Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

EU POLICY: PREVENTING THE DISSEMINATION OF TERRORIST CONTENT ONLINE

This paper, part of the Legal Perspectives on Tech Series, was commissioned in conjunction with the Congressional Counterterrorism Caucus

JORDY KRASENBERG

SEPTEMBER 2019

About the Program on Extremism

The Program on Extremism at George Washington University provides analysis on issues related to violent and non-violent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public.

About the Author

As an advisor at RadarAdvies, Jordy is involved in different projects focused at the public and social domain. These projects are commissioned by municipalities, city districts, ministries, companies and the European Commission. Jordy has been a core staff member and expert in the RAN Centre of Excellence (CoE) since 2017 and has been active in the field of preventing and countering radicalisation for over 4 years. At the RAN, he focused mostly on early prevention, internet and online (de)radicalisation, mental health issues, multi-agency working, lone actors, social care and formal and informal education. He supported, both on process and content the working groups RAN Education, RAN Health and Social Care and CSEP. He first started working on preventing radicalization and counterterrorism in Kuwait, for the Dutch Ministry of Foreign Affairs and has since then been active in adjacent fields, notably inclusive education and the integration and empowerment of minorities and undocumented asylumseekers in the Netherlands. He has delivered multiple workshops on the prevention of online extremism. Additionally, he was active as a board member and treasurer of the social liberals parties think tank on integration, polarisation, radicalisation and other societal issues. Jordy has a university degree in history and international relations, and focused his studies on European integration, policy and legalisation.

The views expressed in this paper are solely those of the author, and not necessarily those of the Program on Extremism or the George Washington University.

Executive Summary

The use of the internet for recruitment and the dissemination of violent extremist materials raises significant policy challenges for the European Union (EU), its Member States, and content sharing platforms (CSPs) [1] alike. This problem requires – through the eyes of the EU – a combination of legislative, non-legislative, and voluntary measures based on collaboration between authorities and CSPs with respect for fundamental (human) rights.

Introduction

Recent terrorist attacks across the world have demonstrated how terrorists abuse the internet to groom and recruit supporters, prepare and facilitate terrorist activity, glorify their atrocities, and urge others to follow suit and instill fear in the general public. Because of this, social media is a powerful marketing tool for an extremist or extremist group.

It seems unlikely that these forces can be driven off the internet entirely, but it is possible to take legal and non-legal action to make it more difficult for potential new recruits to find extremist content and conversations. In the last decade, we've witnessed the development and application by supranational institutions, governments, the private sector and civil society of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the internet. These actions have placed social media at the center of a conflict between users' rights to free speech and the public demands of preventing terrorism and crime.

This presents the public with daunting practical challenges around how unprecedented flows of mediated communication and interaction can be effectively monitored and managed. The regulatory architecture that will emerge in response to these tensions and dilemmas may have far-reaching consequences for many years to come.

This paper will address concrete policy and legislative steps that have been adopted in recent years and some that are at the time of writing still in the making by the European

Union. These steps are meant to tackle the dissemination of terrorist content and to push the social media industry and civil society actors to do more. This paper aims to provide an oversight of these policy and legislative choices.

EU Internet Forum

Beyond the legislative proposals, tackling the challenge of terrorist content online is a common effort that will require more cooperation between the private sector and public authorities. Voluntary arrangements under the EU Internet Forum (EUIF) have produced mixed results.

The EUIF reached out to platforms including: Facebook, YouTube, Microsoft, Twitter, Internet archive, Justpaste.it, Wordpress, Snap, Soundcloud, Baaz, Dropbox, Mega, Userscloud and Telegram. Under the EUIF, more specific indicators for terrorism-related reporting have been developed. Platforms have general reporting mechanisms in place. However, not all companies provide specific terrorism-related reporting.[2]

The European Commission (EC) expects public-private cooperation under the EU Internet Forum to not only continue, but to strengthen in the future. Tech companies and governments also agreed to work together to counter violent extremism by developing interventions to redirect users away from extremist content. Nonetheless, a continuation or strengthening of the voluntary approach was discarded by tech companies and the Commission alike as not being sufficient enough for tackling terrorist content.[3]

Towards Legislation

Just as with the new European GDPR privacy law, Europe might still play a pioneering role. This problem requires a combination of legislative, non-legislative, and voluntary measures based on collaboration between authorities and providers, with respect for fundamental (human) rights. Some of the threat of illegal content has been mitigated by successful initiatives such as the social media industry-led *Code of Conduct*[4] on countering illegal hate speech online. However, it is necessary to establish a legislative

framework for cross-border cooperation between national regulatory authorities to take down illegal content.

A legislative proposal on terrorism content control has been under consideration since September 2018 amid fears that terrorist content on social media is contributing to radicalization.[5] The issue took on a new urgency following the mass shooting at two mosques in Christchurch, New Zealand -- footage of which rapidly spread around the internet via Facebook Live. *The Christchurch Call to Action: To Eliminate Terrorist and Violent Extremist Content Online* text outlines "collective, voluntary commitments" from governments and internet companies[6]. Seventeen countries, the EC, and eight major tech companies have signed the non-binding accord.[7] These include ensuring that there are effective counter-terrorism laws regarding the internet and that proactive measures are being taken to remove extremist content from social media.

Limitations stem from the voluntary approach: For example, the reliance on commitments from companies, the limited outreach, the limited level of progress, and the need to significantly reduce accessibility to terrorist content.[8]

The EU, the big players of the social media industry, and many EU Member States have recently agreed that the previous model – focused on self-regulation and voluntary content control by social media companies—has failed to effectively address online radicalization.[9]

The result is a shift in the discourse across Europe, increasingly moving towards mandatory national and EU leveled legislative measures that make use of direct institutional oversight and incorporate the **"**responsibilization"[10] of CSPs. Additionally, the new proposal gives the EC the option to use legislation for punitive and criminal law sanctions against such companies if they fail to act.

Part of the Commission's engagement with social media companies will involve monitoring and ensuring accountability. There is also the expectation that Member

States will adopt their own legal framework in their respective countries to make CSPs more responsible for the online content they host. The aim of the regulatory proposal is to reinforce these efforts and ensure that all companies at risk comply with a minimum set of requirements.

Terrorist Content Regulation

The European Commission (EC) is, at the time of writing, working on a legislative proposal to improve the detection and removal of illegal and terrorist content.[11] The need to enhance action in relation to terrorist content online has also been reflected in calls by the EU Member States, and some (e.g. Germany's NetzDG law[12]) have already legislated or have expressed plans to do so.

These laws do not come without criticism. Serious concerns have been raised about the Regulation's supposed ineffectiveness in combating violent extremism, collateral damage for human rights, and disparate impact on racial minorities, as well as the anti-competitive impact of requiring small businesses to adopt expensive and poorly understood filtering technologies.[13]

Much of the following is concerned with what is called 'terrorist content control'.[14] These are efforts by the EC to regulate, on a supranational level and national level and in collaboration with CSPs, what material is available on the internet and allows for the removal of accessible yet 'objectionable' content and the erection of barriers to the uploading of such materials in the future.

The proposed rules aim to fully respect the fundamental rights in the EU – notably those guaranteed in the Charter of Fundamental Rights of the European Union[15] – and should only concern the spread of terrorist content online. Parliament backed the legislation with 308 votes in favor and 204 against, and now will have to negotiate the text with the EU's Council of Ministers.

The rules proposed by the Commission have the potential to set a clear legal framework

and will help ensure terrorist content online is swiftly removed from platforms**.** This is best described in Amendment 7 of the proposal, Recital 4 which states that**:**

> "*This legislative framework seeks to build on voluntary efforts, which were reinforced by the Commission Recommendation (EU) 2018/3347 and responds to calls made by the European Parliament to strengthen measures to tackle illegal and harmful content in line with the horizontal framework established by Directive 2000/31/EC[16] and by the European Council to improve the detection and removal of content that incites to terrorist acts."*[17]

For the purpose of this paper, a short oversight will capture some of its key features[18], but will not delve deeper into their possible implications and the ongoing discussions.

The one-hour rule

Informally, the one-hour rule already existed among some of the bigger platforms, but as Christchurch demonstrated, it had limited results. The fast removal of or disabling of access to terrorist content is often essential in order to limit wider dissemination and potential harm. Thus, CSPs should be able to take quick actions. To strengthen public security and combat radicalization, CSPs should remove terrorist content within one hour after receiving an order from the authorities.

Terrorist content is considered most harmful in the first hours after it appears online because of the speed at which it spreads and therefore its reach. With this in mind, the Commission proposed a legally binding one-hour deadline for content to be removed following a removal order from national competent authorities.

Strong and Deterrent Financial Penalties

Member States will have to effectively and proportionately penalize companies for not complying with orders to remove online terrorist content. In the event of systematic

failures to remove such content following removal orders, a CSP could face financial penalties of up to 4% of its global turnover for the last business year.

A Duty of Care Obligation

Depending on the risk of terrorist content being disseminated via their platforms, social media companies will also be required to take proactive measures – such as the use of new tools – to better protect their platforms and their users from terrorist abuse. Companies would have to invest in technology that improves capability to detect (e.g. automated detection tools) and remove terrorist and violent extremist content online.

Although agreeing with most of the proposal, the Civil Liberties Committee (LIBE)[19] rejected the 'duty of care obligation' claiming platforms would subsequently be obligated to monitor content and filter uploads using automated detection tools.

The challenge is that any proactive measures should be proportionate to the risk and the economic capacity of the company involved. For internet giants, with plenty of capacity available to them, this wouldn't be as much of a challenge compared to smaller companies with limited capacity.

Increased Cooperation

The proposal sets up a framework for strengthened co-operation between CSPs, Member States and Europol. CSPs and Member States will be required to designate points of contact reachable 24/7 to facilitate the follow-up to removal orders and referrals.

National authorities are tasked with detecting and identifying terrorist content, and issuing removal orders and referrals. In doing so they should cooperate with CSPs, the authorities in other Member States, and with Europol. To avoid duplication and possible interferences with investigations, they should inform and cooperate with each other and Europol when issuing removal orders or sending referrals to CSPs.

Strong Safeguards

The proposal pushes platforms to increase blocking illegal content using private Terms of Service (TOS). This is not without risk, so the proposal contains a number of safeguards to address freedom of expression concerns.

Most importantly, the proposal requires platforms to allow users to submit complaints if they believe their content has been removed unjustifiably. Where content has been removed unjustifiably, the CSP will be required to reinstate it as soon as possible. Furthermore, the proposal requires human oversight and verification of automated tools that remove terrorist content to prevent unjustified removals.

Content providers will be able to rely on effective complaint mechanisms that all platforms will have to put in place. Lastly, effective judicial remedies should also be provided by national authorities and platforms or content providers will have the right to challenge a removal order.

Increased Transparency and Accountability

Annual transparency reports required from CSPs and Member States on how platforms tackle terrorist content, as well as regular reporting on proactive measures, will guarantee transparency and oversight.

Provisions to ensure transparent processes, and reporting to authorities and the Commission, would increase the accountability and trust in the content moderation process. It would also support policy-makers and national authorities in combating terrorist content and allow users to better understand how hosting service providers apply their content management policies.[20]

Empowering Alternative Narratives

Reducing accessibility to terrorist content online is only one aspect of the EU's response to online radicalization. Terrorist and extremist groups are adept at capitalizing on technology and social media to spread their propaganda, and to radicalize and recruit supporters. Many civil society organizations are actively providing alternative narratives and sharing moderate voices, but they often lack the capacity or resources to produce and disseminate these messages effectively online.[21]

The EUIF also aims to empower civil society partners to increase the volume of alternative narratives online. Parallel to the legislative response and the use of filtering tools, the Commission has been supporting civil society actors in the promotion of credible, positive alternatives and counter-narratives. Through the Civil Society Empowerment Programme (CSEP), the Commission aims to provide civil society actors with the skills and knowledge to deliver effective online campaigns and has been launched to support credible voices in the dissemination of positive, alternative narratives throughout Europe.[22]

Following a pan-European training program for civil society partners in 2017, a first call for proposals in 2018 lead to the selection of 11 projects for funding. The projects were launched in Brussels on 30-31 January 2019 through CSEP and are underway at the time of writing.

Conclusions

The EU's response on preventing the dissemination of terrorist content has been built on trial and error through collaborations and voluntary arrangements and is now taking the next step towards legislation. The EU is recognizing that terrorism and radicalization are complex societal problems that require all of society, including the online world. The internet for all its benefits and despite a scientific lack of understanding on the social implications and effects of terrorist content, is in need of a legislative framework to comprehensively address these issues.

Because online threats have no borders, tech companies should be held to consistent

standards -- they need clarity about their options to act and the consequences if they don't. In this regard, the proposal raised some significant issues that needed to be addressed. Despite some vital amendments, the proposal will still need more political agreement before it is enacted into law. The proposal is, to the authors knowledge, unprecedented and shows strong political will to act despite the risks involved. Whatever the outcome, the EU and most of its Member States can no longer accept the current status quo.

Legislation on removing perceived hateful and possibly dangerous voices online should work in concert with civil society and positive voices. One of the key lessons is that effective online counterterrorism measures and the protection of freedom of expression are not conflicting per se, but have the potential to be complementary and mutually reinforcing. The importance of taking measures to prevent the dissemination of terrorist content online is clear to all, even its most prominent critics.

The Council, the Commission, and Parliament need to ensure that the collective efforts to address these challenges remain effective, efficient, and consistent with applicable human rights principles.

Suggested Sources

- P8_TA-PROV(2019)0421 Tackling the dissemination of terrorist content online ***I European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD))
- http://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.pdf?redirect
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018
- COM/2018/640 final
- https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640
- The Christchurch call
- https://blogs.microsoft.com/on-the-issues/2019/05/15/the-christchurch-call-and-steps-to-tackle-terrorist-and-violent-extremist-content/
- http://www.europarl.europa.eu/news/en/press-room/20190410IPR37571/terrorist-content-online-should-be-removed-within-one-hour-says-ep
- https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online
- https://www.ivir.nl/publicaties/download/TERREG_FoE-ANALYSIS.pdf
- https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf

References

[1] This includes social media platforms and online content sharing services.
[2] Twitter invested in such specific transparent reporting mechanisms.
[3] 2018/0331 (COD). European Commission, Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online, Brussels: European Commission, 12.9.2018, page 25.
[4] ***Code of conduct.*** The Commission has set up a number of sectoral dialogues with stakeholders or initiated other self-regulatory and voluntary mechanisms which inter alia have dealt with the removal of (possible) illegal content. The implementation of the Code of Conduct on countering illegal online hate speech shows that voluntary collaboration can yield very positive results in a relatively short time. Currently 70% of illegal online hate speech is removed upon notification and in more than 80% of the cases the assessment is made within 24 hours. The initiative has also been extended to other online platforms.
"JUST Newsroom - Countering Illegal Hate Speech Online #NoPlace4Hate - European Commission," accessed June 24, 2019, https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.
[5] 2018/0331 (COD). European Commission, Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online, Brussels: European Commission, 12.9.2018.
[6] "The Christchurch Call and Steps to Tackle Terrorist and Violent Extremist Content," Microsoft on the Issues, May 15, 2019, https://blogs.microsoft.com/on-the-issues/2019/05/15/the-christchurch-call-and-steps-to-tackle-terrorist-and-violent-extremist-content/.
[7]"The Christchurch Call and Steps to Tackle Terrorist and Violent Extremist Content," Microsoft on the Issues, May 15, 2019, https://blogs.microsoft.com/on-the-issues/2019/05/15/the-christchurch-call-and-steps-to-tackle-terrorist-and-violent-extremist-content/.
[8] Only a small fraction of affected CSPs have engaged in the EUIF).
[9] Additionally, there have been many other scandals related to social media platforms (such as those related to "fake news," electoral manipulation by foreign agents, and even the misuse of users' personal data).
[10] *Majid Yar*, A Failure to Regulate? The Demands and Dilemmas of Tackling Illegal Content and Behaviour on Social Media, the International Journal of Cybersecurity, Intelligence and Cybercrime, vol.1, issue 1, (Boston 2018).
[11] The proposal is the first legislative text in Europe, together with the new copyright proposal, to require proactive filtering of illegal content, breaking with the e-Commerce Directive approach to intermediary liability. The proposal builds on earlier policy documents released by the European Commission in the broader area of tackling illegal content online, and the co-regulatory initiatives of the EU Hate Speech Code of Conduct and the EU Internet Forum.
[12] "» Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG) German Law Archive," accessed June 24, 2019, https://germanlawarchive.iuscomp.org/?p=1245.
[13] "The EU's Terrorist Content Regulation: Expanding the Rule of Platform Terms of Service and Exporting Expression Restrictions from the EU's Most Conservative Member States," accessed June 24, 2019, /blog/2019/03/eus-terrorist-content-regulation-expanding-rule-platform-terms-service-and-exporting.
[14] Maura Conway, Terrorism and Internet governance: core issues. Disarmament Forum, 3, (Dublin 2007) 23-34.
[15] "Charter of Fundamental Rights of the European Union," accessed June 24, 2019, https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[16] The directive covers all speech-related claims against platforms, from crimes to small-scale copyright infringement. It requires internet hosts that know about unlawful content to remove it, or face liability themselves.
[17] "REPORT on the Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online," accessed June 24, 2019, http://www.europarl.europa.eu/doceo/document/A-8-2019-0193_EN.html.

[18] "European Commission - PRESS RELEASES - Press Release - State of the Union 2018: Commission Proposes New Rules to Get Terrorist Content off the Web," accessed June 24, 2019, http://europa.eu/rapid/press-release_IP-18-5561_en.htm.
[19]"Highlights | Home | LIBE | Committees | European Parliament," accessed June 24, 2019, http://www.europarl.europa.eu/committees/en/LIBE/home.html.
[20] "Soteu2018-Preventing-Terrorist-Content-Online-Swd-408_en.Pdf," accessed June 24, 2019, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf, page 27.
[21] Hayet OUFERROUKH, "EU Internet Forum: Civil Society Empowerment Programme," Text, Migration and Home Affairs - European Commission, March 2, 2017, https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en.
[22]"European Commission - PRESS RELEASES - Press Release - State of the Union 2018: Commission Takes Action to Get Terrorist Content off the Web - Questions and Answers," accessed June 24, 2019, http://europa.eu/rapid/press-release_MEMO-18-5711_en.htm.