Foreign Policy at BROOKINGS

DISINFORMATION AS A WICKED PROBLEM: WHY WE NEED CO-REGULATORY FRAMEWORKS

MOLLY MONTGOMERY

AUGUST 2020

EXECUTIVE SUMMARY

As the harmful effects of disinformation and other online problems on individuals and societies become increasingly apparent, governments are under pressure to act. Initial attempts at self-regulation via mechanisms such as voluntary codes of conduct have not yielded the desired results, leading policymakers to turn increasingly to top-down regulation. This approach is destined to fail.

Disinformation and other online problems are not conventional problems that can be solved individually with traditional regulation. Instead, they are a web of interrelated "wicked" problems — problems that are highly complex, interdependent, and unstable — and can only be mitigated, managed, or minimized, not solved.

Recognizing this wicked web of disinformation and related online problems requires a new mindset, which leads to a different solution set. The most effective strategy to manage wicked problems is co-regulation, a multi-stakeholder approach that requires governments and platforms to increase collaboration among themselves, with each other, and with civil society in a joint effort to balance the benefits of a free and open internet with the need to protect citizens and democratic institutions.

To effectively manage disinformation and related online problems, governments and platforms will need to develop an architecture to promote collaboration and build trust among stakeholders. There are several models for multi-stakeholder collaboration, among them the industry-led Global Internet Forum to Counter Terrorism (GIFCT) and the government-led Information Sharing and Analysis Centers (ISACs). Those that prove successful have in common continuous adaptation and innovation and a focus on trust-building and information-sharing.

This paper recommends the creation of government fusion cells for online problems, which would centralize expertise and decisionmaking and serve as a single point of contact for industry, civil society, and other governments. In parallel, it recommends that platforms expand the mandate of the GIFCT to include a broad range of online problems and to facilitate knowledge- and information-sharing, identify and stress-test potential policy interventions, and develop industry standards and best practices. Together these institutions would create an ecosystem that facilitates the collaboration among multiple stakeholder groups that will be necessary to develop a successful whole-of-society approach to managing online problems.

INTRODUCTION

As our lives have increasingly migrated online, so too have society's ills. The online world not only reflects but magnifies threats to the security of individuals and democratic institutions. The consequences are grave, and liable to become worse as an ever-larger share of the global population comes online. This is particularly the case for the related issues of misinformation and disinformation,[1] each of which pose longstanding threats to the health of democratic institutions.

As the United States saw in the run-up to the 2016 elections, Russian information operations conducted via social media sowed division and undermined trust in democratic institutions.[2] In Myanmar, hate speech and disinformation disseminated via social media helped to ignite an ethnic cleansing campaign against the country's mostly Muslim Rohingya minority.[3] Most recently, the COVID-19 crisis has led to an online explosion of dangerous public health misinformation worldwide, which Russia and China have cultivated through coordinated disinformation campaigns.[4]

These cases and others have spurred governments and platforms alike to act via mechanisms such as the European Union's Code of Practice on Disinformation. Yet these efforts, which rely on voluntary self-regulation by platforms, have failed to sufficiently address the threats online problems pose to citizens and democratic institutions. As a result, platforms have invested in new tools and more forward-leaning policies to combat online problems, including mis- and disinformation, and governments are increasingly turning to top-down regulation.

This paper argues that neither self-regulation nor a top-down approach will succeed, due to the nature of this web of interrelated "wicked" problems that can only be managed, rather than "solved." This paper argues instead for co-regulation — a collaborative, multi-stakeholder approach that seeks to balance the benefits of a free and open internet with the need to protect citizens and democratic institutions.

Effective co-regulation will require governments and online platforms to enhance cooperation among themselves and with each other. The paper concludes with recommendations for government and industry to build the necessary architecture to facilitate collaboration, co-regulation, and a whole-of-society approach to successfully limit online problems.

ONLINE PROBLEMS AND PLATFORM GOVERNANCE

Over the past few years, social media platforms, particularly Facebook and Twitter, have received inordinate blame for many of society's ills, particularly mis- and disinformation. Given the examples cited above, that view is understandable. The critique is alluring in its simplicity; it allows citizens and policymakers alike to direct their ire and prescriptions toward discrete targets that also happen to be wealthy, non-transparent, and elite, easy fodder for the current populist moment. Unfortunately, the challenges with platform governance are more complicated than that, and the solutions are much less clear.

This paper uses the term "online problems" as a catch-all to describe outgrowths of societal ills that predate the internet but have found fertile ground online, particularly on social media, and often with devastating offline consequences. Examples include not just mis- and disinformation but hate speech, incitement to violence, child sexual abuse, terrorist recruitment, and extremist content, among others.

Policymakers have typically approached each of these issues as a discrete problem to be solved. This is particularly the case for activities that have become highly publicized and politicized, such as disinformation. For example, the EU developed its Code of Practice on Disinformation following revelations of Russian election meddling, as public outrage and a sense of impending "real-world" harm spurred governmental action.

As in the case of disinformation, policy remedies for online problems have typically relied on self-regulation via voluntary codes of conduct with which platforms agree to abide. These policies, while well-intended, have frequently been animated more by a need to "do something" than a clear understanding of the problem itself. Nor do the policies reflect much awareness of how each issue relates to other online problems, much less how — and in fact whether — it can be solved at all.

One challenge is that online problems such as disinformation rarely appear in isolation. As we have seen during the COVID-19 pandemic, misinformation and disinformation are often two sides of the same coin. Similarly, the Myanmar example demonstrates the all-too-frequent connection between disinformation and hate speech or incitement to violence.[5] Disinformation often acts as an accelerant for other online problems, which themselves disguise or provide the fodder for disinformation campaigns.[6] These symbiotic relationships between disinformation and other online problems mean that attempting to solve disinformation in isolation from other online problems is destined to fail.

Rapidly changing technologies and vast information asymmetries between platforms and governments make it difficult for policymakers to develop a nuanced understanding of an online problem such as disinformation and conceptualize sophisticated policy responses.

In addition, rapidly changing technologies and vast information asymmetries between platforms and governments make it difficult for policymakers to develop a nuanced understanding of an online problem such as disinformation and conceptualize sophisticated policy responses. Additional complications stem from the need to safeguard fundamental rights and freedoms democratic governments have committed to uphold online.[7] Even after policies are in place, governments often lack the capacity and resources to effectively coordinate implementation, verify compliance, or carry out monitoring.

Unsurprisingly then, efforts to solve disinformation and other online problems have failed to deliver the intended results, as is borne out by the platforms' own statistics. YouTube removed nearly 32 million videos for violating its community standards in 2019,[8] and in April 2020 alone, Facebook applied warning labels to more than 50 million pieces of content that contained misinformation regarding the COVID-19 pandemic.[9]

Faced with the explosion of harmful material and behavior online, governments have begun to embrace a different approach: top-down regulation. France, Germany, India, and other countries have laws requiring platforms to remove various types of offending content within a certain period — and in some cases report it to authorities — or be held liable. The United States took a similar approach in 2018 legislation to counter online sex trafficking, which chipped away at platforms' liability shield under Section 230 of the Communications Decency Act.[10] Each of these laws has generated significant opposition for failing to adequately balance freedom of expression with the imperative to protect individuals and democratic institutions from the effects of online problems.

These top-down policies have a common logic: since platforms are responsible for the problem and have not done enough to fix it, they must either solve the problem themselves or be punished for their failure to do so. The next section of this paper will explain why this approach is doomed to failure and suggest an alternative definition of the problem that leads to a new set of potential policy prescriptions.

A WEB OF INTERRELATED "WICKED" PROBLEMS

The concept of "wicked" problems — in contrast with "tame" problems that are clearly defined and inherently solvable — was coined in 1973 by University of California, Berkeley urban planners Horst W.J. Rittel and Melvin M. Webber.[11] Wicked problems tend to:

- Be unstable, socially complex, and difficult to clearly define;
- Have multiple interdependencies and multiple causes;
- Have no clear solution and create unforeseen consequences when solutions are attempted;
- Involve behavioral change and action by many different actors within and outside government; and
- Leave a string of failed policy attempts to solve them in their wake.[12]

Online problems not only stem from wicked problems that exist in the offline world, but they add an additional layer of complexity, since technology multiplies the reach of malign actors and is constantly evolving.

Researchers have long recognized that many intractable public policy issues fall into the category of wicked problems, from pandemics to poverty. The online analogues of real-world problems, such as racism and terrorism, also fall into this category. Online problems not only stem from wicked problems that exist in the offline world, but they add an additional layer of complexity, since technology multiplies the reach of malign actors and is constantly evolving. These dynamics can make attempting to grasp an online wicked problem akin to riding an intellectual gyroscope — disorienting and endless.

Making matters worse, each online problem exists within a web of interrelated wicked problems. As discussed earlier, the relationship between online hate speech and mis/disinformation can combine to create a dangerous reaction, such as in Myanmar. Online problems also relate to offline problems; there is a clear connection between online hate speech and racial, ethnic, and religious prejudices, for example.[13] In all cases, the ability to solve one problem rests on the need to solve others, trapping policymakers in a negative feedback loop.

Understanding the problem isn't the only challenge. The rapidity of technological development and social adaptation to new technologies means policy interventions are often obsolete even before they are implemented. Many policy instruments must remain off the table due to the competing need to safeguard fundamental rights and freedoms. And the law of unintended consequences is in full effect, as interventions designed to stamp out online problems often succeed only in creating a cascade effect, relocating the problem to another, harder-to-reach, part of the internet.

SOME WICKED PROBLEMS ARE MORE WICKED THAN OTHERS

Most wicked problems are challenging enough for policymakers. Yet some wicked problems are more wicked than others.

We can place online problems on several spectra — legal versus illegal; socially acceptable versus taboo; highly politicized versus apolitical. These spectra measure the level of societal consensus around a problem as a proxy for political will to find a solution. The greater the level of consensus, the less wicked the problem. By this logic, online problems that are illegal, taboo, and apolitical should be the least wicked, and therefore the easiest to solve.

Child sexual abuse may be the least "wicked" of all online problems. It is illegal, taboo, and few would disagree it is a scourge that should be eradicated. Since the advent of the internet, governments have passed legislation, created task forces, and dedicated significant resources to stop its spread. Yet in 2018, social media platforms removed more than 45 million images of child sexual abuse; more than double the previous year's total.[14] And those are the images that were detected. The total number is likely to be many times that, since greater enforcement efforts have caused images to move increasingly to private file-sharing or messaging services like Dropbox or WhatsApp, where encryption makes detection more difficult. In other words, despite a coordinated and concentrated effort to solve the most tractable — or least wicked — online problem, the issue has gotten worse.

RADICAL RETHINKING

Policymakers have largely failed at "solving" wicked problems because they are not, in fact, solvable. The key to developing effective policy interventions for wicked problems is recognizing that there is no one solution. Instead, wicked problems require a shift in vocabulary and mindset to focus on "managing," "limiting," or "minimizing" the problem.

Developing a successful strategy to manage these wicked problems will also require rethinking responsibility for online problems. As discussed above, many governments have adopted an adversarial stance toward digital platforms, one that blames them for online problems and seeks to ratchet up liability for failing to identify and implement solutions. Yet this is both an incomplete explanation for why online problems exist, and an unproductive policy response.

To be sure, platforms should bear some responsibility for online problems. Until recently, most major platforms seem to have adopted willful ignorance as a strategy. And in the United States at least, they have often hidden behind the First Amendment to justify inaction, although it limits government actions to impede free speech, not actions taken by private businesses.[15] Social media platforms have attracted malign actors because they have been permissive and target-rich environments in which to operate.

For example, the lack of prudent safeguards against radicalization in YouTube engagement algorithms has made users vulnerable to terrorist recruiters.[16] Facebook's decision to allow false content in political advertising has increased its vulnerability to disinformation.[17] Twitter's failure to enforce its own terms of service has enabled hate speech and the potential for incitement to violence.[18] The primacy of engagement in advertising models on multiple platforms encourages poor-quality content that is often rife with polarizing misinformation, or worse.

The 2016 U.S. presidential election and the resulting furor from officials and citizenry alike over the scale and potential effects of Russian disinformation on U.S. democratic institutions provided an important wake-up call for platforms.

However, the 2016 U.S. presidential election and the resulting furor from officials and citizenry alike over the scale and potential effects of Russian disinformation on U.S. democratic institutions provided an important wake-up call for platforms. Since then, we have seen the companies behind the major platforms make changes to their policies and, in some cases, to the platforms themselves, to identify and root out inauthentic and/or malign actors, constrain behaviors associated with online problems, and limit the spread of potentially harmful content.

Over the course of the COVID-19 crisis, this trend has accelerated, as platforms have worked to promote information from credible sources while removing or limiting distribution of misinformation.[19] Crucially, some of these decisions have indicated a willingness to prioritize user trust and safety over

revenue growth, albeit in limited ways.

Twitter has emerged as a leader in this respect. In late 2019, Twitter banned all political advertising on its platform, and in May 2020 it implemented a new scheme to identify and limit misleading information, which led the platform to apply labels to several of President Donald Trump's tweets.[20] Most recently, in August 2020, Twitter instituted a new labeling policy for key government officials and state-backed media.[21]

Other platforms have also taken action. Facebook has eliminated its "pseudoscience" advertising category and banned the sale of a variety of medical equipment and "miracle cures" on the platform.[22] Google has blocked tens of thousands of ads capitalizing on the COVID-19 crisis.[23] Multiple platforms have provided free ad credits to the World Health Organization, Centers for Disease Control, and other health authorities.

Few would argue these efforts are sufficient, given the scale of the problem. However, they illustrate an increasing understanding on the part of companies that making their platforms safer runs in line with, rather than counter to, their business interests. If they fail to reduce the incidence of online problems on their platforms, users will go elsewhere — this was the basis of the popular #deleteFacebook campaign following the revelations of Facebook's data breaches in the Cambridge Analytica scandal and how they contributed to the Trump and Brexit campaigns.[24]

Platforms' efforts also demonstrate once again that online problems are both interrelated and insoluble, particularly by any single actor. Large companies' investments in human and technological solutions to detect and deter online problems may succeed in making those platforms less hospitable to malign actors, behavior, and content. However, there are significant negative externalities. Just as regulatory efforts have run up against fundamental rights and freedoms, so too have platforms' efforts to curb online problems. The more actively platforms filter content, the more likely that legitimate expression is stifled. Stronger measures to remove or reduce the virality of harmful content also result in a cascade effect that pushes online problems to smaller platforms that have less capacity to fight them, or to venues — such as private groups or encrypted messaging services — where detection is more difficult.

THE COLLABORATION IMPERATIVE

It is clear the individual efforts of governments and platforms so far have failed to effectively manage the wicked web of online problems. Worse, neither self-regulation nor the top-down approach advocated by many governments will succeed.

More collaborative approaches are needed instead. As other scholars have noted, wicked problems are most effectively managed through multi-stakeholder collaboration and coordination.[25] The same is true when it comes to platform governance. For instance, as the Australian Public Service Commission concluded,

> "The handling of wicked problems requires holistic rather than linear thinking… A true understanding of the problem generally requires the perspective of multiple organizations and stakeholders, and any package of measures identified as a possible solution usually requires the involvement, commitment and coordination of multiple organizations and stakeholders to be delivered effectively."[26]

A collaborative, multi-stakeholder approach can help to:

- Examine multiple angles to improve problem definition;
- Close knowledge and information gaps among stakeholders;
- Increase capacity and buy-in to manage the problem;
- Facilitate the conduct of relevant research;

- Encourage societal or behavioral change;
- Incentivize flexibility, innovation, and iteration in the policymaking process; and
- Anticipate and mediate against unintended consequences of policy interventions.

In the context of online problems, a collaborative approach would require governments and platforms to forge closer relationships among themselves and with each other, as well as with relevant stakeholders, such as advocates for consumer rights and free expression. To succeed, these relationships would need to foster greater trust and mutual understanding, increase knowledge and information sharing, and enhance stakeholder input into — and ideally participation in — the development and implementation of policy interventions.

To be sure, not all governments will be interested in or suited to a collaborative approach that empowers civil society and requires balancing the dangers posed by online problems with the need to safeguard free expression. Authoritarian regimes that view civil society and free expression as threats are likely to continue to utilize censorship and repression to suppress undesirable behavior online, deepening the divide between democracy and autocracy in the so-called "splinternet." While these governments may propose collaboration, platforms should be wary of their motivations and establish clear standards for governments with which they will collaborate. One such criteria could be membership in the Freedom Online Coalition, a collection of 32 countries that have committed to work with civil society and the private sector to support internet freedom worldwide, including free expression, association, assembly, and privacy online.[27]

CASE STUDIES: THE GLOBAL INTERNET FORUM TO COUNTER TERRORISM AND INFORMATION SHARING AND ANALYSIS CENTERS

The closest analogue to this collaborative approach online is the Global Internet Forum to Counter Terrorism (GIFCT), which was founded in 2017 by Facebook, Microsoft, Twitter, and YouTube. The purpose of the GIFCT is to "prevent terrorists and other extremists from exploiting digital platforms."[28] To accomplish this, the GIFCT partners with government, civil society, and wider industry to facilitate innovation, knowledge and information sharing, research, and multi-stakeholder engagement.

Although the GIFCT has by no means solved the problem of terrorist and extremist activity online, it has at least helped stakeholders better manage it.

Although the GIFCT has by no means solved the problem of terrorist and extremist activity online, it has at least helped stakeholders better manage it. The GIFCT's hash database, which contains the digital fingerprints of individual pieces of terrorist or extremist content, grew to more than 200,000 entries in its first two years. Member platforms draw on this database to identify, and potentially remove, reposted content.[29]

The GIFCT has continued to evolve since its founding. Not only has it added smaller platforms like Pinterest and Dropbox to its ranks, but it was recently incorporated as a stand-alone, independent organization. Led by an executive director that reports to a governing board, and an independent advisory committee comprised of government officials and civil society leaders, the GIFCT now features a multi-stakeholder forum and several working groups in which governments, advocacy groups, industry representatives, and

other stakeholders participate. The GIFCT also partners with the United Nations-sponsored public-private partnership Tech Against Terrorism[30] and sponsors the Global Network on Extremism and Technology, which seeks to improve detection of radicalization and recruitment activity online and curtail the spread of extremist material.[31]

The GIFCT has improved trust and facilitated information sharing among platforms and with governments, particularly the U.S. government counterterrorism fusion cell, the National Counterterrorism Center (NCTC). This underlying trust supports expanding the mission of the GIFCT to include smaller platforms, which benefit the most from the GIFCT because they lack indigenous capacity to fight terrorist/extremist content and are likely to be victims of the larger platforms' success, as bad actors move to smaller platforms due to the cascade effect. The GIFCT is also important not just as a funding source for researchers, but also as a potential source of anonymized data that is unobtainable elsewhere. The GIFCT serves as a proof of concept for the model of collaboration — in this case industry-led — to create gains in capacity and effectiveness in managing online problems.

Information Sharing and Analysis Centers (ISACs) are examples of a government-led model. In the late 1990s, the U.S. government asked critical infrastructure providers to create sector-based organizations to share information about threats and vulnerabilities. These organizations, coined ISACs, provide risk mitigation, incident response, and information-sharing services to members representing sectors such as information technology, election infrastructure, aviation, and energy. They also work closely with advocacy groups, identify best practices, and provide members with tools to mitigate risks and enhance resiliency.[32]

A 2014 U.S. National Highway Traffic Safety Administration report assessed the effectiveness of the ISAC model to consider whether the automotive industry would benefit from having its own ISAC. It concluded that ISACs provide industry with important capabilities and that their success "is best defined by their longevity in service and the continued introduction of new ISACs in other industries."[33] Its conclusion was borne out further by the establishment of an automotive industry ISAC a year later, a trend that has continued as the ISAC model spreads to other industries, including with the establishment of the Space ISAC in 2019.[34]

There are many possible models for enhanced collaboration. Those that succeed are likely to have in common with the GIFCT and ISACs a multi-stakeholder approach, continuous adaptation and innovation, and a focus on trust-building and information-sharing.

RECOMMENDATIONS

Effectively managing the wicked web of online problems will require a shift in both mindset and solution set. The first set of recommendations below focus on general principles to guide policymakers in shifting from a solution-centered approach suited to tame problems to the collaboration- and mitigation-focused approach required to manage wicked problems. The second set of recommendations provide a guide for policymakers and industry players to build the architecture necessary to facilitate successful collaboration and co-regulation.

General principles

- Recognize "wickedness." Acknowledge the insolubility of the problem and transition to a vocabulary of "managing," "mitigating," or "limiting" the problem, rather than "solving" it.
- Abandon the adversarial mindset. Apportioning blame is politically tempting but unproductive from a policymaking perspective, as it alienates those parties that policymakers must win over to succeed.
- Resist the urge to create silos. Rather than considering each online harm as a separate problem, recognize that each harm connects to others within the wicked web and must be considered as part of a wider problem set.

- Create a decisionmaking loop. Facilitate decisionmaking that is intentionally flexible and iterative to accommodate a changing problem and accumulated learning.
- Prioritize building trust. This is the key to closing knowledge gaps, facilitating information sharing, and expanding the scope of collaboration over time.

Specific actions

The U.S. government — and other governments — should create fusion cells similar to the National Counter Terrorism Center (NCTC), which would bring representatives of relevant agencies with the appropriate technological and policy backgrounds under one roof with a mandate to lead a whole-of-government strategy to combat online problems.[35] Although the character would inevitably vary from country to country, such organizations would generally:

- Be empowered to provide high-level policy recommendations to interagency decisionmakers;
- Identify and drive resources toward online problems most likely to cause harm to citizens and/or national security;
- Analyze drivers and patterns of online problems to inform policy development;
- Facilitate law enforcement action where appropriate (such as related to child sexual abuse);
- Provide a one-stop-shop for information-sharing with industry, lawmakers, other government agencies, and, in certain cases, foreign governments.

In addition, the operating board of the GIFCT should eventually expand the organization's mandate to include a broad range of online problems, including mis/disinformation, hate speech, and incitement to violence. With a broader mandate, an expanded (and potentially renamed) GIFCT would:

- Build trust and facilitating information-sharing among platforms and with governments;
- Expand capacity to combat online problems via innovation and identification of best practices;
- Explore linkages among online problems and how they respond to interventions;
- Support interdisciplinary research related to detecting, countering, and deterring online problems, including by creating anonymized data sets for use by researchers;
- Develop professional standards and an accreditation process for investigators and researchers, to facilitate the exchange of data and information with platforms; and
- Facilitate regular engagement with stakeholders, including consumer and free expression advocates.

Once operational, government fusion cells and an expanded GIFCT would provide the institutional foundation for the continuous collaboration required for successful co-regulation. The goal would be to establish a high level of trust among platforms and between platforms and regulators to facilitate knowledge- and information-sharing, identify and stress-test potential policy interventions, and develop industry standards and best practices. Over time, an expanded GIFCT could evolve to become a critical node in a whole-of-society approach to managing online problems.

Some platforms, particularly the largest ones, might resist this expansion of the GIFCT's mandate in favor of independent efforts to manage online problems on their own platforms. However, the cascade effect from larger to smaller platforms and public to private fora means this would only cause problems to proliferate in online spaces where neither platforms nor regulators have the resources or reach to control them. Larger platforms may believe they have the capacity to address problems such as disinformation without industry-level cooperation.

Yet recent revelations, such as the existence of the long-undetected Russian disinformation campaign "Sekondary Infektion"[36] and Chinese disinformation efforts piggybacking on COVID-19 misinformation, give lie to claims that platforms have disinformation under control — or that they can manage it without industrywide collaboration and linkages to counter-misinformation efforts.

Like it or not, to effectively manage online problems — and the related risks to their reputations and the industry itself — platforms will need to pool resources, best practices, and information.

Like it or not, to effectively manage online problems — and the related risks to their reputations and the industry itself — platforms will need to pool resources, best practices, and information. Despite the costs involved, this collaborative approach to dealing with one another and with governments is likely to be the most effective way for platforms to minimize further damage to users and democratic institutions.

CONCLUSION

As the saying goes, the first step to solving a problem is recognizing you have one. In the case of online problems such as disinformation, that first step is perhaps the most difficult. It involves recognizing that each individual online harm, including disinformation, is but one of many interrelated and extremely wicked problems, none of which are solvable.

Policy responses should instead focus on mitigating online problems rather than solving them. In particular, government and industry should work to construct an architecture conducive to collaboration and co-regulation, specifically by creating new fusion cells to tackle online problems and expanding the mandate of the GIFCT. The existence of such an architecture will not, on its own, successfully manage the wicked web of online problems. However, it will help to create an ecosystem that facilitates the trust-building and information-sharing among multiple stakeholder groups that will be necessary to develop a true whole-of-society approach to managing online problems.

REFERENCES

1 For this paper, misinformation is defined as the spread of false information — wittingly or unwittingly — by individuals, while disinformation is the spread of false and/or intentionally misleading information by a government-connected individual or organization.

2 "Report of the Senate Intelligence Committee on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media With Additional Views," (Washington, DC: United States Senate Select Committee on Intelligence, October 8, 2019), 4, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

3 Alexandra Stevenson, "Facebook Admits It Was Used to Incite Violence in Myanmar," *The New York Times*, November 6, 2018, https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

4 Jennifer Rankin, "EU Says China Behind Huge Wave of Covid-19 Disinformation," *The Guardian*, June 10, 2020. https://www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign.

5 Paul Moser, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," *The New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

6 Lisa Reppell and Erica Shein, "Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions," (Arlington, VA: International Foundation for Electoral Systems, April 2019), 4, https://www.ifes.org/publications/disinformation-campaigns-and-hate-speech-exploring-relationship-and-programming.

7 "The Founding Declaration - Freedom Online: Joint Action for Free Expression on the Internet," Freedom Online Coalition, December 2011, https://freedomonlinecoalition.com/underpinning-documents/.

8 "YouTube Community Guidelines Enforcement," Google, https://transparencyreport.google.com/youtube-policy/removals?hl=en.

9 Guy Rosen, "An Update on Our Work to Keep People Informed and Limit Misinformation about COVID-19," Facebook, May 12, 2020, https://about.fb.com/news/2020/04/covid-19-misinfo-update/.

10 Nitasha Tiku, "How A Controversial New Sex-Trafficking Law Will Change the Web," *Wired*, March 22, 2018, https://www.wired.com/story/how-a-controversial-new-sex-trafficking-law-will-change-the-web/.

11 Horst W.J. Rittel and Melvin M. Webber, "Dilemmas in a general theory of planning," *Policy Sciences* 4, no. 2, (June 1973): 155–69, https://www.jstor.org/stable/4531523.

12 "Tackling wicked problems: A public policy perspective," Australian Public Service Commission, June 12, 2018, https://www.apsc.gov.au/tackling-wicked-problems-public-policy-perspective.

13 Rachel Hatzipanagos, "How online hate turns into real-life violence," *The Washington Post*, November 20, 2018, https://www.washingtonpost.com/nation/2018/11/30/how-online-hate-speech-is-fueling-real-life-violence/.

14 Michael H. Keller and Gabriel J.X. Dance, "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" *The New York Times*, September 29, 2019, https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

15 Gilad Edelman, "How Facebook Gets the First Amendment Backward," *Wired*, November 7, 2019, https://www.wired.com/story/facebook-first-amendment-backwards/.

16 Rita Katz, "How Terrorists Slip Beheading Videos Past YouTube's Censors," Vice, May 26, 2017, https://www.vice.com/en_us/article/xyepmw/how-terrorists-slip-beheading-videos-past-youtubes-censors.

17 Tony Romm, Isaac Stanley-Becker, and Craig Timberg, "Facebook won't limit political ad targeting or stop false claims under new ad rules," *The Washington Post*, January 9, 2020, https://www.washingtonpost.com/technology/2020/01/09/facebook-wont-limit-political-ad-targeting-or-stop-pols-lying/.

18 David Brennan, "Twitter Is Giving Trump 'Special Treatment' Despite New Rules for World Leaders, Says Free Speech Expert," *Newsweek*, October 16, 2019, https://www.newsweek.com/twitter-giving-donald-trump-special-treatment-new-rules-world-leaders-free-speech-expert-1465663.

19 Bhaskar Chakravorti, "Social media companies are taking steps to tamp down coronavirus misinformation — but they can do more," The Conversation, March 30, 2020, https://theconversation.com/social-media-companies-are-taking-steps-to-tamp-down-coronavirus-misinformation-but-they-can-do-more-133335.

20 Yoel Roth and Nick Pickles, "Updating our approach to misleading information," Twitter, May 11, 2020, https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html.

21 "New labels for government and state-owned media accounts," Twitter, August 6, 2020, https://blog.twitter.com/en_us/topics/product/2020/new-labels-for-government-and-state-affiliated-media-accounts.html.

22 Kang-Xing Jin, "Keeping People Safe and Informed About the Coronavirus," Facebook, July 16, 2020, https://about.fb.com/news/2020/05/coronavirus/.

23 Sundar Pichai, "Coronavirus: How we're helping," Google, March 6, 2020, https://www.blog.google/inside-google/company-announcements/coronavirus-covid19-response/.

24 Andrew Griffin, "How to Delete Facebook for Good: Step-by-Step Guide to Permanently Removing Your Account After Data Hack," *The Independent*, September 28, 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/features/facebook-delete-how-to-step-by-step-remove-account-permanently-deactivate-data-hack-a8264656.html.

25 Leslie Daigle, Konstantinos Komaitis, and Phil Roberts, "Keys to Successful Collaboration and Solving Wicked Internet Problems," Internet Society, January 25, 2017, https://www.internetsociety.org/resources/doc/2017/keys-to-successful-collaboration-and-solving-wicked-internet-problems/.

26 "Tackling wicked problems," Australian Public Service Commission.

27 "The Freedom Online Coalition," Freedom Online Coalition, https://freedomonlinecoalition.com/.

28 "Global Internet Forum to Counter Terrorism: Evolving An Institution," Global Internet Forum to Counter Terrorism, https://www.gifct.org/about/.

29 "Joint Tech Innovation: Hash Sharing Consortium," Global Internet Forum to Counter Terrorism, https://www.gifct.org/joint-tech-innovation/.

30 “”About Tech Against Terrorism,” Tech Against Terrorism, https://www.techagainstterrorism.org/about/.

31 “The Global Network on Extremism and Technology,” Global Network on Extremism & Technology, https://gnet-research.org/.

32 “About ISACs,” National Council of ISACs, https://www.nationalisacs.org/about-isacs.

33 “Assessment of the Information Sharing and Analysis Center Model,” (Washington, DC: National Highway Traffic Safety Administration, U.S. Department of Transportation, October 2014), 2, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812076-assessinfosharingmodel.pdf.

34 “Member ISACs,” The National Council of ISACs, https://www.nationalisacs.org/member-isacs.

35 This concept is not new. The minority staff of the U.S. Senate Foreign Relations Committee recommended a similar fusion cell focused on disinformation in a January 2018 report. “Putin’s Asymmetric Assault on Democracy in Russia, and Europe: Implications for US National Security,” (Washington, DC: United States Senate Committee on Foreign Relations, January 10, 2018), https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf. Daniel Fried and Alina Polyakova echoed this recommendation in their February 2018 and June 2019 Atlantic Council reports on “democratic defense against disinformation.” Daniel Fried and Alina Polyakova, “Democratic defense against disinformation,” (Washington, DC: Atlantic Council, February 2018), https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/; Daniel Fried and Alina Polyakova, “Democratic defense against disinformation 2.0,” (Washington, DC: Atlantic Council, June 2019), https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/.

36 Bobby Allyn, “Study Exposes Russia Disinformation Campaign That Operated In The Shadows For 6 Years,” NPR, June 16, 2020, https://www.npr.org/2020/06/16/878169027/study-exposes-russia-disinformation-campaign-that-operated-in-the-shadows-for-6-.

ABOUT THE AUTHOR

Molly Montgomery is a nonresident fellow at the Brookings Institution's Center on the United States and Europe and a former U.S. Foreign Service officer.

ACKNOWLEDGEMENTS

Ted Reinert and Caroline Klaff edited this paper, and Rachel Slattery provided layout. This paper was inspired by a series of discussions on disinformation hosted by the Brookings Institution and led by Chris Meserole and Alina Polyakova in 2019 and 2020.