Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

DISINFORMATION IN TERRORIST CONTENT ONLINE

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

NINA JANKOWICZ

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

Nina Jankowicz is a Global Fellow at the Wilson Center's Kennan Institute, where she studies the intersection of technology and democracy in Eastern Europe. Her forthcoming book, How to Lose the Information War, will be published by Bloomsbury's IBTauris in 2020.

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.

"Wherever we live, whatever our background, we've all seen the pain caused by senseless acts of terrorism. Just last week, the tragic murder of Christmas shoppers in Strasbourg was a sobering reminder that terrorist attacks can happen at any time. What is clear from such attacks is that we all—government, industry, and civil society—have to remain vigilant and work together to address this continuing threat."

So begins a 2018 blog post from Google's Kent Walker, Senior Vice President of Global Affairs and Chair of the Global Internet Forum to Counter Terrorism (GIFCT).[1] It shows solidarity. It shows community. It shows a common understanding of a threat. In short, this passage displays the key underpinnings of a successful whole-of-society coalition to counter dangerous online content, and while it's not perfect, I envy it.

Though criticized for their delayed reaction, the coalition of tech giants known as GIFCT began working together to curb online terrorist content in late 2016. Facebook, Microsoft, Twitter, and Google announced the creation of a shared "hash database," in which "digital fingerprints" of terrorist content are stored so that organizations might "identify such content on their services, review against their respective policies and definitions, and remove matching content as appropriate."[2] The partnership behind database was formalized in June 2017 as the GIFCT, and grew to include other Internet platforms, such as Ask.fm, Cloudinary, Instagram, Justpaste.it, LinkedIn, Oath, Reddit, Snap, and Yellow.[3] Since the initiative began, the companies added 100,000 hashes to the database.[4] Using this information, Twitter permanently banned over 270,000 accounts in the initiative's first six months,[5] while over the course of 2018, Facebook removed over 14 million pieces of terrorist content.[6]

The partnership has sustained its share of criticisms, however. Because each platform uses its own definitions and terms of service to determine which content to remove, the transparency of the efforts has been criticized from the start. This year, as the European Parliament discussed regulations that would require the proactive monitoring and

takedowns of terrorist content, including via a hash database,[7] a group of civil society experts led by the Center for Democracy and Technology wrote in a letter:

> *Almost nothing is publicly known about the specific content that platforms block using the Database, or about companies' internal processes or error rates, and there is insufficient clarity around the participating companies' definitions of "terrorist content." Furthermore, there are no reports about how many legal processes or investigations were opened after the content was blocked. This data would be crucial to understand to what extent the measures are effective and necessary in a democratic society, which are some of the sine qua non requisites for restrictions of fundamental rights.*[8]

Others, including the Global Network Initiative, insisted that any institutionalization of terrorist takedown mechanisms include clear definitions and include oversight mechanisms, both on the side of technology companies and on the side of governments requesting takedowns.[9] Brian Fishman, who leads Facebook's counter-terrorism efforts, suggests that despite progress in the technology sector, policymakers and technologists in this arena operate on different wavelengths, with different understandings of the problem. In order to make lasting change, he writes, "policy experts and policymakers need a shared lexicon for understanding the ways that terrorists use the Internet and how that manifests on different types of digital platforms."[10]

Despite these challenges, countering terrorist content online succeeds -- or at the very least, has made progress -- in three areas where counter-disinformation work has not. Across sectors, there is an acknowledgement of the threat; an acknowledgement of the role social media plays in perpetuating it; and an acknowledgement that only through cooperation across sectoral lines can it be addressed.

Broadly, this difference can be explained because terrorist content is a recognizable societal ill, one with a clear enemy and more easily understood diffusion pattern and effect. No western leader will argue that murders perpetrated through acts of terror did

not have a discernible effect, that such attacks ought only to be addressed by a single sector, or that they are a political ploy to cast doubt on the results of a democratic process.

This understanding must come from the top of each sector. Government is the only sector with the convening power and the regulatory mechanisms to work towards a coordinated and harmonized response to problematic online content. In the Trump era, leadership of this kind has been lacking both in the fight against foreign disinformation and against terrorist and extremist content online.

Most recently, this has manifested in the Trump administration's decision not to sign the Christchurch Call. New Zealand's Prime Minister Jacinda Ardern spearheaded the call after the March 2019 mass shootings at mosques in her country, which were "terrorist attacks that were designed to go viral."[11] The document "outlines collective, voluntary commitments from Governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in and after the Christchurch attacks."[12] While some members of civil society expressed worry about the broad definitions of terrorist content outlined in the Call and were dismayed to not be included in the finalization of the text,[13] overall the document enjoys broad support. Tech giants Amazon, Google, Microsoft, Facebook, and Twitter released a joint statement committing to work collaboratively and individually to address the threat.[14]

One endorsement was notably missing, however: the U.S. Government's. The White House cited free speech concerns when explaining the United States' absence from the signatories, despite President Trump's calls for stricter regulation of tech platforms in response to what he viewed as politically-motivated user bans. Especially given that the Call does not include binding standards to which signatories will adhere, how it will function without the endorsement and support of the U.S. government, which has the most influence over U.S.-based technology companies, is unclear.

The fight against online terrorist content has succeeded where the fight against disinformation has so far failed because of the crystallization of the threat across sectors.

But neither can truly succeed without leadership from government. In the absence of a White House that cares to fulfill this role, Congress must, and it must do so without political bias.

The current models for regulation and oversight of social media companies -- via the Federal Trade, Communications, and Elections Commissions -- predate the social media era. It is time for Congress to establish and delegate the oversight of social and digital media to a new, independent government commission of the same ilk.

The commission would harmonize definitions of concepts such as terrorist or extremist content, hate speech, abuse, and disinformation across the Internet and ensure platforms are adhering to those definitions; define and require that platforms obtain informed and meaningful consent to their terms of service, serving as an awareness-building mechanism about data privacy issues and the limits of speech on the platforms; serve as a neutral appellate body for users who feel their content has been unjustly removed; and conduct public audits of algorithms, account takedowns, and data stewardship. Most importantly, however, it would have the convening power to bridge the gap between industry, government, and academia, ensuring that these sectors no longer operate in isolation, or worse, counter to shared goals.

In the absence of the political will necessary to create a whole-of-society response to online disinformation, Congress must empower a professional, non-partisan commission to lead this charge, convene disparate stakeholders, and establish a shared understanding of the threat. More than two years after Russia's online interference campaign began in the United States, more than a decade since it began auditioning these tactics in Eastern Europe, and as more malign disinformation from both other foreign as well as domestic actors proliferates online, it is time to stop attempting to

solve a problem that is a complex tapestry with a patchwork solution. It is likely too late for such a body to be established and make significant progress before the 2020 election, but laying the foundation of this structure will have benefits for generations to come.

References

[1] Walker, Kent. "To stop terror content online, tech companies need to work together," Google, 20 December 2018.

[2] "Partnering to help curb spread of online terrorist content," Facebook, 5 December 2016.

[3] "Partnerships," GIFCT.

[4] "About," GIFCT.

[5] *Ibid*.

[6] Bickert, Monica and Brian Fishman. "Hard Questions: What Are We Doing to Stay Ahead of Terrorists?" Facebook, 8 November 2018.

[7] Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online - general approach," 6 December 2018.

[8] Center for Democracy and Technology, "Civil Society Letter to European Parliament on Terrorism Database," 4 February 2019.

[9] Global Network Initiative, "GNI Statement on Europe's Proposed Regulation on Preventing the Dissemination of Terrorist Content Online," 15 January 2019.

[10] Fishman, Brian. "Crossroads: Counter-terrorism and the Internet," *Texas National Security Review*, Vol. 2, Iss. 2, April 2019.

[11] "The Christchurch Call," https://www.christchurchcall.com/call.html

[12] *Ibid*.

[13] "Community Input on Christchurch Call (13 May) Copy.Pdf," Google Docs, accessed June 21, 2019, https://drive.google.com/file/u/1/d/1RfXLUnx662mmOJv3Z2c0NXEpsAXS8HGN/view?usp=embed_facebook.

[14] The Globe and Mail (The Globe and Mail), "Christchurch Joint Statement and Commitment," accessed June 21, 2019, https://www.documentcloud.org/documents/6004469-Christchurch-Joint-Statement-and-Commitment.html.