, in the future more focus should be put on smaller online platforms, as well. Moreover, difficult issues such as algorithmic amplification of terrorist content on major platforms are not yet solved. Therefore, a mix of voluntary and regulatory approaches is needed to counter the threat of online extremism and terrorism.

Derek I. Schmeck

Senior Policy Advisor, Bureau of Counterterrorism, U.S. Department of State

Recent high-profile attacks by racially or ethnically motivated violent extremist (RMVE) actors indicate a growing transnational connectivity, particularly through online communities.

The Biden administration’s priorities/actions are, inter alia:

- The State Department is working on a range of countermeasures, such as a study on global connections of threat actors or the development of interagency knowledge collection.
- A comprehensive review of how the U.S. government tackles domestic terrorism
- The release of the new National Strategy for Countering Domestic Terrorism (including strengthening of prevention programs and resilience to extremist messages; online

counter-recruitment; increased support for local enforcement; increased collaboration with civil society)

In all efforts of the U.S. government, the focus is on the voluntary enforcement of community standards by online companies so that freedom of speech is not impeded. However, analysis of potential future regulation/legislation, especially regarding algorithmic amplification is ongoing. Finally, the United States has joined the Christchurch Call this year and is looking forward to effective collaboration in this forum.

Yolanda Gallego-Casilda Grau

Head of Unit "Prevention of Radicalization", DG Migration & Home Affairs, European Union

The European Union's approach concerning countermeasures includes both the development of regulation and the encouragement of voluntary action by online platforms. The Terrorist Content Online (TCO) Regulation responds to the need to tackle online content disseminated by terrorists in order to spread their message, to radicalize and recruit followers, and to facilitate and direct terrorist activity. It will be fully in force in June 2022.

TCO Regulation – Main Features:

- Removal orders:
  - Binding instrument for hosting service providers (HSPs)
  - Assessment of content is done by Member States no further assessment by HSPs
  - HSPs remove within 1 hour after order is received
  - Feedback to issuing authority of removal order
- Specific measures:
  - HSPs exposed to terrorist content: apply terms and conditions
  - Decision which measures to apply (human or automated) is done by HSP
  - National authority can request that additional measures are taken by HSP
  - HSP to report on measures implemented
- TCO regulation – safeguards:
  - Annual transparency reports by HSPs and competent government authorities
  - Educational, journalistic, research, and artistic content is exempt
  - Information to content providers and complaint mechanism
  - Judicial redress is ensured
  - Host Member States of HSPs can review removal orders
  - Content provider and HSP can ask for review

Voluntary-Based Cooperation: EU Internet Forum – Knowledge Package:

- Support to voluntary content moderation efforts by companies
- Contains terrorist groups, symbols, and manifestos on the basis of Member States' input
- Yearly releases with updated information

Dr. Erin Saltman

Director of Programming, Global Internet Forum to Counter Terrorism (GIFCT)

The Global Internet Forum to Counter Terrorism (GIFCT) is an NGO designed to prevent terrorists and violent extremists from exploiting digital platforms. Founded by Facebook, Microsoft, Twitter, and YouTube in 2017, the Forum was established to foster technical collaboration among member companies, advance relevant research, and share knowledge with smaller platforms. Since 2017, GIFCT's membership has expanded beyond the founding companies to include over a dozen diverse platforms committed to cross-industry efforts to counter the spread of terrorist and violent extremist content online.

Four foundational goals guide the newly independent organization's work:

- Empower a broad range of technology companies, independently and collectively, with processes and tools to prevent and respond to abuse of their platforms by terrorists and violent extremists
- Enable multi-stakeholder engagement around terrorist and violent extremist misuse of the Internet and encourage stakeholders to meet key commitments consistent with the GIFCT mission
- Promote civil dialogue online and empower efforts to direct positive alternatives to the messages of terrorists and violent extremists
- Advance broad understanding of terrorist and violent extremist operations and their evolution, including the intersection of online and offline activities.

GIFCT is governed by an Operating Board made up of members from the Forum's founding companies: Facebook, Microsoft, Twitter, and YouTube. GIFCT is advised by an Independent Advisory Committee made up of representatives from civil society, government, and intergovernmental organizations.

In 2017, the founding members of GIFCT spearheaded a shared, safe and secure industry database of "perceptual hashes" of known images and videos produced by terrorist entities on the United Nations designated terrorist groups lists- which GIFCT members had removed from their services.

One of the most important ways GIFCT facilitates this effort is by streamlining member communication as they each respond to terrorist and violent extremist attacks in which those responsible use digital platforms as part of their violence. Following the attacks in Christchurch, New Zealand in March 2019, GIFCT members established a centralized communications mechanism to share news of ongoing incidents that might result in the spread of violent content tied to the specific incident unfolding. These communications allow for widespread situational awareness and a more agile response among member companies.

The Global Network on Extremism and Technology (GNET) is the academic research arm of GIFCT.

CEP POLICY RECOMMENDATIONS

- A mix of regulatory and voluntary approaches seems necessary in countering extremism and terrorism online. However, the current regulatory framework requires further development. In addition to addressing algorithmic amplification, the current “Notice and Action” system, exemplified by the removal orders of the EU TCO, should be further refined. Currently platforms are only required to address content if a removal order is received. Such a system cannot be effective as far as global platforms with millions of uploads are concerned. Outside monitoring by a limited number of competent authorities can never have full visibility of all content on a global platform. Therefore, internal platform defense mechanisms, operating on regulated standards and procedures and effectively audited by competent authorities are necessary.
- Competent authorities, such as for example Internet Referral Units (IRUs) should develop further expertise and capacities focused on violence-oriented right-wing extremist actors. The EU Internet Forum knowledge package is a first positive step in this direction. However, competent authorities should also ensure that sufficient technical expertise exists to effectively analyze and audit measures taken by platforms.
- Civil society and policymakers must make clear to the major platforms negligent behavior of allowing key (violence-oriented) right-wing extremists on social media, even if they don’t explicitly violate the rules there, is dangerous and should not be permitted, in particular when these activities generate financial profits for these actors and fuel violent extremism. At minimum they present significant reputational risks for platforms as their services financially enable violent extremist actions.
- A more systemic perspective on "Dangerous Persons and Organizations"—as set out in the most recent Facebook policy for example, which also includes the behavior of users outside the platforms—should be added to the mission statements of policy dialogues such as the EU Internet Forum, the Christchurch Call for Action and the Global Internet Forum to Counter Terrorism (GIFCT). As the Facebook policy example shows, implementation is as important as policy.
- The draft EU Digital Services Act (DSA) could open up the possibility that providers must enforce their community standards to protect their users. Art. 12(2) regulates that providers must act "carefully" and, among other things, "objectively" when applying their contractual regulations. It should therefore be made clear that the regulations must also be applied "effectively" to protect users. This opportunity should be clarified and strengthened.
- Due to the limited-liability privilege, the existing legal framework in the United States and the EU does not provide sufficient incentives for social media companies to put their best experts and the resources necessary into fixing the rampant hate speech, as well as extremist and terrorist content, on their platforms. At the moment, even the biggest companies do not need to take down illegal or harmful content unless someone gave them notice to act. This even applies when illegal and/or harmful content gets recommended to users by the platform. Hence, the liability regime needs to be updated to represent and manage the challenges users, governments and companies face today.