DISINFORMATION ON TRIAL: FIGHTING FOREIGN DISINFORMATION BY EMPOWERING THE VICTIMS

Ari B. Rubin†

Foreign disinformation catapulted into the national spotlight with the 2016 presidential election, but its impact is not confined to the electoral map or season. This Article addresses the threat of foreign disinformation by proposing a new statute: a private right of action, enabling harmed persons to directly sue state or private actors, foreign or domestic, who knowingly or recklessly spread disinformation from abroad. Scholars and policymakers have proposed other, far-flung solutions ranging from greater online security to outright censorship. Each of those ideas stumbles on common challenges and lacks a valuable ingredient: an interested party, directly harmed by the foreign campaign, who benefits from a solution and thus has a motivation to act. This proposal adds to the arsenal and grants benefits found nowhere else: public notice of foreign interference; a tool to restrain domestic accomplices who spread disinformation; and a moral, if not always financial, payoff for victims.

TABLE OF CONTENTS

† Ari B. Rubin is a term law clerk to the Hon. Roy B. "Skip" Dalton, Jr. of the U.S. District Court for the Middle District of Florida. He previously clerked for Chief Judge Matthew J. Fader of the Maryland Court of Special Appeals. Prior to law, the author was a film and TV writer and producer, and he has written opinion pieces for publications including *Politico*, *The Huffington Post*, and *The New York Daily News*. The author would like to thank Professor Erin Carroll. She is both a teacher and a mentor. Georgetown Law, J.D. 2020; Wesleyan University, B.A. 2002.

INTRODUCTION

You open a website. A bright red banner flashes: "Breaking News." This page usually covers political controversies, misdeeds by the politicians destroying America. But this story is headlined, "13-Year Old Girl Brutalized; Illegal Immigrants Abduct and Gang Rape Local Honors Student." Last night, the girl's parents reported her missing. Now, an online video shows an interview with a woman claiming to be the girl's aunt, crying about "immigrant gangsters." The video goes viral. Facebook users share it over a million times. The original site notes that the police are not investigating. Other websites, some seemingly fly-by-night, call for protests. Trustworthy community advocates begin retweeting those calls. Soon, at the behest of faceless online organizers, thousands gather at police headquarters calling for the chief to resign.

But none of it, other than the girl—who in fact had run away to visit a boy—and the protests, is real. Not the abduction, the aunt, and certainly not the attack by immigrants. This episode, these facts, played out beat-by-beat in Germany in 2016,[1] inflaming already rife anti-

[1] *See* Stefan Meister, *The "Lisa Case": Germany as a Target of Russian Disinformation*, NATO REV. (July 25, 2016), https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html [https://perma.cc/Y6D9-DVWY]; Damien McGuinness, *Russia Steps into Berlin "Rape" Storm Claiming German Cover-Up*, BBC NEWS (Jan. 27, 2016), https://www.bbc.com/news/blogs-eu-35413134 [https://perma.cc/5UAS-GJG5] (describing contours of the false reporting).

immigrant tensions and weakening the vulnerable governing party.[2] The so-called "Lisa case" was an early Russian disinformation effort that all began with a fake report on a Russian-owned news channel.[3]

In America, foreign disinformation catapulted into the spotlight with the 2016 presidential election, but its impact is not confined to the electoral map or season.[4] As with Germany's "Lisa case," the real-world harm can extend beyond sore feelings,[5] and the costs can escalate quickly.[6] The similar though distinct threat of domestic disinformation

---

2 *See* Kaan Sahin, *Germany Confronts Russian Hybrid Warfare*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 26, 2017), https://carnegieendowment.org/2017/07/26/germany-confronts-russian-hybrid-warfare-pub-72636 [https://perma.cc/YV6Q-MK2Z] ("The [refugee] crisis has become the main ongoing theme on Germany's political scene and has split society into two roughly equal camps. Russian disinformation operations have highlighted alleged or real misbehavior by refugees or have spread the image of an overburdened government failing to cope with the refugee influx.").

3 *See* Suzanne Spaulding, Devi Nair & Arthur Nelson, *Russia's Attacks on Democratic Justice Systems*, CTR. FOR STRATEGIC & INT'L STUD. (2019), https://www.csis.org/features/russias-attacks-democratic-justice-systems [https://perma.cc/V6E9-Q3XB] (describing the story that was originally "picked up by First Russia TV, and soon 10 other Russian-language Kremlin-sponsored media outlets began reporting on the kidnapping and rape").

4 *See* SENATE SELECT COMM. ON INTEL., RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS, S. REP. NO. 116-xx, at 8 (2019) [hereinafter RUSSIA SENATE REPORT] ("After election day, the Russian government stepped on the gas. Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election.").

5 *See, e.g.*, Isaac Stanley-Becker, *Russian Disinformation Network Is Said to Have Helped Spread Smear of U.S. Ambassador to Ukraine*, WASH. POST (Dec. 17, 2019), https://www.washingtonpost.com/technology/2019/12/17/russian-disinformation-network-said-have-helped-spread-smear-us-ambassador-ukraine [https://perma.cc/2QU4-F2AL] (describing the Russian effort to spread untrue, career-threatening information about Marie Yovanovitch, the U.S. ambassador to Ukraine).

6 An extreme example of disinformation's harm is genocidal purges fueled through propaganda on social media or traditional news sources, as in Rwanda in 1994 and presently against the Rohingya minority in Burma. *See* Sharon Lafraniere, *Court Convicts 3 in 1994 Genocide Across Rwanda*, N.Y. TIMES (Dec. 4, 2003), https://www.nytimes.com/2003/12/04/world/court-convicts-3-in-1994-genocide-across-rwanda.html [https://perma.cc/F5NX-RX6E] (describing the propaganda leading to Rwandan genocide); Paul Mozur, *A Genocide Incited on Facebook, with Posts from Myanmar's Military*, N.Y. TIMES (Oct. 15, 2018), https://nyti.ms/2QToYQA [https://perma.cc/E38J-T4N5] (describing government's use of Facebook to rally anti-Rohingya sentiment). Traditionally, internal majority groups or the regime in power have led such campaigns, but recent reporting captures foreign nations now stepping in and widening those divides. *See generally* SHELBY GROSSMAN, DANIEL BUSH & RENÉE DIRESTA, STAN. INTERNET OBSERVATORY, EVIDENCE OF RUSSIA-LINKED INFLUENCE OPERATIONS IN AFRICA (Oct. 29, 2019), https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf [https://perma.cc/AV8S-JXWV].

dominated the 2020 election cycle,[7] but foreign disinformation remains an ongoing danger.[8] More so, it poses a bold new front in today's Great Power conflict because, unlike traditional interstate espionage in which harm to nongovernmental interests or officials is rare, this threat sees the public—media, private individuals, and civic norms—as its primary target.

Since the 2016 election, scholars and public officials proposed many solutions, ranging from greater online security[9] and news trustworthiness ratings,[10] to outright censorship.[11] The response so far—by government, the technology sector, and civil society—has floundered.[12] While government investigations have uncovered the

---

7 *See* Alistair Somerville & Jonas Heering, *The Disinformation Shift: From Foreign to Domestic*, GEO. J. OF INT'L AFFS. (Nov. 28, 2020), https://gjia.georgetown.edu/2020/11/28/the-disinformation-shift-from-foreign-to-domestic [https://perma.cc/Y5RG-82H2] (describing the 2020 election cycle as "a shift from a narrative of foreign interference to one of domestic disinformation"); *see also* Matthew Rosenberg, Jim Rutenberg & Nick Corasaniti, *The Disinformation Is Coming from Inside the White House*, N.Y. TIMES (Jan. 8, 2021), https://www.nytimes.com/2020/11/05/us/politics/trump-white-house-disinformation.html?smid=url-share [https://perma.cc/J53S-C823] (describing politicians' contribution to disinformation).

8 *See* Dustin Volz & Warren P. Strobel, *Russia, Iran Acted to Influence 2020 Presidential Election, Report Says*, WALL ST. J. (Mar. 17, 2021, 6:29 AM), https://www.wsj.com/articles/putin-authorized-influence-operations-to-hurt-bidens-2020-candidacy-report-says-11615918958 (last visited Sept. 19, 2021) (describing the revelation of attacks by Russia, China, and Iran in "the first official U.S. government finding about foreign interference in the 2020 presidential campaign to be made public").

9 *See* Max Boot & Max Bergmann, *Defending America from Foreign Election Interference*, COUNCIL ON FOREIGN RELS. (Mar. 6, 2019), https://www.cfr.org/report/defending-america-foreign-election-interference [https://perma.cc/BRN4-3FMK].

10 *See* Federico Guerrini, *Fake News: Could a New Online Rating System Help Fight Misinformation?*, FORBES (July 10, 2018, 2:01 PM), https://www.forbes.com/sites/federicoguerrini/2018/07/10/fake-news-could-a-new-online-rating-system-help-fight-misinformation/#5f7347ec66d6 [https://perma.cc/6ZJC-5JWL].

11 Andrew Marantz is a high-profile media commentator who has advocated limiting First Amendment protections. In a recent New York Times op-ed, he wrote, "We can protect unpopular speech from government interference while also admitting that unchecked speech can expose us to real risks. And we can take steps to mitigate those risks." Andrew Marantz, *Free Speech Is Killing Us*, N.Y. TIMES (Oct. 4, 2019), https://nyti.ms/337afaR [https://perma.cc/HY4G-9SJD].

12 *See, e.g.*, Colleen Long, Zeke Miller & Michael Balsamo, *Officials See Extremist Groups, Disinformation in Protests*, AP NEWS (May 31, 2020), https://apnews.com/article/violence-social-media-ny-state-wire-new-york-virus-outbreak-32bc90566697388645f01675359dcad1 [https://perma.cc/J2XM-KGMD] (noting indications of foreign disinformation playing a role at the outset of the 2020 George Floyd domestic protests); Chris Meserole & Alina Polyakova, *Disinformation Wars*, FOREIGN POL'Y (May 25, 2018, 12:10 AM), https://foreignpolicy.com/2018/05/25/disinformation-wars [https://perma.cc/DS93-73YD]; Davey Alba & Adam Satariano, *At Least 70 Countries Have Had Disinformation Campaigns, Study Finds*, N.Y. TIMES (Sept. 26, 2019), https://nyti.ms/2nl9lrv [https://perma.cc/8Q9T-DBGE]; John S. Ehrett, *Confronting*

breadth of previous attacks, institutions have not secured their IT systems against foreign intrusion,[13] tech companies have zigzagged in a much-derided series of changes,[14] and some entities have taken drastic and potentially unconstitutional steps.[15] These efforts expose the enormous difficulties in responding—from First Amendment protections to entrenched, opposed interests—and leave the playing field open for better solutions.

This Article enters that breach and advances a supplementary approach, one that avoids many of the fault lines and, more significantly, adds a valuable ingredient that the others lack: an interested party directly harmed by the foreign interference who materially benefits from a solution and has a motivation to act. This Article proposes a statutory private right of action enabling harmed persons to directly sue state or private, and foreign or domestic, actors who knowingly or recklessly spread foreign disinformation. Fueling real-world protests with false accounts of a little girl's rape, as in the Lisa case, violated her privacy, turned her attempt to hide a secret pre-teen romance into a national story, and left her reputation in tatters.[16] As that event showed, the impact from these attacks can impose clear and lasting material costs, on top of the diffuse, harder-to-define harms to civic trust. This Article argues for a solution that takes on this broad danger by empowering individuals who suffer directly.

Disinformation Warfare, YALE J.L. & TECH. (Apr. 18, 2017), https://yjolt.org/blog/confronting-disinformation-warfare [https://perma.cc/SV4T-ESUG].

13 *See* Ben Popken, *Election Security Experts Say Hack of Voters' Confidence May Be Biggest Threat to 2020*, NBC NEWS (Sept. 21, 2019, 2:55 AM), https://www.nbcnews.com/politics/elections/election-security-experts-say-hack-voters-confidence-may-be-biggest-n1057246 [https://perma.cc/HBW2-MXVQ] ("[S]ecurity experts warned of very real ongoing threats to the election process in the U.S. and other global democracies. Threats include social media disinformation, cyber espionage against key participants, hack and leak operations, and attacks on critical infrastructure to tamper with or alter votes . . . . While the firm has seen limited indication of successful attempts on election systems themselves, it has observed numerous instances where actors have targeted related organizations and entities, including election commissions and state boards of elections . . . ." (internal quotations omitted)).

14 Sheera Frenkel, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg & Jack Nicas, *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), https://nyti.ms/2DlsGPi [https://perma.cc/G8L9-CMRJ]; Julian King & Mariya Gabriel, *Facebook and Twitter Told Us They Would Tackle "Fake News." They Failed*, GUARDIAN (Feb. 28, 2019, 8:57 PM), https://www.theguardian.com/commentisfree/2019/feb/28/facebook-twitter-fake-news-eu-elections [https://perma.cc/5TTG-5PLR].

15 California Governor Gavin Newsom signed a law that would criminalize altered videos, known as deepfakes, in the leadup to elections. *See* Will Fischer, *California's Governor Signed New Deepfake Laws for Politics and Porn, but Experts Say They Threaten Free Speech*, BUS. INSIDER (Oct. 10, 2019, 12:51 PM), https://www.businessinsider.com/california-deepfake-laws-politics-porn-free-speech-privacy-experts-2019-10 [https://perma.cc/DHF5-94DA].

16 *See* Jim Rutenberg, *RT, Sputnik and Russia's New Theory of War*, N.Y. TIMES (Sept. 13, 2017), https://nyti.ms/2eUIdrU [https://perma.cc/U3UB-896Q].

A private right of action will not end disinformation. Civil litigation's demands and inefficiencies will limit its use. Challenges include proving harm and collecting awards. But this approach grants benefits found nowhere else: public notice of foreign interference, especially important when government leaders fail to act or actively deny it; a tool to restrain domestic accomplices who spread disinformation; and a moral, if not financial, resolution for victims. The private right of action adds crucial elements in the broader response.

This Article proceeds in four Parts. Part I defines the problem, revealing what is meant by disinformation and distinguishing it from other forms of controversial rhetoric. Part I also illustrates disinformation's historical use, shows how it has evolved, and establishes why we must tackle the threat. Part II then describes how policymakers are addressing it. It highlights the most intriguing proposals and illustrates the challenges they face. With that foundation laid, Part III presents this Article's solution. It carefully describes each element of the new right of action and lays out the statute's goals and limits. Finally, Part IV hardens support for the proposal by showing how its elements are constructed to overcome the obstacles. Here, the Article recruits an analogous suite of laws in a related context: antiterrorism. By building off those laws' evolution and judicial application, the proposed disinformation statute can avoid many of the traps the antiterrorism laws suffered.

Disinformation is a complex knot, coopting and harming core democratic interests. Addressing its challenges will be hard enough that it is tempting to instead resign oneself to the costs. This Article argues that no all-encompassing response will work, and instead, leaders must fight on multiple fronts. The proposed private right of action can be a key tool in that campaign.

I. THE THREAT

Parts I and II of this Article lay out the disinformation playing field, allowing the remaining Parts to argue the statute's purpose, application, and effectiveness. Section I.A defines what we mean by disinformation and distinguishes it from other types of controversial speech. Section I.B then shows that disinformation is an age-old problem, but today, several factors turn what had been a chronic concern into a clear and present danger.

A. *What We Mean by "Disinformation"*

Before confronting the challenge of distinguishing disinformation from real news comes the important step of defining disinformation. It is popular in the current political era to bandy about the phrase "fake news."[17] Even seasoned media analysts and academics use it.[18] But it is far more helpful to divide harmful information into three types: misinformation, mal-information, and disinformation.[19]

Misinformation, in this typology, "is information that is false, but the person who is disseminating it believes that it is true."[20] Without yet weighing the issue of mens rea—whether an actor knows her words are untrue—an example of misinformation is a reporter whose claims in response to breaking news later turn out to be wrong. An example of widespread misinformation occurred in 1995 after the Murrah Federal Office Building attack in Oklahoma City, when numerous otherwise reliable news sources initially blamed Middle Eastern terrorists, when in fact the plot was domestic.[21] Key to the definition is that the speakers' errors were not intentionally malicious.

A second category is mal-information. Mal-information is a statement that is primarily *true* but the issuer spreads it in order to cause harm.[22] This can also be a more localized form of harmful information, one meant to be heard by only a few people. An example is a speaker revealing damaging facts about a competitor in order to tarnish the

---

17 *See* Craig Silverman, *I Helped Popularize the Term "Fake News" and Now I Cringe Every Time I Hear It*, BUZZFEED NEWS (Dec. 31, 2017, 5:21 PM), https://www.buzzfeednews.com/article/craigsilverman/i-helped-popularize-the-term-fake-news-and-now-i-cringe [https://perma.cc/3E85-DNUD] (claiming to have helped coin the term).

18 *See* Ari Ezra Waldman, *The Marketplace of Fake News*, 20 U. PA. J. CONST. L. 845, 849 n.17 (2018) (describing the difficulties in and varying attempts at defining the term "fake news").

19 *See* Claire Wardle & Hossein Derakhshan, *Thinking about "Information Disorder": Formats of Misinformation, Disinformation, and Mal-Information*, *in* JOURNALISM, "FAKE NEWS" & DISINFORMATION 44 (Cherilyn Ireton & Julie Posetti eds., UNESCO 2018), https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0_0.pdf [https://perma.cc/Y6RM-N2DG].

20 *See id.*

21 Jim Naureckas, *The Oklahoma City Bombing: The Jihad that Wasn't*, FAIR (July 1, 1995), https://fair.org/extra/the-oklahoma-city-bombing [https://perma.cc/PJP3-H8S2] ("'Knowing that the car bomb indicates Middle Eastern terrorists at work, it's safe to assume that their goal is to promote free-floating fear and a measure of anarchy, thereby disrupting American life,' the New York Post editorialized."); *see also* Mitch Smith, *Richard Jewell Was Wrongly Implicated in a Mass Attack. He's Not the Only One.*, N.Y. TIMES (Dec. 29, 2019), https://www.nytimes.com/2019/12/29/us/mass-shootings-communications.html?smid=nytcore-ios-share [https://perma.cc/FPT2-LKRQ] (listing examples of misinformation in the media related to authorities' erroneous investigatory leads).

22 *See* Wardle & Derakhshan, *supra* note 19, at 44.

target's reputation or material well-being, such as leaks about criminal conduct or the target's closeted lifestyle.[23] Mal-information, described simply, is the release of factual information to commit a harm.

The third category is disinformation. These are statements that are either partially or entirely false and known to be false by the person who is disseminating them; thus, she is maliciously lying in order to cause harm.[24] Here, the harm and falsity factors combine. This is the category that encompasses foreign influence campaigns.

One must recognize that a given piece of information can move between categories depending on the user's intent, and the same statement might require a different response as it appears in different forms. An example of a statement that could be defined all three ways, depending on who says it and when, arose from the story of NFL player Colin Kaepernick kneeling during the national anthem.[25] Based on that fact, a provocative Russian tweet on March 13, 2018, from an account named @wokeluisa spoke in support of Kaepernick, while another Russian right-wing account, @BarbaraForTrump, was simultaneously tweeting content hostile to NFL players' protests, both aimed at their respective ideological camps.[26] The pro-Kaepernick tweet prompted 37,000 presumably unwitting retweets.[27] It began in traditional media as mal-information: actual facts in popular discussion that other parties used to tarnish the player's reputation. The Russian tweeters then took those facts and made them into disinformation, twisting the truth with the goal of spreading civic discord. Then, at least some of the people who retweeted those messages, oblivious to the source, spread what would properly be called misinformation (information the actor does not know is false).

This Article focuses on disinformation, and in fact, a narrower subset thereof: disinformation arising from a foreign source. To state it bluntly, foreign disinformation is speech used as a strategic weapon. The foreign source is uniquely worrying because that other nation's pursuit of a strategic end, while hiding its role, is effectively active espionage. Even if international law does not specifically forbid

---

23 *See id.*

24 *See id.*

25 *See generally* Juliet Macur, *Colin Kaepernick's Anthem Protest Leaves the N.F.L. Necessarily Uneasy*, N.Y. TIMES (Sept. 7, 2016), https://nyti.ms/2clIFzZ [https://perma.cc/HW2G-7UW7].

26 *See* RUSSIA SENATE REPORT, *supra* note 4, at 53–54.

27 *See id.* At the same time, to complete the effect, Russian agents issued contradictory messages from right-leaning Twitter accounts, which also spread. *See id.*

disinformation, like unpredicted acts of war,[28] such efforts transgress international norms and should evoke moral abhorrence.[29] Narrowing the focus to foreign disinformation is not intended to discount domestic actors.[30] Indeed, this Article's proposed statute would impose liability on domestic actors for spreading foreign disinformation. A domestic actor who furthers the foreign state's aims by recklessly amplifying its message is facilitating the attack and shares culpability.[31] Weaponized speech to achieve strategic goals turns America's core liberties against it.

With these distinctions, a full definition of foreign disinformation requires four prongs:

(1) the content's foreign source;

(2) the content's factual mistruth;

(3) the originator's malicious intent and strategic aim to undermine civic well-being; and

(4) the content's release into the public sphere causes harm.[32]

A final consideration in accurately identifying disinformation is recognizing that under this definition, its manifestations can look very different depending on two variables: the actor (the entity, proximately speaking) and the target (the ultimate audience). The many combinations of actor and target each prompt different considerations in order to combat disinformation. In justifying the proposed statute

---

28 *See* Ashley C. Nicolas, *Taming the Trolls: The Need for an International Legal Framework to Regulate State Use of Disinformation on Social Media*, 107 GEO. L.J. ONLINE 36, 47–51 (2018) (describing the absence of controlling international law and arguing that "actions short of a use of force may be considered a violation of the principle of non-intervention even if the U.N. Charter does not prohibit the act").

29 *See* The U.N. Special Rapporteur on Freedom of Opinion & Expression, OCSE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression & the ACHPR Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and "Fake News," Disinformation and Propaganda* (Mar. 3, 2017), https://www.osce.org/files/f/documents/6/8/302796.pdf [https://perma.cc/Z3QU-LZWG] (deriding the rise of disinformation and stating principles to guide acceptable countermeasures).

30 In a worrying trend, domestic actors trying to manipulate real-world events are now adopting many of the same techniques that foreign actors have deployed. *See, e.g.*, Matthew Rosenberg & Nick Corasaniti, *Close Election in Kentucky Was Ripe for Twitter, and an Omen for 2020*, N.Y. TIMES (Nov. 10, 2019), https://www.nytimes.com/2019/11/10/us/politics/kentucky-election-disinformation-twitter.html [https://perma.cc/QAX3-URD9] (describing recent domestic disinformation attacks in a narrow Kentucky gubernatorial election).

31 Such participation by domestic actors arguably constitutes an act of treason or other related offense, which are criminalized under 18 U.S.C. §§ 2381, 2384, and similar provisions.

32 *See* Oreste Pollicino & Elettra Bietti, *Truth and Deception Across the Atlantic: A Roadmap of Disinformation in the US and Europe*, 11 ITALIAN J. PUB. L. 43, 49 (2019).

and explaining why other solutions stumble, this Article will refer to different pairings between these two categories:

> Actors: (1) state agents; (2) state subsidiaries; (3) knowing domestic amplifiers; and (4) unwitting accomplices.
>
> Targets: (1) government leaders; (2) media companies and online influencers; (3) corporations; and (4) the public.[33]

With the boundaries drawn, the next Section will discuss actual occurrences and harm from foreign disinformation and show why today's threat is worse.

B. *The Harm: Its Evolution and Material Effect*

Consider how states have used disinformation before. It has deep historical roots,[34] and its face is everchanging. Its impact is often nominal or abstract, but sometimes its consequences can be striking. Looking at disinformation in practice not only shows why a response is more important now, but it shows how tangibly words can hurt.

States have used disinformation as a weapon since the beginning of armed conflict.[35] The disinformation definition here encompasses foreign espionage campaigns stretching back to ancient Rome—used often in combination with other spy craft to mislead enemies as to Roman troop movements.[36] More advanced techniques appeared in the Great Powers era. In early 1918, during WWI, the Allied nations flagged against their entrenched German enemy.[37] The Russians, opposed to the

---

33 *See* ELIZABETH BODINE-BARON, TODD C. HELMUS, ANDREW RADIN & ELINA TREYGER, RAND CORP., COUNTERING RUSSIAN SOCIAL MEDIA INFLUENCE 7–11 (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf [https://perma.cc/Q2T3-24WZ] (establishing these categories for analysis).

34 *See generally* Richard Stengel, Stemming the Tide of Global Disinformation, Meeting at the Council on Foreign Relations (Oct. 11, 2019) [hereinafter Stengel, Stemming the Tide], https://www.cfr.org/event/stemming-tide-global-disinformation [https://perma.cc/CY4C-YKD3] ("The way they used to do it in the '50s was they bought out a journalist in a remote newspaper in India to put out a false story about something and then the Russian media would start echoing it and then it would get into the mainstream. Now, they hire a bunch of kids to work in a troll farm in St. Petersburg and put it up on social media with no barrier to entry, no gatekeepers to prevent it from happening.").

35 *See* ROSE MARY SHELDON, INTELLIGENCE ACTIVITIES IN ANCIENT ROME: TRUST IN THE GODS, BUT VERIFY 81–82 (2005).

36 *See id*.

37 John Maxwell Hamilton & Meghan Menard McCune, *Lessons from White House Disinformation a Century Ago: "It's Dangerous to Believe Your Own Propaganda*," CONVERSATION (Sept. 13, 2018, 6:47 AM), https://theconversation.com/lessons-from-white-house-disinformation-a-century-ago-its-dangerous-to-believe-your-own-propaganda-102155 [https://perma.cc/4RWF-JELH].

Germans, broke into civil war, pitting the Allied-aligned provisional government against the unaligned Bolsheviks. The western Allies had not yet taken a side in the Russian conflict. To help survive their civil war, the provisional government hatched a plot. In cahoots with an American journalist, Edgar Sisson, they leaked a story, which U.S. newspapers eagerly repeated, that the Bolsheviks were secretly negotiating an alliance with Germany, causing the American public to turn against the Bolsheviks overnight.[38] Years later, researchers revealed that all of the documents on which Sisson relied were false.[39] From its earliest days, Russian operatives successfully manipulated the American public.[40] Russia continued to use disinformation as a strategic weapon throughout the Cold War.[41]

America is no less complicit, and in terms of addressing today's problem, it is essential to recognize its disinformation history and motives. The same instance described above of Russian disinformation in WWI in fact began when Sisson, the reporter, traveled to Russia at the behest of America's de facto propaganda ministry, the Committee on Public Information.[42] While the agency's mandate was mainly to drum up domestic support for involvement in the war, its Foreign Section was responsible for spreading both overt and unofficial pro-American messages around the world.[43] American disinformation took on a far more aggressive and duplicitous form as well. From 1963 to 1973, the CIA led a disinformation campaign in Chile that ultimately swung popular sentiment against the left-leaning government and led to Augusto Pinochet's rise to power.[44] In Nicaragua in the 1980s, CIA operatives planted enough false stories against the Sandinista regime

---

38 *See id*.

39 *See id*.

40 *See id.*

41 *See, e.g.*, CHRISTINA NEMR & WILLIAM GANGWARE, PARK ADVISORS, WEAPONS OF MASS DISTRACTION: FOREIGN STATE-SPONSORED DISINFORMATION IN THE DIGITAL AGE 14–15 (2019), https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf [https://perma.cc/Y6U4-GKJC] ("During the late 1980s, for example, the Soviet Union coordinated a global disinformation campaign to convince the world's public that the United States had created the AIDS virus as a biological weapon.").

42 *See* Christopher B. Daly, *How Woodrow Wilson's Propaganda Machine Changed American Journalism*, SMITHSONIAN (Apr. 28, 2017), https://www.smithsonianmag.com/history/how-woodrow-wilsons-propaganda-machine-changed-american-journalism-180963082/#032GcZ0zmcfUoclv.99 [https://perma.cc/47KU-WDQK]; Hamilton & McCune, *supra* note 37.

43 *See* Cedric Larson & James R. Mock, *The Lost Files of the Creel Committee of 1917–19*, 3 PUB. OP. Q. 1, 16–17 (1939).

44 *See generally* STAFF OF SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTEL. ACTIVITIES, 94TH CONG., COVERT ACTION IN CHILE 1963–1973 (Comm. Print 1975).

that papers ran seventy to eighty of them a day, ultimately undermining the Sandinistas as well.[45] One count of American-led disinformation efforts in elections abroad cited eighty-one occurrences between 1946 and 2000.[46] America has long used disinformation to real-world effect, and even though its methods and goals have evolved into a less malicious form,[47] American leaders have a vested interest in keeping it in the arsenal.[48] Thus, in combatting disinformation, policymakers must consider the blowback against American interests.

Today, the threat from foreign disinformation has transformed, grown rife, and is harming Americans more than ever. The stability of U.S. elections is not the only concern, but it is an overriding one. Disinformation burst into the public's attention in 2016, when authorities began uncovering a far-reaching plot by Russia's Internet Research Agency (IRA) to divide society and potentially alter the election.[49] Regardless of whether Donald Trump's narrow electoral college win was attributable to Russian efforts,[50] the breadth of those efforts was clear. The agency developed a network of imposter media accounts publishing inflammatory messages to the American electorate on topics including race, immigration, and public safety.[51] A later Senate Intelligence Committee investigation revealed that the 2016 effort was disproportionately focused on stoking dissent and repressing voter turnout among African Americans.[52] Foreign hackers have

---

45 *See* Scott Shane, *Russia Isn't the Only One Meddling in Elections. We Do It, Too.*, N.Y. TIMES (Feb. 17, 2018), https://nyti.ms/2BycLfI [https://perma.cc/W8QB-ETK7].

46 *See* Dov H. Levin, *Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset*, 36 CONFLICT MGMT. & PEACE SCI. 88, 94 (2016).

47 *See* Joshua Geltzer & Jake Sullivan, *How to Prevent the Next Election Disaster*, POLITICO (Jan. 22, 2019), https://www.politico.com/magazine/story/2019/01/22/prevent-election-disaster-224032 [https://perma.cc/W995-Y8PG].

48 *See* ALVIN A. SNYDER, WARRIORS OF DISINFORMATION: AMERICAN PROPAGANDA, SOVIET LIES, AND THE WINNING OF THE COLD WAR 97–99 (1995) (offering examples of U.S. intelligence agencies' previous disinformation attacks).

49 *See* Indictment at ¶¶ 1–2, United States v. Internet Rsch. Agency LLC, No. 18-cr-00032-DLF, 2018 WL 914777 (D.D.C. Feb. 16, 2018) (noting that the Russian disinformation efforts affecting the 2016 election actively commenced in 2014).

50 *See* KATHLEEN HALL JAMIESON, CYBERWAR; HOW RUSSIAN HACKERS AND TROLLS HELPED ELECT A PRESIDENT 11 (2018).

51 *See id.* at 11.

52 *See* RUSSIA SENATE REPORT, *supra* note 4, at 6 ("The Committee found that no single group of Americans was targeted by IRA information operatives more than African-Americans. By far, race and related issues were the preferred target of the information warfare campaign designed to divide the country in 2016."). "Some of the videos [Russian operatives posted to YouTube] featured expressly voter suppressive content intended to dissuade African-American voters from participating in the 2016 presidential election, while others encouraged African-Americans to vote for Jill Stein." *Id.* at 59.

hijacked established publications across the media spectrum.[53] News analyses revealed that readers began to repeat and amplify those messages.[54] The impact extended beyond online invective and riled emotions; it spilled physically out onto the streets.

In one well-reported incident, the IRA used two fake online groups—one anti- and the other pro-Islamist—to promote a nonexistent rally in Houston.[55] Unwitting supporters and opponents spread the news, and dozens of riled protestors appeared at the designated time, effectively on Russia's marching orders.[56] On another occasion, Trump supporters in Florida featured two Russian-troll-backed events on their election websites.[57] Facebook identified at least 130 events promoted on its platform tied to IRA activity.[58] Robert Mueller's investigators uncovered one incredible example in which IRA operatives, working entirely online, hired individuals in the United States to build a cage on a flatbed truck and a costumed actress to portray Hillary Clinton in a prison outfit while the truck drove through a Florida rally.[59]

The threat is not limited to elections, nor does it exist on only digital platforms. The IRA's effort to stoke dissent continued after the election and by many accounts grew.[60] *The Washington Post* reported

---

53 "The most successful Russian operations blend covert hacking and dissemination operations, social media operations, and fake personas with more overt influence platforms like state-funded online media, including RT and Sputnik." *Id.* at 16. RT operates a television network and Sputnik lives on the Internet, TV, and radio. *See* Elizabeth Flock, *After a Week of Russian Propaganda, I Was Questioning Everything*, PBS (May 2, 2018, 4:25 PM), https://www.pbs.org/newshour/arts/after-a-week-of-russian-propaganda-i-was-questioning-everything [https://perma.cc/2ZKS-5T9Y].

54 *See* Gillian Cleary, *Twitterbots: Anatomy of a Propaganda Campaign*, BROADCOM (June 5, 2019), https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation [https://perma.cc/P29C-9RA9].

55 *See* Mike Glenn, *A Houston Protest, Organized by Russian Trolls*, HOUS. CHRON. (Feb. 20, 2018, 11:46 AM), https://www.houstonchronicle.com/local/gray-matters/article/A-Houston-protest-organized-by-Russian-trolls-12625481.php [https://perma.cc/9VQ6-TH8Y].

56 *See id.*

57 *See* JAMIESON, *supra* note 50.

58 *See* RUSSIA SENATE REPORT, *supra* note 4, at 46.

59 *See* Indictment at ¶¶ 55, 77, United States v. Internet Rsch. Agency, No. 18-cr-00032, 2018 WL 914777 (D.D.C. Feb. 16, 2018).

60 *See* RUSSIA SENATE REPORT, *supra* note 4, at 8 ("Accounts operated by the IRA troll farm became more active after the election, confirming again that the assault on our democratic process is much bigger than the attack on a single election." (citing August 2018 testimony by John Kelly)); Alex Finley, John Sipher & Asha Rangappa, *Why the 2020 Election Will Be a Mess: It's Just Too Easy for Putin*, JUST SEC. (Feb. 19, 2020), https://www.justsecurity.org/68728/why-the-2020-election-will-be-a-mess-its-just-too-easy-for-putin [https://perma.cc/QL5C-QBFD] (describing the 2020 election threat expectation of "a barrage of disinformation, from fake think tanks, fake media outlets, false social media accounts, false identities, trolls, and bots to launder fringe narratives into the mainstream and hijack the public discourse").

in September 2019 that a North Macedonian troll farm took over multiple accounts and spread right-wing messages unassociated with any election—mostly with the account owner's awareness and an absence of intervention by the social media platforms.[61] Disinformation can affect national policy and transnational business interests.[62] Chinese nationals have actively penetrated U.S. communities to rewrite the narrative on their nation's conduct.[63] Online publication *The Intercept* revealed a series of paid advertisements that Twitter allowed on its platform from June through August 2019 that mischaracterized and positively reframed China's treatment of its Uighur population in Xinjiang.[64] The ad campaign, it turned out, was from the *Global Times*, a Chinese state-owned media organization.[65] More overtly—with albeit faint reference to the fact that it was a paid advertisement—the *Des Moines Register* ran a four-page spread of articles in September 2018 that touted free trade's benefits for U.S. farmers, the risks of China-U.S. trade tensions, and President Xi's long ties to Iowa.[66] Other adversarial states—Iran and North Korea—have launched similar disinformation attacks against regional enemies and the United States.[67] And demonstrating their tactic of piggybacking on breaking news, in just the first three days of the George Floyd police-killing protests in late May 2020, Chinese ambassadors, Russian-sponsored news outlets, and other

---

61 Craig Timberg, *The Facebook Page "Vets for Trump" Was Hijacked by a North Macedonian Businessman. It Took Months for the Owners to Get It Back*, WASH. POST (Sept. 17, 2019), https://www.washingtonpost.com/technology/2019/09/17/popular-facebook-page-vets-trump-seemed-be-place-former-military-months-macedonians-controlled-it [https://perma.cc/G3MK-KLWT].

62 *See, e.g.*, Michael Schwirtz & Gaelle Borgia, *How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader*, N.Y. TIMES (Nov. 11, 2019), https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html [https://perma.cc/VY73-HWW4] (describing shifting priorities by Russian actors) ("[W]hile Russia's efforts in the United States fit Moscow's campaign to upend Western democracy and rattle Mr. Putin's geopolitical rivals, the undertaking in Madagascar often seemed to have a much simpler objective: profit.").

63 *See* Ryan Gallagher, *Twitter Helped Chinese Government Promote Disinformation on Repression of Uyghurs*, INTERCEPT (Aug. 19, 2019, 3:28 PM), https://theintercept.com/2019/08/19/twitter-ads-china-uighurs [https://perma.cc/83HB-QBND].

64 *See id.*

65 *See id.*; *see also* Casey Newton, *China Is the Latest Superpower to Get Caught Waging a Disinformation Campaign on Twitter*, VERGE (Aug. 20, 2019, 6:00 AM), https://www.theverge.com/interface/2019/8/20/20813046/china-disinformation-campaign-hong-kong-twitter-facebook [https://perma.cc/PX3V-8XP9] (reporting on similar but more advanced efforts by China in Hong Kong).

66 *See* Donnelle Eller, *Chinese-Backed Newspaper Insert Tries to Undermine Iowa Farm Support for Trump, Trade War*, DES MOINES REG. (Sept. 24, 2018, 2:58 PM), https://www.desmoinesregister.com/story/money/agriculture/2018/09/24/china-daily-watch-advertisement-tries-sway-iowa-farm-support-trump-trade-war-tariffs/1412954002 [https://perma.cc/VT7Z-UBM2].

67 *See* NEMR & GANGWARE, *supra* note 41, at 23–25.

foreign-controlled accounts tweeted provocative antigovernment messages more than 1,200 times.[68] When the Covid-19 pandemic erupted, Russian operatives launched a disinformation barrage, aiming to undercut the World Health Organization and spread messages about American and European mismanagement, all while praising the performance of China and Iran.[69] In a dynamic turn, China then symbiotically amplified Russian efforts; Chinese diplomats aggressively reposted Russian disinformation on their Twitter accounts, and Chinese news agencies spread it further.[70]

Recently, weaponized disinformation has moved beyond the sole control of state actors or cybercriminals. Unlike the fly-by-night North Macedonian troll farm that peddled general right-wing propaganda during the 2020 election, a global wave of public relations firms has begun to offer professionalized disinformation for hire.[71] These firms take disinformation techniques that once only intelligence agencies could deploy and offer them to a variety of governmental and private clients, coating those services with a gloss of professionalism—even sinister respectability.[72] The menu of services caters to nearly any

---

68 *See* Mark Scott, *Russia and China Target US Protests on Social Media*, POLITICO (June 1, 2020, 4:26 PM), https://www.politico.eu/article/russia-china-us-protests-social-media-twitter [https://perma.cc/F3ZZ-Q3QJ].

69 *See* Lea Gabrielle, Special Envoy & Coordinator, Glob. Engagement Ctr., Briefing on Disinformation and Propaganda Related to COVID-19 (Mar. 27, 2020), https://2017-2021.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19/index.html [https://perma.cc/H4GS-F6DU].

70 *See* Jessica Brandt & Torrey Taussig, *The Kremlin's Disinformation Playbook Goes to Beijing*, BROOKINGS (May 19, 2020), https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing [https://perma.cc/EA9N-ZLWF] ("In promoting its conspiracy theories, China exploits Russia's propaganda apparatus. RT and Sputnik, pro-Kremlin media outlets, are among the top five most-retweeted non-Chinese news outlets by China's state-funded media. Several individuals associated with pro-Kremlin websites are among the top 100 accounts most frequently retweeted by Chinese state funded media and diplomats.").

71 *See* Craig Silverman, Jane Lytvynenko & William Kung, *Disinformation for Hire: How a New Breed of PR Firms Is Selling Lies Online*, BUZZFEED NEWS (Jan. 6, 2020, 8:08 PM), https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms [https://perma.cc/5AN6-W7XR]; *see also* Max Fisher, *Disinformation for Hire, a Shadow Industry, Is Quietly Booming*, N.Y. TIMES (July 25, 2021), https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html [https://perma.cc/G5ZJ-W754] ("Commercial firms conducted for-hire disinformation in at least 48 countries [in 2020]—nearly double from the year before, according to an Oxford University study. The researchers identified 65 companies offering such services.").

72 *See* Ben Popken, *Trolls for Hire: Russia's Freelance Disinformation Firms Offer Propaganda with a Professional Touch*, NBC NEWS (Oct. 1, 2019, 11:40 AM), https://www.nbcnews.com/tech/security/trolls-hire-russia-s-freelance-disinformation-firms-offer-propaganda-professional-

purpose a client might desire.[73] Journalists have found PR firms offering to engage in high-tech corporate espionage and market influence, promoting a given company, and tarring the reputation of competitors.[74] Clients have also unleashed these firms' services against political opponents, both abroad[75] and in the United States.[76]

National governments have also gotten in on the outsourcing act. Just like Russia has given an effective free pass to criminal syndicates to engage in cybercrimes as a means of outsourcing these destabilizing campaigns,[77] governments, including the United States, have enabled disinformation for hire groups both indirectly and directly.[78] In one

---

n1060781 [https://perma.cc/C25U-LDEW] (describing such firms as "highly professional, offering responsive, polite customer service, and a menu of services," and noting that "[o]ne firm even had a public website with customer testimonials" and that "[r]esearchers said the disinformation firms offered the kind of professional responsiveness a company might expect from any contractor").

73 *See* Silverman, Lytvynenko & Kung, *supra* note 71 (describing one such firm's clients as "companies, brands, political parties, and candidates in Asia . . . purchasing an end-to-end online manipulation system, which can influence people on a massive scale—resulting in votes cast, products sold, and perceptions changed," and in light of the ethical concerns, highlighting one mainstream PR umbrella organization representative as saying, "[o]ur members are furious that they are ever tainted with the stain of these people who operate outside of [the industry's] ethical parameters" (second alteration in original)).

74 *See* Jeff John Roberts, *Disinformation for Hire: How Russian PR Firms Plant Stories for Companies in U.K. News Outlets, Social Media*, FORTUNE (Sept. 30, 2019, 5:45 AM), https://fortune.com/2019/09/30/russian-disinformation-for-hire [https://perma.cc/575Y-GDUF] (detailing investigation by a cybersecurity firm into Russia-based disinformation-for-hire organizations that provided such services, noting one "which spread stories that the fictitious [competitor] company had mistreated its employees, [and] offered a further service for filing false accusations with law enforcement and tax authorities").

75 *See, e.g.*, ELENA CRYST, ESTEBAN PONCE DE LEÓN, DANIEL SUÁREZ PÉREZ & SHELBY PERKINS, STANFORD INTERNET OBSERVATORY, BOLIVARIAN FACTIONS: FACEBOOK TAKES DOWN INAUTHENTIC ASSETS 3, 7 (2020), https://stanford.app.box.com/v/20200903-cib-bo-vz [https://perma.cc/U7PF-7HKL] (describing one private firm's disinformation campaigns bolstering certain political leaders and weakening others in Bolivia and Venezuela apparently at the direction of the strengthened politician).

76 *See* Hannah Murphy & Siddharth Venkataramakrishnan, *Boom in Private Companies Offering Disinformation-for-Hire*, FIN. TIMES (Jan. 12, 2021), https://www.ft.com/content/cb6b3342-a320-486e-b54c-a49ad32f2166 [https://perma.cc/D54E-AJW3] (noting use of such services in the 2020 presidential election and elections abroad).

77 *See* Isabelle Khurshudyan & Loveday Morris, *Ransomware's Suspected Russian Roots Point to a Long Detente Between the Kremlin and Hackers*, WASH. POST (June 12, 2021, 5:00 AM), https://www.washingtonpost.com/world/europe/russia-ransomware-cyber-crime/2021/06/11/e159e486-c88f-11eb-8708-64991f2acf28_story.html (last visited Sept. 16, 2021) (discussing understandings between ransomware groups and Russian government that "[a]s long as hackers left alone Russia and selected friendly countries, they could largely do as they wished without fear of a crackdown or extradition").

78 *See, e.g.*, JACK STUBBS & C. SHAWN EIB, GRAPHIKA, COORDINATED INAUTHENTIC BEE-HAVIOR: THE THIN LINE BETWEEN MARKETING AND POLITICAL PROPAGANDA: HOW AN

such case, the Pentagon hired a British PR firm to conduct both mainstream political media campaigns and secretive psyops in Iraq for a reported $540 million.[79] Such outsourcing allows governments to secure the benefits of disinformation warfare—riling an enemy's internal polity or weakening other nations' political leaders—with lower costs and greater deniability.[80]

Disinformation can impose immediate and sometimes life-and-death costs. In Syria, a combined Syrian-Russian disinformation campaign sought to undermine public support for the local humanitarian group, the White Helmets, because their efforts had uncovered evidence of Syrian and Russian human rights abuses.[81] The campaign portrayed the group "as terrorists," using chemical weapons on civilians and threating civilians as "legitimate targets."[82] The group's public backing waned and, as *The Washington Post* described, White Helmet personnel were arrested and tortured. "This isn't just buzz on the Internet," one stated. "We're dying for this."[83]

While on one hand the enormous durability and reach of these campaigns is alarming, those same factors plausibly imply that the status quo is more or less okay. That is, if states have effectively matched

---

EGYPTIAN FIRM RAN FAKE NEWS PAGES TARGETING ETHIOPIA, SUDAN AND TURKEY 1–2 (2021), https://public-assets.graphika.com/reports/graphika_report_inauthentic_beehavior.pdf [https://perma.cc/MF9D-NGH2] (describing a Cairo- and Dubai-based firm operating apparently at the behest of the Egyptian government to criticize political events in Ethiopia, Sudan, and Turkey); Nick Fielding & Ian Cobain, *Revealed: US Spy Operation that Manipulates Social Media*, GUARDIAN (Mar. 17, 2011, 9:19 AM), https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks [https://perma.cc/9H5V-PUZ2] (discussing U.S. military developing technology to facilitate foreign language social media manipulation); Stephen Zunes, *U.S. Intervention in Bolivia*, HUFFPOST (Oct. 23, 2008, 5:12 AM), https://www.huffpost.com/entry/us-intervention-in-bolivi_b_127528 [https://perma.cc/JJ9F-QAXJ] (describing U.S. effort in early-2000s to support oppositional political campaigns in Bolivia).

79 *See* Crofton Black & Abigail Fielding-Smith, *Fake News and False Flags*, BUREAU OF INVESTIGATIVE JOURNALISM (Oct. 2, 2016), https://labs.thebureauinvestigates.com/fake-news-and-false-flags [https://perma.cc/P476-RW23].

80 *See* Fisher, *supra* note 71 (stating that private disinformation services "appear to be cheap," often on the order of just tens of thousands, and "[t]he layer of deniability frees governments to sow disinformation more aggressively, at home and abroad, than might otherwise be worth the risk").

81 *See Chemical Weapons and Absurdity: The Disinformation Campaign Against the White Helmets*, BELLINGCAT (Dec. 18, 2018), https://www.bellingcat.com/news/mena/2018/12/18/chemical-weapons-and-absurdity-the-disinformation-campaign-against-the-white-helmets [https://perma.cc/9KAW-HAQZ].

82 *Id.*

83 Louisa Loveluck, *Russian Disinformation Campaign Targets Syria's Beleaguered Rescue Workers*, WASH. POST (Dec. 18, 2018), https://www.washingtonpost.com/world/russian-disinformation-campaign-targets-syrias-beleaguered-rescue-workers/2018/12/18/113b03c4-02a9-11e9-8186-4ec26a485713_story.html (last visited Sept. 11, 2021).

each other in their efforts and capabilities going back to the Roman era, existing solutions are capably addressing the threat and the costs have already been accepted. But there are differences today, which will grow with time, that should greatly dissuade inaction.

In one recent consideration of the problem, scholar Nabiha Syed identified five issues in contemporary geostate relations—each aggravated by pervasive internet connectedness—that leave America uniquely vulnerable to disinformation's effect.[84] First, manual and algorithmic filters curate the information to which a person exposes herself.[85] Americans are increasingly likely to hear only a single, slanted view of the world.[86] Second, localized communities creating their own online content further limits the inflow of facts.[87] As Syed describes it, "[E]ven though a television anchor might present you with a visual of Obama's American birth certificate, your online community—composed of members you trust—can present to you alternative and potentially more persuasive perspectives on that certificate."[88] Third, amplification: truly anyone can spread harmful messages to millions with the push of a button.[89] Fourth, and adding to that ease: exponential acceleration using AI and social media bots.[90] One more example of speed-enhancing technology, which Syed does not mention, is the threat of deepfakes. Even though Russian operatives were half-convincingly manipulating photos with scissors and tape back in the 1930s,[91] contemporary digital technology can make fake content appear real to all but the best-equipped experts.[92] And fifth, profit incentives deter capable actors from working to limit the problem. Syed suggests that "[s]ocial media platforms make fake news uniquely lucrative."[93]

---

84 Nabiha Syed, *Real Talk About Fake News: Towards a Better Theory for Platform Governance*, 127 YALE L.J.F. 337, 345–53 (2017).

85 *Id.* at 346.

86 *Id.*

87 *Id.* at 347.

88 *Id.* at 348.

89 *Id.* at 348–49.

90 *Id.* at 350–51.

91 *See* Colin Marshall, *Long Before Photoshop, the Soviets Mastered the Art of Erasing People from Photographs—and History Too*, OPEN CULTURE (Aug. 21, 2017), https://www.openculture.com/2017/08/long-before-photoshop-the-soviets-mastered-the-art-of-erasing-people-from-photographs-and-history-too.html [https://perma.cc/V3NW-J6LS].

92 *See* Washington Post Editorial Board, Opinion, *Deepfakes Are Dangerous—and They Target a Huge Weakness*, WASH. POST (June 16, 2019), https://www.washingtonpost.com/opinions/deepfakes-are-dangerous—and-they-target-a-huge-weakness/2019/06/16/d3bdbf08-8ed2-11e9-b08e-cfd89bd36d4e_story.html (last visited Sept. 11, 2021).

93 Syed, *supra* note 84, at 352 ("Advertising exchanges compensate on the basis of clicks for any article, which creates the incentive to generate as much content as possible with as little effort as possible.").

To these five factors, one more development makes disinformation more dangerous now: asymmetric warfare.[94] This concept implies that when a nation confronts a significantly stronger military power, the weaker nation's strengths will come from cheap and repeatable techniques whose damage is *asymmetric* to the cost.[95] In this sense, disinformation is the proverbial slingshot to the American giant, where such nations would have little or no chance on a physical battlefield.[96] Because America, more than any other nation, is dedicated to free speech, and many institutional protections support that right, using speech as the primary attack vector makes it exceedingly difficult for Americans to defend against it.

Not only has foreign disinformation grown as a threat, but American disinformation abroad has turned outright peaceful. Legal scholars Josh Geltzer and Jake Sullivan have valuably codified what makes Russia or China's contemporary disinformation campaigns wildly more abhorrent than any current American efforts.[97] They start from the premise that U.S. information campaigns, at least since the Cold War, might aim at supporting a particular electoral outcome, but always operate on the principles of transparency and stronger democracy.[98] In contrast, recent foreign campaigns: first, intend to divide communities and destroy common meanings of truth; second, utilize criminal methods like hacking and defamation; third, promote preferred candidates, like U.S. efforts; but fourth, seek to conceal their foreign role and turn Americans on each other; and fifth, ultimately unravel the democratic process, rather than deepen it.[99] This sea change in technology and global strategy has transformed an ancient battlefield technique into a contemporary, potentially existential threat to democratic society.

To summarize, though the term foreign disinformation is a broad concept, it has identifiable boundaries and a succinct definition. It poses

---

94 *See* Wolff Heintschel von Heinegg, *Asymmetric Warfare: How to Respond?*, 87 INT'L L. STUD. 463, 464 (2011).

95 *See id.* (defining asymmetric warfare as "leveraging inferior tactical or operational strength against [the] vulnerabilities of a superior opponent to achieve disproportionate effect with the aim of undermining [the opponent's] will in order to achieve the asymmetric actor's strategic objectives" (alterations in original)).

96 The affordability of disinformation makes this front of the cyberwar uniquely attractive to small states, or even terrorist groups. *See* Stengel, Stemming the Tide, *supra* note 34 ("[I]t's asymmetric warfare in that countries that can't afford missiles or jets or tankers or whatever can engage in this."). The operational costs for the IRA's 2016 election operation are estimated to have been only $1.25 million a month. *See* RUSSIA SENATE REPORT, *supra* note 4, at 39.

97 Geltzer & Sullivan, *supra* note 47.

98 *See id.*

99 *See id.*

a threat that is not new but escalating rapidly. While the factors in present-day information exchange described above might not be the only changes feeding the threat, they alone are enough to capture why new defenses are needed. Foreign disinformation, properly understood, can be deterred.

II. ALREADY-PROPOSED SOLUTIONS

This Part surveys already-proposed solutions and the challenges on which those solutions have stumbled. It groups them according to the four potential actors: (1) state agents; (2) state subsidiaries; (3) knowing domestic amplifiers; and (4) unwitting accomplices. This taxonomy is helpful because the most effective means of combatting disinformation varies depending on who is proximately disseminating that mistruth. With this survey of potential solutions spelled out (and indeed, it is only a sampling), the remainder of this Part explores five common challenges holding the solutions back: (1) defining policy goals; (2) which party is best situated to address those goals; (3) First Amendment concerns; (4) enforceability; and (5) the risk of the solution being used against legitimate players. These challenges affect each of the proposed solutions to some extent, and therefore, the existing menu is at best incomplete.

A. *The Actors*

State agents. State agents includes foreign leaders themselves, government ministries, or military detachments.[100] In practice, this might be the Iranian President or an elite Chinese army cyber unit, like the so-called Unit 61398.[101] These actors have unique immunity protections from U.S. law that can deter legal redress, whether civil or criminal.[102] Government officials are protected by diplomatic immunity

100 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 7–8.

101 *See* Kevin Townsend, *The United States and China—a Different Kind of Cyberwar*, SECURITYWEEK (Jan. 7, 2019), https://www.securityweek.com/united-states-and-china-different-kind-cyberwar [https://perma.cc/7S86-EVGM].

102 *See, e.g.*, Tel-Oren v. Libyan Arab Republic, 726 F.2d 774, 775 n.1, 805 n.13 (D.C. Cir. 1984) (Edwards, J., concurring) (Bork, J., concurring) (both concurrences agreeing that plaintiffs' suit against Libya was barred by the FSIA's noncommercial tort exception, which permits a plaintiff to recover against a foreign state only for noncommercial torts that cause injury, death, or property damage occurring in the United States).

in the case of foreign individuals,[103] or foreign sovereign immunity in the case of foreign governments.[104] Militaries are protected from legal process by customary international and treaty law, as well as status of forces agreements.[105] Of course, no state may deploy its armed forces into another state without a valid legal justification, and this includes cyber operations.[106] But in practice, military disagreements are often addressed on the battlefield or in diplomatic chambers.

Most groups forging responses to disinformation attacks by any type of state agent have focused on foreign policy solutions undertaken by the federal government, such as sanctions, democracy promotion, and bilateral agreements.[107] The U.S. government took this approach against Russian disinformation with economic countermeasures like the 2017 Countering America's Adversaries Through Sanctions Act (CAATSA).[108] At the same time, the U.S. military and intelligence agencies also seek to prevent disinformation attacks by attacking first.[109] As already noted, America has a history of active disinformation campaigns,[110] and in recent years, has advanced its kinetic offensive cyber capabilities.[111]

State subsidiaries. This category includes publicly acknowledged, state-owned agencies like Russia's RT media group and Sputnik[112] or

---

103 *See* Vienna Convention on Diplomatic Relations art. 31, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95 (granting diplomatic agents immunity from criminal jurisdiction and most civil actions in the receiving state).

104 *See* Foreign Sovereign Immunities Act of 1976, 28 U.S.C. §§ 1602–1611 (2020).

105 *See* DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL §§ 1.7–1.9 (2016); INT'L SEC. ADVISORY BD., REPORT ON STATUS OF FORCES AGREEMENTS 4–5, 31, 41 (2015).

106 *See* G.A. Res. 2131 (XX) (Dec. 21, 1965); G.A. Res. 2625 (XXV) (Oct. 24, 1970). *See generally* DANESH SAROOSHI, THE UNITED NATIONS AND THE DEVELOPMENT OF COLLECTIVE SECURITY: THE DELEGATION BY THE UN SECURITY COUNCIL OF ITS CHAPTER VII POWERS (1999). Deployment of armed forces into the territory of another state without its consent against a nonstate actor raises different legal questions. Such deployments often occur under the self-defense exception. *See* Terry D. Gill, *Legal Basis of the Right of Self-Defense Under the UN Charter and Under Customary International Law*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS 187–98 (Terry D. Gill & Dieter Fleck eds., 1st ed. 2010).

107 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at xii.

108 Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44 (codified in scattered sections of 22 U.S.C.).

109 *See* Jim Garamone, *Esper Describes DOD's Increased Cyber Offensive Strategy*, U.S. DEP'T OF DEF. (Sept. 20, 2019), https://www.defense.gov/News/News-Stories/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy [https://perma.cc/T5V7-CGFV].

110 *See supra* Section I.B.

111 *See* Isaac R. Porche III, *Fighting and Winning the Undeclared Cyber War*, RAND BLOG (June 24, 2019), https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html [https://perma.cc/QK7F-FVP3] ("[T]he United States is now actively responding to Russia's incursion on U.S. CI with its own attacks on Russian power plants.").

112 *See* Rutenberg, *supra* note 16.

China's China Central Television (CCTV),[113] as well as unacknowledged groups acting independently of a nation's organized intelligence services.[114] A key example of the latter was the key driver of the Russian 2016 U.S. election attack, the IRA, which Russian oligarch Yevgeny Viktorovich Prigozhin nominally owned and operated as a private holding.[115] State subsidiaries can also be quite autonomous, as with private firms that state actors hire.[116] The shadowy Archimedes Group is one such firm; based in Israel, it is reported to have conducted disinformation campaigns on behalf of unknown actors in Africa, Latin America, and Southeast Asia.[117] This category of actors rarely benefits from the same immunity protections as officials operating as a state agent, and as such, court processes are an option.[118] Individuals in the group that Prigozhin operated were among the defendants whom the Mueller team indicted—on charges of bank fraud, wire fraud, and conspiracy.[119]

Solutions that might also be used against state agents could deter this category. For example, as an early response to the Russian election interference, the Obama administration expelled from the United States

---

113 Louisa Lim & Julia Bergin, *Inside China's Audacious Global Propaganda Campaign*, GUARDIAN (Dec. 7, 2018, 1:00 AM), https://www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping [https://perma.cc/2QWZ-EXEP].

114 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 8–10.

115 *See* Tess Owen, *How Russian Trolls Screwed with America, According to the Mueller Report*, VICE NEWS (Apr. 18, 2019, 3:32 PM), https://www.vice.com/en_us/article/j5wqd3/how-russian-trolls-screwed-with-america-according-to-the-mueller-report [https://perma.cc/C728-RXML].

116 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 8–10.

117 *See* Craig Timberg & Tony Romm, *Facebook Shuts Down Israel-Based Disinformation Campaigns as Election Manipulation Increasingly Goes Global*, WASH. POST (May 16, 2019), https://www.washingtonpost.com/technology/2019/05/16/facebook-shuts-down-israel-based-disinformation-campaigns-election-manipulation-increasingly-goes-global (last visited Sept. 19, 2021); Simona Weinglass, *Who Is Behind Israel's Archimedes Group, Banned by Facebook for Election Fakery?*, TIMES ISR. (May 19, 2019, 4:34 PM), https://www.timesofisrael.com/who-is-behind-israels-archimedes-group-banned-by-facebook-for-election-fakery [https://perma.cc/6KLS-SEBR]; *see also* Gopal Ratnam, *Hired Guns of Disinformation Proliferate Online, Report Finds*, ROLL CALL (Aug. 26, 2020, 11:50 AM), https://www.rollcall.com/2020/08/26/hired-guns-of-disinformation-proliferate-online-report-finds [https://perma.cc/STU8-5D44] (describing other private firms that have conducted operations in Tunisia, UAE, and the United Kingdom).

118 *See generally* David E. Sanger & Nicole Perlroth, *As Election Nears, Government and Tech Firms Push Back on Russia (and Trump)*, N.Y. TIMES (Oct. 22, 2020), https://www.nytimes.com/2020/10/20/us/politics/election-hacking-trump-microsoft-cyber-command.html [https://perma.cc/MDG9-7BCR].

119 *See* Neil MacFarquhar, *Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as "Putin's Cook,"* N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html [https://perma.cc/DMB3-NX7U].

thirty-five Russian nationals associated with Kremlin spy agencies.[120] Technological defenses also reemerge. Commentators like White House national security coordinator Richard Clarke have proposed a cyberwar fortification response, hardening domestic infrastructure and, if necessary, launching online countermeasures to directed attacks.[121]

Domestic Amplifiers. Amplifiers transform otherwise isolated disinformation into mass media. They are often a key vehicle turning a story viral. They include social media platforms, so-called influencers[122] (real and fake), bots or other automation and augmentation technologies, domestic news media, or independent news-like websites.[123] Here, potential solutions are weaker. The number of actors is far greater and diverse, amplifiers sit smack in the middle of free speech and free press protections, and, because they are private actors, compelling action or inaction might be impossible.

Here, analysts and leaders have proposed or enacted a wide range of legislative remedies, some that promote transparency[124] and others that restrict threatening speech.[125] An example of the latter is a recent California law that makes it a crime to distribute deepfakes intended to manipulate an election,[126] and another California law creating a private right to sue entities that produce pornographic deepfakes using the

120 *See* Lauren Gambino, Sabrina Siddiqui & Shaun Walker, *Obama Expels 35 Russian Diplomats in Retaliation for U.S. Election Hacking*, GUARDIAN (Dec. 30, 2016, 2:47 AM), https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack [https://perma.cc/M2RF-XCSL].

121 *See generally* RICHARD A. CLARKE & ROBERT K. KNAKE, THE FIFTH DOMAIN: DEFENDING OUR COUNTRY, OUR COMPANIES, AND OURSELVES IN THE AGE OF CYBER THREATS (2019).

122 *See* Suzanne Kapner & Sharon Terlep, *Online Influencers Tell You What to Buy, Advertisers Wonder Who's Listening*, WALL ST. J. (Oct. 20, 2019, 8:59 PM), https://www.wsj.com/articles/online-influencers-tell-you-what-to-buy-advertisers-wonder-whos-listening-11571594003 (last visited Jan. 28, 2022) ("What began as friends and family sharing their favorite products has become a lucrative advertising industry of celebrity endorsers, influencers and meme creators. Such paid endorsements, known as sponsored content, are the online equivalent of a 30-second TV spot.").

123 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 7; Pollicino & Bietti, *supra* note 32, at 47–48.

124 *See United States Efforts to Counter Russian Disinformation and Malign Influence: Hearing Before the Subcomm. on State, Foreign Ops., and Related Programs of the H. Comm. on Appropriations*, 116th Cong. 8 (2019) [hereinafter Polyakova Remarks] (statement of Dr. Alina Polyakova, Brookings Inst.) (proposing an "Honest Ads Act").

125 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 17–19.

126 *See* Colin Lecher, *California Has Banned Political Deepfakes During Election Season*, VERGE (Oct. 7, 2019, 12:11 PM), https://www.theverge.com/2019/10/7/20902884/california-deepfake-political-ban-election-2020 [https://perma.cc/7SCD-UKEJ]. The law comes with significant limitations. It applies within only sixty days of an election. *Id.* Furthermore, "[n]ews media will be exempt from the requirement, as will videos made for satire or parody. Potentially deceptive video or audio will also be allowed if it includes a disclaimer noting that it's fake. The law will sunset in 2023." *Id.*

victim's identity.[127] Activist groups of different ideological shades have turned their spotlight on media companies themselves, urging corporate changes through consumer pressure.[128] Here, when restricting threatening speech by domestic entities, First Amendment concerns reach their apex.

This is also the category where technological and internal-corporate solutions are most prominent. In dealing with bots and deepfakes, which many social media platforms prohibit by their own bylaws,[129] private companies and public-private partnerships have developed solutions like algorithms designed to detect and flag (or block) automated and altered content.[130]

Social media platforms have also announced policy changes independent of, or at least in response to, market pressure. Twitter in Fall 2019 asserted it would block political advertisements for at least the next year.[131] Facebook established a new "oversight board," consisting of up to forty paid, part-time members who "will adjudicate controversies arising from Facebook's in-house efforts to enforce its standards on hate speech, misinformation[,] and other prohibited content."[132] Without yet exploring the reasons why, it bears mention that commentators and interest groups have already attacked these

---

127 *See* Carrie Mihalcik, *California Laws Seek to Crack Down on Deepfakes in Politics and Porn*, CNET (Oct. 7, 2019, 8:32 AM), https://www.cnet.com/news/california-laws-seek-to-crack-down-on-deepfakes-in-politics-and-porn [https://perma.cc/G7ER-XZ6G].

128 *See, e.g.*, AVAAZ, U.S. 2020: ANOTHER FACEBOOK DISINFORMATION ELECTION? 5 (2019), https://avaazimages.avaaz.org/US_2020_report_1105_v04.pdf [https://perma.cc/9BSW-3TYF] (progressive group calling on Facebook to work "with independent factcheckers to ensure that every user who has seen or interacted with false information is notified and offered a correction" (emphasis omitted)). In summer 2019, the White House joined in on the social pressure and held a summit of two hundred conservative organizations and personalities calling social media firms biased against conservative views. *See* Tony Romm, *White House Social Media Summit Not a "One-and-Done," Trump's Allies Say*, WASH. POST (July 12, 2019), https://www.washingtonpost.com/technology/2019/07/12/white-house-social-media-summit-not-one-and-done-trumps-allies-say (last visited Sept. 9, 2021).

129 *See* Adi Robertson, *Twitter Bans Bulk Tweeting and Duplicate Accounts in Bot Crackdown*, VERGE (Feb. 21, 2018, 1:37 PM), https://www.theverge.com/2018/2/21/17036708/twitter-automation-rule-changes-ban-bulk-tweeting-bot-crackdown-election [https://perma.cc/9GR2-K767].

130 *See, e.g.*, Sophia Ignatidou, *The Promise and Limitations of Technological Solutions to Disinformation*, EUR. SCI.-MEDIA HUB (Mar. 20, 2019), https://sciencemediahub.eu/2019/03/20/the-promise-and-limitations-of-technological-solutions-to-disinformation [https://perma.cc/PW4K-7SUZ].

131 Tony Romm & Isaac Stanley-Becker, *Twitter to Ban All Political Ads amid 2020 Election Uproar*, WASH. POST (Oct. 30, 2019), https://www.washingtonpost.com/technology/2019/10/30/twitter-ban-all-political-ads-amid-election-uproar (last visited Sept. 14, 2021).

132 Jeff Horwitz, *Facebook Forms Independent Board to Oversee Content Decisions*, WALL ST. J. (Sept. 17, 2019, 5:29 PM), https://www.wsj.com/articles/facebook-forms-independent-board-to-oversee-content-decisions-11568752897 (last visited Sept. 9, 2021).

internal measures as half-hearted, unmanageable, or pure window-dressing.[133] This is not to say that amplifiers themselves should not play a role. For firms like Facebook that host disinformation, it is impossible to imagine a solution in which they are not involved.[134] But there are many perceived shortcomings in their attempts, which means at least for now, their capacity and value in countering the threat is unknown.

Unwitting accomplices. This final category includes the recipients of information: the consumer public, individual decisionmakers, or information-consuming agencies.[135] The distinction between them and amplifiers is that accomplices have no intention of promoting disinformation or responsibility for others who may. Accomplices might be anyone who takes in disinformation and, if they share it, do so unaware of its mistruth, or they do so to call attention to its purpose.[136] It also includes elected leaders or government agencies when consuming rather than making the news. Here, the effects are most diffuse and so are the potential solutions.

Common proposals touch on better education and online security (the latter because disinformation often comes from hijacked accounts or is microtargeted based on hacked information).[137] Transparency is a

---

133 *See, e.g.*, Davey Alba, *Ahead of 2020, Facebook Falls Short on Plan to Share Data on Disinformation*, N.Y. TIMES (Sept. 29, 2019), https://www.nytimes.com/2019/09/29/technology/facebook-disinformation.html [https://perma.cc/Y3WH-ZD57]; Emily Dreyfuss, *Facebook's Fight Against Fake News Keeps Raising Questions*, WIRED (July 20, 2018, 7:42 PM), https://www.wired.com/story/facebook-fight-against-fake-news-keeps-raising-questions [https://perma.cc/R3SM-SBMJ]. *See generally* Bradley Hanlon, *A Long Way to Go: Analyzing Facebook, Twitter, and Google's Efforts to Combat Foreign Interference*, ALL. FOR SECURING DEMOCRACY, 2018, at 4–6.

134 *See* Mark Scott, *False Attacks on Facebook Could Bring "a Titanic-Sized Disaster" in 2020*, POLITICO (Nov. 6, 2019, 7:30 AM), https://www.politico.com/news/2019/11/06/facebook-misinformation-disaster-2020-elections-066539 [https://perma.cc/WM5R-5WVQ] (noting Facebook's defense against report that "[f]alse news reports that attack U.S. politicians have been viewed more than 150 million times on Facebook since the beginning of 2019").

135 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 7.

136 This analysis makes a distinction between two types of consumers if they repeat foreign disinformation that they acquire, such as by retweeting or reposting: those who do and those who do not know that the information that they are spreading is false. The latter category as it is used here encompasses only unwitting actors; those who know that they are spreading disinformation should be thought of as amplifiers. Other typologies often use a less accurate term for this last category, one which might encompass both groups: "consumer."

137 *See* BRENNAN CTR. FOR JUST., LIMITING FOREIGN MEDDLING IN U.S. CAMPAIGNS: KEY POLICY RECOMMENDATIONS 7–8 (2019), https://www.brennancenter.org/sites/default/files/analysis/BCJ_LimitingForeignMeddling_August2019.pdf [https://perma.cc/82KD-M5SP]; Dipayan Ghosh, *What Is Microtargeting and What Is It Doing in Our Politics?*, DISTILLED (Oct. 4, 2018), https://blog.mozilla.org/internetcitizen/2018/10/04/microtargeting-dipayan-ghosh [https://perma.cc/5Q5L-GGM6].

recurring theme.[138] Many groups have called for greater consumer data privacy to prevent nefarious microtargeting and manipulation of users.[139]

B. *The Challenges*

With the four types of actors spelled out, one can more readily identify the challenges. In distinguishing the actors from each other, even if there is overlap, each category has unique vulnerabilities and capabilities. As noted, some solutions are appropriate for only some groups, while other solutions are universal. Relevant to this analysis, legal processes have been notably absent from discussion. In considering why a new legal response is needed, the first step is to identify where the existing solutions fall short. There are at least five common challenges that any disinformation solution will confront.

First, the challenge of defining the underlying policy goals. This challenge becomes clear when considering the variety of actors. There are so many potential sources of disinformation and so many ill effects that it is hard to imagine one technique fixing the disinformation problem writ large. What threat then should the solution redress? Limiting foreign intelligence attacks during elections? The looming issue of AI, bots, and deepfakes? Or, is it the underlying lack of civic education and media literacy? Advocates can justify pursuing each of these goals, but limited resources and appetite require that policymakers address where the nation will get the most bang for the buck. For instance, solutions aimed at elections might overestimate the cost of electoral interference,[140] in which case, sweeping efforts to curtail political speech[141] might weaken the capacity to address the costlier threat of disinformation stoking racial conflict.[142] Or instead, a narrow

---

138 *See, e.g.*, BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 16, 18–19; Polyakova Remarks, *supra* note 124, at 8.

139 *See, e.g.*, Polyakova Remarks, *supra* note 124, at 5, 8 ("Such data collection limitation would make microtargeting and exploitation of individuals' personal data more difficult . . . .").

140 *See, e.g.*, Alexander Lanoszka, *Have We Overestimated International Disinformation?*, POL'Y OPTIONS POLITIQUES (May 21, 2019), https://policyoptions.irpp.org/magazines/may-2019/overestimated-international-disinformation [https://perma.cc/J47T-LJ5E]; Roberto Rocha, *Fears of Election Meddling on Social Media Were Overblown, Say Researchers*, CBC NEWS (Nov. 3, 2019, 4:00 AM), https://www.cbc.ca/news/canada/social-media-bots-trolls-canadian-election-2019-1.5343210 [https://perma.cc/7JUK-676T].

141 *See, e.g.*, Romm & Stanley-Becker, *supra* note 131.

142 *See* RUSSIA SENATE REPORT, *supra* note 4, at 39 ("Historically, the KGB's active measures program also made race a central feature of its operational targeting. As KGB archivist Vasili Mitrokhin noted: 'The attempt to stir up racial tensions in the United States remained part of

focus like limiting disinformation on social media might be ineffective or counterproductive. For example, an earlier Facebook tool to label false information as "disputed" perversely caused more sharing of the flagged content and thus increased public interest.[143] It ignored the bigger challenge of how to reduce disinformation's resonance and reach. Moreover, a misguided policy response into sensitive terrain, like free speech and elections, might further disrupt the public's trust in institutions and further fuel the threat.

Second, who are the parties best situated to combat the specified goals? Dividing the solutions into categories of actors reveals many leverage points at which to respond, but only certain entities are suited for some of those efforts. For instance, only government can lead a cyberwar counteroffensive or levy economic sanctions. Private companies are in control of regulating information online unless governments compel them.[144] Likewise, the media bears a burden to identify disinformation channeled through it or spot other parties who spread it.[145] Civic institutions and consumers play a large role in public education and resilience.[146]

Here, a grave challenge manifests in that each group might have perverse incentives not to take corrective action. Government might hesitate because it uses similar techniques.[147] For the U.S. military, it has to consider the cost of lowering the normative bar to counterattacks.[148]

Service A's stock-in-trade for the remainder of the Cold War.'"); NAT'L URB. LEAGUE, STATE OF BLACK AMERICA 10 (2019), http://soba.iamempowered.com/sites/soba.iamempowered.com/files/SOBA19G2E_NUL-SOBA-2019-ExecutiveSummary_FINAL%20COPY.pdf [https://perma.cc/554H-CDE5] ("Russian propagandists specifically targeted African Americans through a wide-reaching influence campaign. Their tactics included posing as legitimate activist groups, eroding trust in democratic institutions and spreading disinformation.").

143 *See* Jeff Smith, *Designing Against Misinformation*, MEDIUM (Dec. 20, 2017), https://medium.com/facebook-design/designing-against-misinformation-e5846b3aa1e2 [https://perma.cc/6ZZK-6TR5].

144 *See* Polyakova Remarks, *supra* note 124, at 7–9 (suggesting a slate of legislative proposals for Congress to consider).

145 *See* Amy S. Mitchell, Pew Rsch. Ctr., Countering Disinformation and Building Trust with News Consumers, Panel at the Council on Foreign Relations (Jan. 18, 2019), https://www.cfr.org/event/countering-disinformation-and-building-trust-news-consumers [https://perma.cc/GD7K-3D6A] ("[E]ven some of these sites that put in huge letters, you know: Satire! This is fake! People don't care. This is what they want to see, and so they're going to spread that anyway.").

146 *See* Ryan J. Foley, *Spread of Fake News Prompts Literacy Efforts in Schools*, PBS (Dec. 31, 2017, 12:11 PM), https://www.pbs.org/newshour/education/spread-of-fake-news-prompts-literacy-efforts-in-schools [https://perma.cc/DU42-9PDN].

147 *See* Nicolas, *supra* note 28, at 39–42 (describing the U.S. military's avowed PSYOPs strategies).

148 *See* Jonathan Reiber, *States Must Explain When a Cyber Attack Might Draw a Violent Reprisal*, DEF. ONE (June 6, 2019), https://www.defenseone.com/ideas/2019/06/states-must-explain-when-cyber-attack-might-draw-violent-reprisal/157533 [https://perma.cc/533F-KT8D].

It also goes without saying that some individuals in government will benefit from disinformation campaigns and they might have political reasons to deter enforcement. Online platforms and the news media often profit on disinformation.[149] And the public reads disinformation because they like it; the stories stimulate short-term interests and subconscious beliefs.[150] A RAND study applying workgrouping methods to these challenges noted that most consumer educational initiatives failed based on lack of ability or motivation.[151] It puts the burden of training on the consumer without granting them additional time or incentives.[152] Where it comes to choosing who is best equipped to tackle these problems, perverse incentives becomes an essential test.

Third is the issue of how to address America's First Amendment protections. Without attempting to summarize all relevant First Amendment doctrine,[153] suffice it to say that most but not all forms of speech are protected.[154] Though private communications platforms operate largely outside the First Amendment's reach, if the government

---

149 *See* Marin Dell, *Fake News, Alternative Facts, and Disinformation: The Importance of Teaching Media Literacy to Law Students*, 35 TOURO L. REV. 619, 626 (2019) ("[F]ake news is 'intentionally misleading articles, often published for profit or other gain.'" (citation omitted)).

150 *See* Tom Chatfield, *Why We Believe Fake News*, BBC (Sept. 8, 2019), https://www.bbc.com/future/article/20190905-how-our-brains-get-overloaded-by-the-21st-century [https://perma.cc/8LGJ-LEQH]. "The appetite for selective, biased, or partisan information is growing, and it will continue to do so given apparent trends in the U.S. public's information literacy, critical thinking, and partisanship." Micah Zenko, *The Problem Isn't Fake News from Russia. It's Us.*, FOREIGN POL'Y (Oct. 3, 2018, 3:22 PM), https://foreignpolicy.com/2018/10/03/the-problem-isnt-fake-news-from-russia-its-us (last visited Sept. 19, 2021).

151 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 49 ("[M]edia literacy efforts do not account for the fact that most people do not have the time, energy, or desire to put forth the kind of effort that media literacy demands. Most people are susceptible to emotional manipulation that plays on their existing prejudices and biases. While media literacy campaigns will certainly work for some people, it is possible that they will not work for those masses of people who are actually most vulnerable to emotional manipulation.").

152 *See* MONICA BULGER & PATRICK DAVISON, DATA & SOC'Y RSCH. INST., THE PROMISES, CHALLENGES, AND FUTURES OF MEDIA LITERACY 17 (2018), https://datasociety.net/pubs/oh/DataAndSociety_Media_Literacy_2018.pdf [https://perma.cc/9PAD-S7A4].

153 For a good summary, consider REPS. COMM. FOR FREEDOM OF THE PRESS, FIRST AMENDMENT HANDBOOK (Gregg P. Leslie ed., 7th ed. 2011) [hereinafter REPORTERS COMMITTEE], https://www.rcfp.org/resources/first-amendment-handbook [https://perma.cc/8JCZ-D7EL].

154 *See* KATHLEEN ANN RUANE, CONG. RSCH. SERV., FREEDOM OF SPEECH AND PRESS: EXCEPTIONS TO THE FIRST AMENDMENT 1–5 (2014), https://fas.org/sgp/crs/misc/95-815.pdf [https://perma.cc/8BE2-TY8F] (listing exemptions including obscenity, child pornography, "fighting words," and "true threats").

imposes restrictions, it risks overreach and either reversal in court, or alarmingly, no pushback at all and a shift in norms.[155]

Avoiding overreach is possible in one of two ways. First, by limiting new efforts to stay within an existing First Amendment exemption. Despite the Constitution's broad free speech protections, for decades, courts have accepted restrictions on various types of "unwanted speech."[156] The most fitting exemption for disinformation might be "fighting words," which the Court has described as "those which by their very utterance inflict injury or tend to incite an immediate breach of the peace."[157] To construe disinformation in such terms requires focusing on its propensity to disrupt civil society and fuel social conflict. Russian agents in the 2016 attack indisputably intended as much.[158] But the conflict and incitement the Russians attempted is a different breed from what the Court envisioned in *Chaplinsky v. New Hampshire*. Describing the fighting words exception in *Brandenburg v. Ohio*, the Court said advocating the use of force or criminal conduct is protected unless "such advocacy is directed to inciting or producing *imminent lawless action* and *is likely to* incite or produce such action."[159] There, the Court struck down a law that Massachusetts had used to prosecute Ku Klux Klan members who were participating in a cross-burning rally because the likelihood of violence was too indirect; one member in that rally had threatened the possibility of "revengeance taken" on the President, Congress, and Supreme Court if they continued "to suppress the white, Caucasian race."[160] This core interpretation of the fighting words exemption would need to be

155 *See* Prager Univ. v. Google LLC, 951 F.3d 991, 999 (9th Cir. 2020) (discussing the distinction between state speech and private forums and holding that posting on YouTube is not a First Amendment protected activity).

156 Eugene Volokh, *One-to-One Speech vs. One-to-Many Speech, Criminal Harassment Laws, and "Cyberstalking*," 107 NW. U. L. REV. 731, 740–41 (2013). Recognized First Amendment exceptions include "libel, and intentional incitement to likely and imminent criminal attack," *id.* at 751, as well as less nefarious forms, like "the 'seven dirty words' on radio." *Id.* at 747 (quoting FCC v. Pacifica Found., 438 U.S. 726, 777 (1978) (Brennan, J., dissenting)).

157 Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

158 *See* RUSSIA SENATE REPORT, *supra* note 4, at 34 (describing one IRA employee who said on the morning after the 2016 election, when "the most important result of our work arrived, we uncorked a tiny bottle of champagne . . . took one gulp each and looked into each other's eyes . . . utter[ing] almost in unison: '[w]e made America great'"); *see also* Julia Ioffe, *What Putin Really Wants*, ATLANTIC (Feb. 2018), https://www.theatlantic.com/magazine/archive/2018/01/putins-game/546548 [https://perma.cc/S4GN-VNJP] (describing Russia's explicit intent by 2016 to undermine the election).

159 Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (emphasis added); *see also* Schenck v. United States, 249 U.S. 47, 52 (1919) ("The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic. . . . The question in every case is whether the words used . . . create a clear and present danger . . . .").

160 *Brandenburg*, 395 U.S. at 446.

radically reconceived in the disinformation context to encompass disinformation's more diffuse effects. Alternative First Amendment exceptions, like defamation, might also encompass foreign disinformation, but even then, it could be an awkward fit.[161] That said, the Court has allowed expansion of these exceptions over time and a disinformation solution would likely need to do just that—push the constitutional boundaries further—but policymakers should attempt such expansion with caution because of the many types of acceptable and essential speech it might swallow.

A second way to limit overreach is to sidestep First Amendment concerns by targeting only unprotected speakers. But this is a narrow subset of actors. Free speech protection covers U.S. citizens, whether located on U.S. soil or abroad,[162] and permanent lawful residents residing in the United States.[163] This approach to avoid a First Amendment conflict could be applied only against state agents and state subsidiaries—that is, noncitizens. This would omit many domestic amplifiers—they often are citizens.[164] As nations take a more proactive stance against disinformation, there has already been a trend by foreign actors to encourage partners inside the targeted nations to create and spread disinformation themselves.[165] Evidence also exists of "[h]omespun operations on social media" in America, by Americans.[166] Foreign states will likely recruit local actors in America because local voices are far more influential in their communities.

Though neither of these existing routes to avoid First Amendment conflict will allow an easy solution, that does not mean the First Amendment is an unbreachable barrier. In other contexts such as terrorism, lawmakers and courts have found a narrow path through

---

161 For instance, a defense against slander and libel can be that the statements made are true or that "a defamatory falsehood involves a matter of public concern." RUANE, *supra* note 154, at 21.

162 The Supreme Court has long assumed, without specifically holding, "that First Amendment protections reach beyond our national boundaries." Haig v. Agee, 453 U.S. 280, 308 (1981). That said, the Court has weakened, without eliminating, certain rights for U.S. citizens while abroad. *See* Timothy Zick, *The First Amendment in Trans-Border Perspective: Toward a More Cosmopolitan Orientation*, 52 B.C. L. REV. 941, 942–44 (2011).

163 *See* Kwong Hai Chew v. Colding, 344 U.S. 590, 596 n.5 (1953).

164 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 10–11.

165 *See* GROSSMAN, BUSH & DIRESTA, *supra* note 6, at 54.

166 Isaac Stanley-Becker & Tony Romm, *Opponents of Elizabeth Warren Spread a Doctored Photo on Twitter. Her Campaign Couldn't Stop Its Spread.*, WASH. POST (Nov. 27, 2019), https://www.washingtonpost.com/technology/2019/11/27/opponents-elizabeth-warren-spread-doctored-photo-twitter-her-campaign-couldnt-stop-its-spread (last visited Sept. 19, 2021).

these constraints to fashion statutes that control unacceptable conduct without unfairly limiting constitutional rights.[167]

The fourth challenge is enforceability, which encompasses a whole slate of legal and practical issues. In addition to First Amendment protections, there are statutory protections for many online platforms or news agencies, undermining the capacity to regulate them.[168] This includes not only online platforms' immunity from private suits, but essential press protections like whistleblower laws and state-law reporter shield privileges.[169] Another enforceability problem is whom to hold liable and how. How will the original sources of disinformation be identified? In retrospect, it is easy to point at the actors in the 2016 Russian disinformation operation, but that took separate investigations by the CIA, Senate, and a special prosecutor to achieve.[170] Outside groups and media platforms have launched their own analyses recently, but it could be difficult for a lone victim to obtain the necessary evidence to identify, let alone convict, the culprit.[171] The introduction of private firms acting on behalf of state actors does not prevent fixing blame, but it heightens the burden of proving a state's culpability, requiring the plaintiff to identify another link in the chain. Separately, in terms of fixing blame, it seems fair that unwitting consumers should not be held liable for spreading content, but if authorities are to target amplifiers, policymakers must determine what mens rea is required to separate those categories. Lastly, the issue of remedy. When the target is a foreign actor in noncooperative nations, authorities may be unable or uninterested in enforcing verdicts.[172] Is it sufficient to have a court verdict holding a foreign actor responsible, even if the remedy is never fulfilled?

---

167 *See infra* Section IV.F (discussing material support under the antiterrorism statute, 18 U.S.C. § 2339B).

168 *See, e.g.*, Mike Masnick, *NY Times Opinion Section Gets CDA 230 Wrong Again!*, TECHDIRT (Oct. 4, 2019, 12:03 PM), https://www.techdirt.com/articles/20191004/10073843124/ny-times-opinion-section-gets-cda-230-wrong-again.shtml [https://perma.cc/BW9N-M726] (discussing the First Amendment conflicts in proposed changes to the safe harbor provisions of the Online Copyright Infringement Act § 230).

169 *See* REPORTERS COMMITTEE, *supra* note 153, at 23 ("Thirty-nine states and the District of Columbia have adopted shield laws affording the media varying degrees of protection against subpoenas.").

170 *See* JAMIESON, *supra* note 50, at 31–33 (crediting U.S. intelligence agencies, congressional intelligence committees, and the Mueller investigation among many other sources for exposing Russia's role).

171 *See, e.g.*, Tonya Mosley & Serena McMahon, *How One Organization Is Curbing the Spread of Disinformation in Black, Brown Communities*, WBUR (Sept. 2, 2020), https://www.wbur.org/hereandnow/2020/09/02/disinformation-black-brown-voters [https://perma.cc/H8PH-H2HQ].

172 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 36–37.

The fifth and final challenge is that the solutions themselves could be weaponized and turned back against legitimate players.[173] Asymmetric warfare necessarily looks for a nation's greatest vulnerabilities, and those are often the areas that the target nation has an interest in leaving free. Using speech against America is the perfect example of turning a shield into a sword. America's enemies can turn the First Amendment against it, not only by defending their attacks under its provisions (for example, recruiting domestic partners), but by forcing an overzealous response.[174] Any restriction on harmful speech necessarily risks weakening rights for similar types of speech. Policymakers and society broadly must agree where to draw the line, balancing national security and freedom. Even efforts to increase transparency can result in blowback by authoritarian regimes. When American authorities sought to counter Russian election interference by forcing media groups RT and Sputnik to register under the Foreign Agents Registration Act (FARA), Russian authorities in turn forced Voice of America, Radio Free Europe/Radio Liberty, and seven other U.S.-backed outlets to register as foreign agents, which in turn "had a powerful chilling effect on Russian outlets."[175] "[T]he cost of continuing to call out Russian actors as foreign agents may well be the demise of the dissemination of independent media voices within Russia."[176] Many of the currently proposed remedies are prone to misuse.[177]

In considering the proposed solutions and their challenges, two points bear reinforcing: First, useful solutions will remain conscious of which actors they are targeting. In the end, all actors must be addressed. Second, challenges arising from imprecise policy goals, enforceability, and First Amendment protections apply in each instance. The right solutions will be prepared to wisely tackle them all.

---

173 *See* Amanda Bennett, Stemming the Tide of Global Disinformation, Meeting at the Council on Foreign Relations (Oct. 11, 2019) [hereinafter Bennett, Stemming the Tide], https://www.cfr.org/event/stemming-tide-global-disinformation [https://perma.cc/CY4C-YKD3] ("I will say what I always say . . . write the laws as if your adversaries are going to be the ones implementing them. . . . [T]hink about a law like that in the hands of somebody you don't like.").

174 *See* Marantz, *supra* note 11 ("Noxious speech is causing tangible harm.").

175 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 34.

176 *See id.* at 35.

177 *See, e.g.*, Dave Maass, *California Bill to Ban "Fake News" Would Be Disastrous for Political Speech*, ELEC. FRONTIER FOUND. (Mar. 28, 2017, 12:00 PM), https://www.eff.org/deeplinks/2017/03/california-bill-ban-fake-news-would-be-disastrous-political-speech [https://perma.cc/M94J-U23Z] (criticizing a proposed 2017 California law that would have banned "fake news," warning of "candidates and others being accused of crimes at the slightest hint of hyperbole, exaggeration, poetic license, or common error").

III. A NEW PRIVATE RIGHT OF ACTION

With the terrain defined, this Part, in concise terms, constructs the statute. First, this Part lists the statute's elements; second, it defines the precise goal. Subsequently, in Part IV, the Article digs deeper into the elements and shows how they enable the statute, unlike already-proposed solutions, to succeed.

A. *A Law that Balances Security and Freedom*

Solving the online disinformation problem should provoke gut-level discomfort. At its heart, the goal is to limit one of democracy's great freedoms—that of expressing and consuming ideas. From its birth, the internet was celebrated as an engine of free expression[178] and a source of global liberalization.[179] The fact that the internet has veered from these ideals does nothing to lessen the essentiality of those values. In proposing any means to combat online disinformation, wise policymakers must operate with these goals intact. In some ways, that means imperfect solutions. Better to let some harmful speech through than to over-restrict. A solution that protects against all harmful speech would become a First Amendment cancer. The type of speech that people need protection from is not that which is upsetting or untrue, but instead, lies that are strategically milled to harm.

The statute proposed here is aimed squarely at weaponized speech. As Justice Holmes once wrote, "[I]f there is any principle of the Constitution that more imperatively calls for attachment [to the Constitution] . . . it is the principle of free thought—not free thought for those who agree with us but freedom for the thought that we hate."[180] And to state it crudely, sticks and stones may break one's bones, but most words can never hurt. The anti-disinformation law we need would target only those words that truly injure.

---

178 *See* David Foster, *On the Open Internet and the Free Web*, CERN (Mar. 12, 2014), https://home.cern/news/opinion/computing/open-internet-and-free-web [https://perma.cc/PG69-XBBA] ("The internet created the platform and opportunity for people to communicate, to collaborate and to share at unprecedented scale and speed.").

179 *See* Timothy Kirkhope, *How the Internet Is Transforming Democracy*, INDEPENDENT (Dec. 12, 2012, 2:56 PM), https://www.independent.co.uk/voices/comment/how-the-internet-is-transforming-democracy-8411474.html [https://perma.cc/BM5V-T5SD] ("[T]he internet can transform economies by allowing companies to work more efficiently, it can also change the relationship between governments and citizens—for the better.").

180 United States v. Schwimmer, 279 U.S. 644, 654–55 (1929) (Holmes, J., dissenting), *overruled in part by* Girouard v. United States, 328 U.S. 61 (1946).

This proposed statute aims to fill a narrow but important gap. Namely, it would thwart disinformation when the actor maliciously causes demonstrable harm. It does this by achieving another goal that already-proposed solutions largely miss: empowering the victim. Whereas many approaches try to help consumers avoid disinformation, this statute seeks to make the victims whole.[181] Whereas others leave in place perverse incentives—pecuniary, political, and psychological—this solution encourages parties to act. Though many solutions target only one actor, this proposal can be used against all parties. Finally, this solution can attack a wide variety of disinformation, whether meant to alter an election, sabotage industries, or simply sow dissent.

The Proposed Statute

This anti-disinformation law grants individuals who have suffered harm a private right of action for money damages against other parties—domestic or foreign; and state, corporate, or private—who by reckless neglect or intentional malice, spread false information that is fairly traceable to a foreign disinformation program.[182]

The statute has the following specific provisions:

> Culpable foreign disinformation is defined by: (1) a foreign source; (2) factual mistruth; (3) the originator's malicious intent and strategic aim to undermine civic well-being; and (4) resulting harm when the factual mistruth is released into the public sphere.
>
> A court would have jurisdiction over an American person who suffers injury, regardless of where the foreign disinformation is propagated or where the harm occurred, as long as the defendant used a United States–based facility of commerce or communication.
>
> The plaintiff must show injury in fact to obtain standing.
>
> Any mens rea less than recklessness will be insufficient to satisfy guilt.
>
> The plaintiff must show that the defendant's actions were a substantial factor in causing her harm. Pure comparative negligence

---

181 The goal of making the victim whole depends on successful payment of the remedy, and in many instances with foreign actors, collection will be prohibitively difficult. That said, collection is not impossible. And the deterrent effect of outstanding claims—both against the named defendant and other actors pursuing similar ends—carries its own benefits. *See supra* Section II.B.

182 A final statute would have to be part of a larger omnibus bill. This is in no small part because it would require changes to laws that grant foreign immunity or establish corporate safe harbors, which means any passed legislation would lie scattered throughout the U.S. Code. As a result, this Section focuses on the key provisions that should be included in the legislation rather than specific language of a final statute.

> applies. If the plaintiff or other parties were contributorily negligent, the factfinder should apportion fault accordingly.
>
> If the plaintiff successfully proves liability, the court may award up to treble punitive damages, plus compensatory damages.
>
> As an exception to the FSIA, a foreign state's government, military, intelligence community leaders or members, or supported entities thereof may be held financially liable under this provision.
>
> The United States government may assist in collecting damages by attaching claims under this law to funds seized from the foreign nation or entity (sources from which funds may be attached will be enumerated).
>
> There will be no executive waiver whereby the executive branch may halt proceedings.

B. *The Policy Goal*

Plainly stated, the specific goal of this law is to reduce the flow of foreign disinformation to American consumers at all times. It is broad in that it encompasses all varieties of actors and targets, but narrowed by requiring a provable, initial foreign source.

At its base, any smart policy goal maximizes objectives relative to resources. The objective must also be in line with the community's desires. Many proposed anti-disinformation solutions stumble at the policy stage. A key example is consumer education, where the goal—turn the tide of news readers against foreign disinformation by helping them identify mistruths—is misaligned with (or oblivious to) consumer desires and capacities.[183] Another example is industry self-regulation, which ignores companies' financial interest in the status quo.[184]

---

183 *See* Bertin Martens, Luis Aguiar, Estrella Gomez-Herrera & Frank Mueller-Langer, Joint Rsch. Ctr., Eur. Comm'n, *The Digital Transformation of News Media and the Rise of Disinformation and Fake News* 7 (JRC Digital Econ. Working Paper No. 02, 2018), https://ec.europa.eu/jrc/communities/sites/jrccties/files/dewp_201802_digital_transformation_of_news_media_and_the_rise_of_fake_news_final_180418.pdf [https://perma.cc/47E2-FY8T] ("Strengthening media literacy may help consumers to better assess the quality of news articles but also shifts the burden of quality control from distributors to consumers.").

184 *See* BODINE-BARON, HELMUS, RADIN & TREYGER, *supra* note 33, at 46 ("[S]olutions must originate with social media companies on their own terms, and the tension between the companies' interests and the public interest in combating disinformation simply cannot be wished away."); Olivia Beavers, *Rosenstein: Social Media Companies Need to Self-Regulate or Government Will Take Action*, HILL (Nov. 29, 2018, 2:52 PM), https://thehill.com/policy/technology/418952-rosenstein-social-media-companies-need-to-self-regulate-or-they-will [https://perma.cc/QXC5-MZPL].

This proposed statute requires minimal investment of resources. The costs are borne by the litigants and partially reimbursed through successful suits. Enforcement—seeking attached funds—would sometimes require state assistance and the proceeds would come out of monies that would otherwise go to another recipient, but law enforcement would be doing that forfeiture collection regardless, and ultimately, the cost is paid by the complicit actors.

Empowering the victim has other advantages. Even if civil discovery is not always easy, it will be a new tool to pry into secretive firms or state actors and expose disinformation attacks and their techniques. As for financial awards, while large monetary judgments might do little to deter foreign states, they could limit assistance by oligarchs who are exposed via Western business interests and have an outsized effect on domestic companies or public figures, discouraging reckless behaviors. Furthermore, fighting disinformation is truly an all-hands-on-deck effort. The failed response so far has shown that further, wise contributions to the battle are needed, and this new law will empower a force of "private attorney[s] general" to contribute.[185] Most importantly, this solution carries a natural incentive to use it: financial and/or emotional payoff. The reward for fighting disinformation in this approach is not merely deterring future attacks—a goal that is hard to take personal appreciation of—but also making the victim whole if winnings are collected or at least giving the victim the satisfaction of her day in court.[186]

This law does not purport to be a complete solution. But it will be an important one.

IV. WHY THIS STATUTE SUCCEEDS

This final Part identifies the six most demanding obstacles the statute might face and shows how its elements account for each. Implementing any solution will mean running a practical and constitutional gauntlet, but from the start, this statute is primed to succeed.

---

185 *See, e.g.*, Newman v. Piggie Park Enters., Inc., 390 U.S. 400, 402 (1968).

186 *See generally* Karen A. Hegtvedt & Caitlin Killian, *Fairness and Emotions: Reactions to the Process and Outcomes of Negotiations*, 78 SOC. FORCES 269 (1999); Tracy M. Loos, *Name-Clearing Hearings, Gratuitous Remedies, and Common Law Writs of Certiorari—Are They Worth Their Weight in Gold?*, 22 S. ILL. U. L.J. 201, 215 (1997) ("Practically speaking, a gratuitous remedy is more comforting than a flat denial of all prayed for remedies. However, when the judge addresses the plaintiff's prayed for remedies, the plaintiff at least feels that he has had his day in court.").

A. *Private Right of Action in a Terrorism Context*

This statute's strongest attraction is that the federal government has successfully fielded something very much like it before. In so doing, courts and policymakers have worked out the kinks, which gives this proposal a racing start. An analog for the anti-disinformation law exists in the antiterrorism context: the 1992 Antiterrorism Act, modified in 2016 by the Justice Against Sponsors of Terrorism Act and the Anti-Terrorism Clarification Act of 2018 (hereinafter referred to collectively as the Antiterrorism Act, or ATA).[187] Through this legislation, Congress created a private right of action for terrorism victims or their beneficiaries to seek civil remedies against the responsible groups or their state sponsors.[188] Just as foreign disinformation victims currently have no means to win recompense, Congress passed the Antiterrorism Act to enable other victims who had no recourse: the family members of Americans killed in the 1985 hijacking of the Achille Lauro cruise ship[189] and the Pan Am Flight 103 bombing.[190] The bills achieved this by amending the Foreign Sovereign Immunities Act (FSIA), eliminating protection for states or their agents if claimants proved them culpable in a terrorist act.[191] Through its many revisions, Congress expanded the Antiterrorism Act's reach. These combined changes, primarily codified in the criminal code as 18 U.S.C. § 2333, empowered victims and their family members to do in the terrorism context exactly what the proposed disinformation law seeks to do in its context: punish and weaken wrongdoers through civil enforcement and, to some degree, make the victims whole.[192]

---

187 18 U.S.C. § 2333 (2020); *see* Federal Courts Administration Act of 1992, Pub. L. No. 102-572, § 1003(a)(4), 106 Stat. 4506, 4522 (1992); Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, § 3(a), 130 Stat. 852 (2016); Anti-Terrorism Clarification Act of 2018, Pub. L. No. 115-253, § 3(a), 132 Stat. 3183 (2018).

188 *See* 18 U.S.C. § 2333.

189 *See* Judith Miller, *Hijackers Yield Ship in Egypt; Passenger Slain, 400 Are Safe; U.S. Assails Deal with Captors*, N.Y. TIMES (Oct. 10, 1985), https://www.nytimes.com/1985/10/10/world/hijackers-yield-ship-egypt-passenger-slain-400-are-safe-us-assails-deal-with.html [https://perma.cc/VW9R-LQ9G] (discussing the cruise ship Achille Lauro hijacking).

190 *See* Tom Jackman, *Pan Am Pilots, Still Feeling Victimized 28 Years After Lockerbie, Seek Money from Libya Fund*, WASH. POST (Dec. 16, 2016), https://www.washingtonpost.com/news/true-crime/wp/2016/12/16/pan-am-pilots-still-feeling-victimized-28-years-after-lockerbie-seek-money-from-libya-fund [https://perma.cc/A7WM-2GYJ] (discussing ongoing civil litigation over Lockerbie bombing).

191 *See* Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. 104-132, §§ 221–233, 110 Stat. 1214, 1241–43 (1996) (codified as 28 U.S.C. § 1605).

192 *See* 18 U.S.C. § 2333(a).

The biggest challenge that Congress dealt with in the Antiterrorism Act was expanding jurisdiction.[193] In a 1996 revision, Congress made a private right of action explicit in the text (rather than presuming an implied right under international law), broadened the law's extraterritorial reach, and opened the possibility of foreign aliens suing in the United States' courts.[194] The 2018 revision expanded jurisdiction further by enabling claims against an actor-defendant if that defendant had taken advantage of the United States' facilities or material assistance in any way.[195] This allowed suits against nonstate actors in instances of so-called secondary liability, when those actors aided and abetted but did not directly participate in attacks (allowing material-support claims against individuals and companies that enabled terrorist acts).[196] The proposed anti-disinformation statute takes heed of this slow expansion of jurisdiction by opening the door at the outset to claims by any harmed citizen, regardless of where the harm occurs. And Courts will gain personal jurisdiction over foreign actors whenever they rely on domestic channels of commerce or

193 *See* Stephen J. Schnably, *The Transformation of Human Rights Litigation: The Alien Tort Statute, the Anti-Terrorism Act, and JASTA*, 24 U. MIA. INT'L & COMPAR. L. REV. 285, 309, 314–15 (2017) (describing jurisdictional challenges to civil terrorism suits before the Antiterrorism Act).

194 *See* Pub. L. 104-132, § 221(a), 110 Stat. 1241 (codified as 28 U.S.C. § 1605) (1996); DAVID P. STEWART, FED. JUD. CTR., THE FOREIGN SOVEREIGN IMMUNITIES ACT: A GUIDE FOR JUDGES 100–02 (2d ed. 2018), https://www.fjc.gov/sites/default/files/materials/41/FSIA_Guide_2d_ed_2018.pdf [https://perma.cc/XK6Y-REEN]; Harold Hongju Koh, *Civil Remedies for Uncivil Wrongs: Combatting Terrorism Through Transnational Public Law Litigation*, 50 TEX. INT'L L.J. 661, 671 n.46 (2016).

195 More specifically, JASTA established that any defendant "shall be deemed to have consented to personal jurisdiction" if it does one of two things: (1) receives U.S. foreign assistance from international law enforcement authorities; or (2) establishes or maintains a headquarters or other facility in the United States while benefiting from a waiver or suspension of a statutory provision that bars groups from operating such facilities in the United States. Harry Graver & Scott R. Anderson, *Shedding Light on the Anti-Terrorism Clarification Act of 2018*, LAWFARE (Oct. 25, 2018, 12:00 PM), https://www.lawfareblog.com/shedding-light-anti-terrorism-clarification-act-2018# [https://perma.cc/G9BH-GZDH]. The 2018 revision also eliminated certain legal defenses (such as a loophole that allowed a terrorist defendant to argue it was engaged in a state-authorized use of force, as had the PLO) and made more assets available for attachment. *See id.*

196 JASTA extended ATA liability to those who conspire to commit acts of international terrorism or who aid and abet those acts by "knowingly providing substantial assistance." 18 U.S.C. § 2333(d)(2) (2020). While JASTA was written in general terms, it was avowedly drafted to help 9/11 victims' families sue Saudi Arabia for its suspected role in those attacks and the Act received widespread bipartisan support. *See* Ingrid Wuerth, *Justice Against Sponsors of Terrorism Act: Initial Analysis*, LAWFARE (Sept. 29, 2016, 2:19 PM), https://www.lawfareblog.com/justice-against-sponsors-terrorism-act-initial-analysis# [https://perma.cc/EU2M-NZ3W]; Patricia Zengerle, *Senate Passes Bill Allowing 9/11 Victims to Sue Saudi Arabia*, REUTERS (May 17, 2016, 12:38 PM), https://www.reuters.com/article/us-saudi-usa-congress/senate-passes-bill-allowing-9-11-victims-to-sue-saudi-arabia-idUSKCN0Y8239 [https://perma.cc/5K9C-G74R].

communication: posting information on American-owned social media firms, using U.S.-based internet servers, or contributing money to amplifiers via American credit card processors, for instance.

Immunity posed a similar jurisdictional barrier for the Antiterrorism Act. Before Congress passed it, FSIA prohibited claims against any foreign leader and many foreign companies and officials.[197] The statute overcame the immunity bar by modifying FSIA to include acts of terrorism officially endorsed or enabled by foreign states, referred to as primary responsibility.[198] The exception was originally limited to a handful of nations that had been formally designated by the Secretary of State.[199] The government gradually expanded that list, and in 2016, Congress entirely removed the requirement that the defendant group be an officially named sponsor.[200] The law did not (and still does not) allow victims to sue states for aiding and abetting (only nonstate actors may face secondary liability).[201] In other words, the state or state agent must be directly involved in planning or executing the action. The immunity challenge should serve several cautionary notes in drafting the anti-disinformation law, another of which—executive waiver—is discussed in depth below. But as to jurisdiction, while the proposal does not directly address secondary liability, its framers might consider adding a more specific aiding-and-abetting provision that waives immunity for state defendants.

The Antiterrorism Act has also dealt with complex procedural issues, like how to serve process.[202] In March 2019, the Supreme Court

---

197 *See* John F. Murphy, *Civil Litigation Against Terrorists and the Sponsors of Terrorism: Problems and Prospects*, 28 REV. LITIG. 315, 332 (2008).

198 JASTA allows suit against foreign officials for

> any case in which money damages are sought against a foreign state for physical injury to person or property or death occurring in the United States and caused by . . . an act of international terrorism in the United States; and . . . a tortious act or acts of the foreign state, or of any official, employee, or agent of that foreign state while acting within the scope of his or her office, employment, or agency, regardless where the tortious act or acts of the foreign state occurred.

Steve Vladeck, *The Senate Killed JASTA, Then Passed It . . .*, JUST SEC. (May 18, 2016), https://www.justsecurity.org/31156/senate-killed-jasta-passed-it [https://perma.cc/4M48-FLGK].

199 Before 9/11, this was Cuba, Iran, Libya, North Korea, Sudan, Syria, and Iraq. *See* STEWART, *supra* note 194, at 100.

200 *See* Jason B. Binimow, Annotation, *Justice Against Sponsors of Terrorism Act ("JASTA"), Pub. L. No. 114-222, 130 Stat. 852 (2016) (Codified at 28 U.S.C.A. § 1605B)*, 31 A.L.R. Fed. 3d Art. 4 (2018).

201 *See* Schnably, *supra* note 193, at 382–83.

202 *See* Brief for the United States as Amicus Curiae, Tel-Oren v. Libyan Arab Republic (1984), *reprinted in* 24 I.L.M. 427, 434 (1985) ("In these circumstances, we question whether this Court

held that mailing notice directly and expeditiously to a minister of foreign affairs at his ordinary place of business in the foreign state was an appropriate mechanism for suing Sudan for a terrorist attack.[203] The rule should stand in the disinformation context as well.

The Antiterrorism Act did not expand discovery procedures beyond the standard rules, and litigation shows that discovery remains a hurdle, especially when it involves suits against state actors.[204] Admittedly, when actors cover up their tracks, as with disinformation attacks and in contrast to terrorist attacks (where actors often seek credit), the barrier is even higher. But the antiterrorism legislation has set actual examples that anti-disinformation plaintiffs can follow to overcome this hurdle. Arguably, if a plaintiff has enough resources, there are few statutory bars on discovery in antiterrorism cases; FSIA is not prohibitive. The Supreme Court upheld broad discovery under FSIA in a post-judgment execution action against Argentina in 2014, even over the objection of the U.S. government.[205] A factor that might lower the discovery bar in disinformation campaigns is that there are a number of other organizations—government and private—that often publish evidence of these attacks and their participants.[206] To the extent that discovery remains a challenge, there are extreme measures that the anti-disinformation framers might consider. For instance, Rep. John Conyers proposed a solution to the discovery problem in a proposed antiterrorism amendment that would have allowed courts to conclude any fact against the defendant if a foreign state thwarted attempts at discovering that fact.[207]

---

should exercise its discretionary jurisdiction to construe a statute as complex and little understood as the alien tort statute in a context in which the outcome of the case is unlikely to be affected.").

203 *See* Republic of Sudan v. Harrison, 139 S. Ct. 1048, 1056 (2019).

204 *See In re* Terrorist Attacks on Sept. 11, 2001, No. 03-MD-1570, 2020 WL 1181943, at *1–2 (S.D.N.Y. Mar. 12, 2020) (setting forth legal standard and consideration of judicial restraint that apply when conducting jurisdictional discovery against state actors under the ATA).

205 *See* Ingrid Wuerth, Republic of Argentina v. NML Capital*: Discovery and the Foreign Sovereign Immunities Act*, LAWFARE (June 16, 2014, 10:28 PM), https://www.lawfareblog.com/republic-argentina-v-nml-capital-discovery-and-foreign-sovereign-immunities-act [https://perma.cc/C2A2-ZJTB].

206 Reports from organizations like the ones cited here and above are examples. *See, e.g.*, GROSSMAN, BUSH & DIRESTA, *supra* note 6; AVAAZ, *supra* note 128; *see also* MATTHEW HINDMAN & VLAD BARASH, KNIGHT FOUND., DISINFORMATION, "FAKE NEWS" AND INFLUENCE CAMPAIGNS ON TWITTER (2018), https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/238/original/KF-DisinformationReport-final2.pdf [https://perma.cc/N9MZ-L7ZC].

207 *See* JUSTICE FOR VICTIMS OF TERRORISM ACT, H.R. COMM. REP. NO. 106-733, at 28 (2000) ("In cases involving foreign terrorist states, obtaining discovery from such litigants can be difficult, if not impossible. American citizens are subject to a very burdensome discovery process

The antiterrorism legislation worked through the issue of mens rea at the pleading level, establishing the minimum requirements to state a claim. In one recent case under the law, *Crosby v. Twitter, Inc.*, victims of the 2016 Pulse Nightclub shooting sued Twitter for hosting ISIS messages that allegedly radicalized the attacker.[208] The Sixth Circuit upheld the district's court dismissal, ruling that the victims had not made a facial claim that Twitter "knowingly and substantially assist[ed]" the attacker.[209] In doing so, the Sixth Circuit affirmed the district court's six-factor mens rea analysis, which other circuits use as well: "(1) the nature of the act encouraged, (2) the amount of assistance given by defendant, (3) defendant's presence or absence at the time of the tort, (4) defendant's relation to the principal, (5) defendant's state of mind, and (6) the period of defendant's assistance."[210] In its analysis, the district court held that plaintiffs could point to no facts showing Twitter was aware that ISIS was using it to facilitate attacks and continued to provide ISIS its services.[211] This six-step test is directly transferrable to disinformation litigation, for courts to assess the proposed statute's reckless or knowing standard.

The final issues that the Antiterrorism Act dealt with were the remedy, namely collecting foreign assets if a victim succeeds in her suit, and potential executive waivers. The Act eliminated some FSIA restrictions that would have blocked collection from seized state assets, allowed for successful plaintiffs to file superior liens on a defendant's holdings, and enabled plaintiffs to attach many types of proceeds gathered by law enforcement to pay those liens.[212] For state defendants,

---

under the FSIA and Hague Evidence Convention, which requires the involvement of foreign courts and diplomatic offices and are subject to foreign 'blocking statutes' designed to thwart our discovery process. Moreover, foreign states have substantial incentives not to respond to discovery requests seeking information about their involvement in terrorist activities. My amendment therefore requires that when a foreign state fails to respond to a discovery order, the foreign state will be deemed to have admitted the facts to which the discovery order pertains.").

208 Crosby v. Twitter, Inc., 921 F.3d 617, 621 (6th Cir. 2019).

209 *Id.* at 624–26, 627 n.6.

210 Crosby v. Twitter, Inc., 303 F. Supp. 3d 564, 573 (E.D. Mich. 2018) (citing Halberstam v. Welch, 705 F.2d 472, 483–84 (D.C. Cir. 1983)), *aff'd*, 921 F.3d 617 (6th Cir. 2019); *see also* Linde v. Arab Bank, PLC, 882 F.3d 314, 329 (2d Cir. 2018); Copeland v. Twitter, Inc., 352 F. Supp. 3d 965, 975 (N.D. Cal. 2018).

211 *See Crosby*, 303 F. Supp. 3d at 577 ("In this case, although the plaintiffs have alleged that the defendants provided routine social media services to ISIS, they have not pointed to any individual or cognizable entity that the defendants plausibly knew to be facilitating or carrying out any acts of terrorism, and to whom the defendants nevertheless knowingly continued to provide services or support to in any form.").

212 *See* Jack Goldsmith & Ryan Goodman, *U.S. Civil Litigation and International Terrorism* 15–16, 20–21 (Univ. of Chi. Pub. L. & Legal Theory, Working Paper No. 26, 2002), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1364&context=public_law_

the Act expanded the avenues of recovery to include any corporation in which the state or its actors held a majority interest,[213] even if the entity was not itself an agency or instrumentality of the state.[214] Congress further complemented these techniques with powerful civil enforcement tools under the USA Patriot Act.[215] But admittedly, victims found more obstacles than success in asset recovery, and Congress's multiple attempts to overcome those challenges have floundered in court.[216] This primary hurdle has seen pushback from the White House over concerns about encroachment on foreign policy goals. The 2016 revision to the Antiterrorism Act passed, despite Obama's veto for fear of its effect on foreign diplomacy.[217] Congress tried in 2018 to expand the eligible pool of money to which defendants could attach their claims to include funds seized in anti-narcotics enforcement.[218] This time Congress cut out the greatest barrier to defendant recovery, an executive waiver, but immediately felt pressure to put that waiver power back in place for fear that plaintiffs will use the expanded jurisdiction and recovery capabilities against friendly states, or that other states

---

and_legal_theory [https://perma.cc/VRQ3-24JK]; JENNIFER K. ELSEA, CONG. RSCH. SERV., SUITS AGAINST TERRORIST STATES BY VICTIMS OF TERRORISM 50–59 (2008), https://fas.org/sgp/crs/terror/RL31258.pdf [https://perma.cc/2XZN-MZKZ] (discussing new asset recovery tools made available in a 2008 amendment to that ATA).

213 *See* 28 U.S.C. § 1603(b)(2) (2020); Dole Food Co. v. Patrickson, 538 U.S. 468, 474 (2003).

214 *See* ELSEA, *supra* note 212, at 55–57.

215 *See* 18 U.S.C. § 981 (2020). These statutory provisions enable law enforcement to not only seize and forfeit the assets belonging to those individuals who directly plan, participate, and perpetrate terrorism-related crimes, but also allow for the seizure and forfeiture of the assets of those individuals or entities who provide services or launder funds to known terrorist organizations. *See* Sharon Cohen Levin & Carolina A. Fornos, *Using Criminal and Civil Forfeiture to Combat Terrorism and Terrorist Financing*, U.S. ATT'YS' BULL., Sept. 2014, at 42, https://www.justice.gov/sites/default/files/usao/legacy/2014/09/23/usab6205.pdf [https://perma.cc/BSH4-MURV].

216 Despite changes in the 1996 and 2000 amendments, courts often ruled against plaintiffs' attempts to attach funds, citing exclusive presidential power over foreign relations. *See* Sean K. Mangan, *Compensation for "Certain" Victims of Terrorism Under Section 2002 of the Victims of Trafficking and Violence Protection Act of 2000: Individual Payments at an Institutional Cost*, 42 VA. J. INT'L L. 1037, 1038 (2002). Changes in 2016 failed to close these loopholes, still leaving significant opportunity for a presidential override. After threatening to eliminate an executive waiver entirely, Congress ultimately passed the 2016 law with a limitation for such situations by delaying enforcement of successful claims. *See* Vladeck, *supra* note 198; Jennifer Elise Plaster, *Cold Comfort and a Paper Tiger: The (Un)availability of Tort Compensation for Victims of International Terrorism*, 82 WASH. U. L.Q. 533, 543 (2004).

217 The Obama administration asserted that significant foreign relations harms would result aside from any enforcement efforts by, for example, exposing the U.S. government and U.S. officials to suits in other countries or by allowing for discovery against foreign states. *See* Veto Message from the President—S.2040, White House (Sept. 23, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/09/23/veto-message-president-s2040 [https://perma.cc/C2CF-VAK9].

218 *See* Graver & Anderson, *supra* note 195.

might respond—returning to FSIA concerns—by weakening American immunity.[219]

The Antiterrorism Act's executive waiver fight is a useful guide for the disinformation statute, and the White House's pushback over encroachment carries an important lesson: There will be occasions when personal and governmental interests conflict. Concern about foreign policy repercussions cannot be overstated. This law's framers would certainly not take the threat lightly and that pushback deserves consideration here.

America's standing is largely defined by its global interconnectedness. It does business in nearly every country, sends troops and diplomats abroad, builds infrastructure on which other nations rely, and in turn depends on multilateral institutions to responsibly settle disputes.[220] As one prominent scholar on the subject said: "The United States has more to lose than any other country by removing the shield of foreign sovereign immunity . . . ."[221] Critics argue that by allowing suits against foreign actors in U.S. courts, competitor and even friendly nations will respond with a tidal wave of challenges to American conduct in their courts.[222] Instead of resolving disputes diplomatically or through suits brought in the United States, American businessmen engaged in trade could be arrested the moment they exit a plane in any nation with a standing warrant.[223]

---

219 *See* Scott R. Anderson, *Congress Has (Less than) 60 Days to Save Israeli-Palestinian Security Cooperation*, LAWFARE (Dec. 7, 2018, 8:00 AM), https://www.lawfareblog.com/congress-has-less-60-days-save-israeli-palestinian-security-cooperation [https://perma.cc/LCR2-5C2P] (discussing concerns over expanded jurisdiction under the revised ATCA and discussion of new executive waiver).

220 Robert D. Williams & David Dollar, *Don't Count on Suing China for Coronavirus Compensation*, BROOKINGS INST. (May 18, 2020), https://www.brookings.edu/podcast-episode/dont-count-on-suing-china-for-coronavirus-compensation [https://perma.cc/5C4U-VB6P] ("[T]he United States has unrivaled diplomatic, military, economic and scientific research activities around the world. So we stand to lose more from the weakening of the sovereign immunity principle than any other country. Again, sovereign immunity is about reciprocity. It's not a privilege we grant as a favor to other countries.").

221 *The Foreign Sovereign Immunities Act, Coronavirus, and Addressing China's Culpability: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. 1 (2020) [hereinafter Keitner Testimony] (statement of Chimène Keitner, Alfred and Hanna Fromm Professor of International and Comparative Law, UC Hastings Law San Francisco).

222 *See, e.g.*, *Justice Against Sponsors of Terrorism Act: Hearing on H.R. 2040 Before the Subcomm. on the Const. and Civil Just. of the H. Comm. on the Judiciary*, 114th Cong. 45–60 (2016) (statement of Richard D. Klingler, Partner, Sidley Austin LLP).

223 *See* Felix Salmon, *China's Extraterritorial Threat*, AXIOS (July 9, 2020), https://www.axios.com/china-hong-kong-security-law-extraterritorial-9a8609af-83ea-40ff-acfc-674fdbe8ec89.html [https://perma.cc/8G8B-HSXV] ("You won't get arrested so long as you remain outside China and Hong Kong. But for many businesses, that's not an option.").

This recrimination issue garnered renewed attention during the Covid-19 pandemic, when over a dozen parties, including the states of Missouri and Mississippi, sued China's government and communist party for their putative roles in the disease's rise.[224] These claims arose primarily under tort law and were therefore subject to FSIA.[225] To overcome an immunity challenge, they relied on an FSIA exception that nominally waives immunity for foreign commercial activity (if it has a direct effect in the United States).[226] But as practitioners made clear, that exception likely did not apply to the actions in question and thus the claims were bound to fail at immunity's gate.[227] Tapping the public mood, several congressmen in turn proposed new legislation modeled on the Antiterrorism Act, aiming to do exactly what the anti-disinformation law would: create a new FSIA exemption for a specific purpose (pandemic suits).[228] In turn, critics warned of in-kind reprisals by other states and likely violations of international law if U.S. cases proceed.[229]

These attacks should be expected again in the disinformation context, but for at least three reasons, fewer punches will land. First, it is true that unlike terrorism (and more like Covid-related, public health matters),[230] the United States will be more prone to suits in reprisal. Although America does not engage in anything like traditional terrorism, U.S. intelligence agencies do use implicit and explicit

---

224 *See* Keitner Testimony, *supra* note 221, at 11.

225 But at least one suit attempted to evade FSIA constraints by suing under the ATA, claiming that Covid-19 was a secret Chinese biological weapon, and bizarrely seeking twenty trillion dollars in damages. *See, e.g.*, Complaint at 2, 24, Buzz Photos v. People's Republic of China, No. 20-cv-656-K-BN, 2020 WL 6889016 (N.D. Tex. Nov. 24, 2020).

226 *See* 28 U.S.C. § 1605(a)(2) (2020) (creating an immunity exception for "an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States").

227 *See* Williams & Dollar, *supra* note 220 ("The complaint here is that China suppressed information, silenced whistleblowers, failed to notify international organizations in a timely manner, and failed to protect public health in other ways. So the thrust of the activity is basically governmental or regulatory acts and omissions, not commercial activity.").

228 *See, e.g.*, Stop COVID Act of 2020, H.R. 6444, 116th Cong. (2020); Holding the Chinese Communist Party Accountable for Infecting Americans Act of 2020, S. 3662, 116th Cong. (2020).

229 The statutes would violate international law by imposing domestic jurisdiction over other states when American authorities failed to mitigate the pandemic's harm in the first place (for example, with insufficient lockdowns). Hence, the harm would not have been sufficiently intentional to merit a legal violation. *See* Chimène Keitner, *Missouri's Lawsuit Doesn't Abrogate China's Sovereign Immunity*, JUST SEC. (Apr. 22, 2020), https://www.justsecurity.org/69817/missouris-lawsuit-doesnt-abrogate-chinas-sovereign-immunity [https://perma.cc/4VEQ-65NG]; *see also* Keitner Testimony, *supra* note 221, at 7.

230 The White House resisted the Antiterrorism Act by warning that foreign states could pass similar laws to sue U.S. officials. *See* Kenneth Bullock, *United States Tort Liability for War Crimes Abroad: An Assessment and Recommendation*, 58 L. & CONTEMP. PROBS. 139, 147 (1995).

disinformation-style campaigns abroad,[231] and more worryingly, a claim could be made against entirely truthful information sources like the Voice of America.[232] But there is also a reason not to worry; America's disinformation-style efforts are different. As mentioned, at least since the Cold War, America has operated with striking transparency in its electoral and social influence campaigns.[233] American information efforts bend toward supporting global democracy, while competitor states aim to undermine it. While the distinctions might matter less to the competitor states, they do make a difference under international law, where Russia's and China's disinformation attacks violate national sovereignty and non-interference norms, but American efforts broadly comport.[234] America's allies are less likely to express concern for this reason.

Second, unlike with Covid-19 where many of the suits relied on theories of negligence by the Chinese government,[235] the concern in both the terrorism and disinformation contexts is whether the acts are intentional.[236] Because the disinformation law requires an initial, aggressive act by a state actor, it would never allow liability against a foreign government for negligent misstatements. Likewise, foreign governments would be unjustified in criminalizing the sort of dunderheaded but not intentionally harmful statements that U.S. authorities occasionally let loose.

Third, whereas Covid-19 presented worrying scenarios of U.S. litigants attempting to use their claims for extensive legal discovery

---

231 *See* JAMIESON, *supra* note 50, at 10 ("Some may argue that because the United States has a history of insinuating disinformation, deception, and funding into the elections of other countries, including Russia, taking umbrage at the Russian attacks and categorizing them as an act of war are hypocritical.").

232 *See* Bennett, Stemming the Tide, *supra* note 173 ("The word 'message' is a very, very dirty word at the *Voice of America* because that implies that you are deliberately moving your content in order to achieve a particular end.").

233 Geltzer & Sullivan, *supra* note 47.

234 *See* MICHAEL MEYER-RESENDE, DEMOCRACY REPORTING INT'L, A NEW FRONTIER SOCIAL MEDIA / NETWORKS DISINFORMATION AND PUBLIC INTERNATIONAL LAW IN THE CONTEXT OF ELECTION OBSERVATION 11–16 (2018), https://www.intgovforum.org/multilingual/sites/default/files/webform/a-new-frontier_social-media_election-observation_briefing-paper-by-michael-meyer-resende.pdf [https://perma.cc/F8F2-ZTFP] (describing likely international law restrictions on the use of disinformation under the U.N.-adopted International Covenant on Civil and Political Rights and European Convention on Human Rights).

235 *See* Jan Wolfe, *In a First, Missouri Sues China over Coronavirus Economic Losses*, REUTERS (Apr. 21, 2020, 2:17 PM), https://www.reuters.com/article/us-health-coronavirus-china-lawsuit/in-a-first-missouri-sues-china-over-coronavirus-economic-losses-idUSKCN2232US [https://perma.cc/JJ4D-226S].

236 *See* Chimène Keitner, *Don't Bother Suing China for Coronavirus*, JUST SEC. (Apr. 8, 2020), https://www.justsecurity.org/69460/dont-bother-suing-china-for-coronavirus [https://perma.cc/6GVW-7WAA].

against China, the fact-finding demand would be lesser against foreign states in dealing with disinformation, reducing backlash on this front.[237] History has already shown that a surprising amount of evidence has emerged without foreign cooperation, through congressional investigations or public reporting. Moreover, unlike Covid-19 where most of the documentary proof was kept in government annals, reliance on domestic channels for disinformation means that significant proof will be available on U.S. soil.

For each of these reasons, combined with the important point that this law is designed to be used against entirely domestic actors that amplify foreign disinformation more often than states themselves, the actual threat of reprisal by other nations is likely slight.

Despite these distinctions, just as the ATA's framers wrestled with whether to include an executive waiver, there will still be pressure to do so for disinformation. It would be one functional mechanism to allow at least some suits through, while enabling the White House to screen out ones posing foreign repercussions. Two unpleasant factors make granting a waiver unacceptable. First is the similarity in America's influence campaigns abroad with the techniques that foreign nations use in disinformation attacks. Even if these programs can be distinguished in the careful language of diplomatic halls and legal briefs, a White House worried about optics over substance might simply quash suits that look bad to foreign partners. Second, a policymaker might have benefitted from a disinformation attack and would be perversely incentivized to block a suit. It suffices to say of the 2016 election and Trump's controversial relationship with Russian President Putin that executive waiver is a power some White Houses might abuse.[238] The Trump administration was bound to be uncooperative at best. Both factors combined suggest that any President would attempt a waiver more often in the disinformation context, which would neuter the

---

237 *See* Keitner Testimony, *supra* note 221, at 4; *see also* Jen Patja Howell, *The Lawfare Podcast: Taking China to Court over the Coronavirus*, LAWFARE, at 6:45 (July 1, 2020, 5:01 AM), https://www.lawfareblog.com/lawfare-podcast-taking-china-court-over-coronavirus [https://perma.cc/RJP8-BX9Y] (adding that many Covid-19 suits would fail for inability to prove causation and harm, creating a rash of frivolous litigation and discovery claims).

238 *See* JAMIESON, *supra* note 50, at 35 ("Whether the Russian interventions affected votes is more difficult to determine than whether they 'meddled.' Knowing if the effect was significant enough to change the outcome is even more challenging. But what we can know is whether past research indicates that the kinds of messaging that they used and generated are capable of producing sizable enough results to alter a close election.").

statute's effectiveness. Congress has excised the waiver from the Antiterrorism Act. The disinformation statute should never have one.[239]

Recovery through antiterrorism suits has resulted in many failed cases, but plaintiffs have landed important victories as well, and Congress has spent three decades reworking its provisions to ensure even more success. The current framework offers important lessons in the disinformation context: it illustrates the obstacles disinformation framers will face and potential workarounds, and it provides future plaintiffs a map for litigation and solace that there is light at the end of the tunnel.

B. *Defining Disinformation*

Although public figures apply the term "fake news" with many meanings, this statute's provisions define disinformation clearly. Here, it is simply a matter of returning to the definition offered in Part I.[240] Foreign disinformation has: (1) a foreign source; (2) factual mistruth; (3) a detrimental intent and strategic goals associated with the content's generation and initial sharing; and (4) resulting harm when the mistruth is released into the public sphere.[241]

By adopting this definition, the law enables litigants to identify what types of harmful information are targetable. This is not to say that the litigant will easily prove each prong, but the courts will have a fully deployable standard to determine whether the plaintiff's prima facie case is met. For instance, a foreign effort using false information to spark a heated political rally could be actionable. If it comes from abroad, plaintiffs could show it was based on provable mistruth,[242] the goal was to broadly inflame social tensions, and the rally—if it occurred—would likely have inflicted measurable harm. Compare this to a similar act that would not be covered: a local community member

---

239 Still, considering the concern over foreign reprisals, it is important to remember that there are other hurdles and gatekeepers, none more powerful than the judges who hear these cases. To the extent that lawmakers seek to bake discretion into the statute, the logical powerbroker would be the judge. She determines whether a plaintiff's claim is too attenuated to constitute a prima facie case. A judge who recognizes that a suit against China describes actions eerily similar to what Americans are doing, might conclude that the Chinese actions did not rise to reckless, and deny the case on summary judgment. Better this than to let the White House into the mix.

240 *See supra* Section I.A.

241 *See supra* Section I.A.

242 As with defamation, Congress could draft this law such that the initial burden is on the plaintiff to establish mistruth, then the burden shifts to the defendant to rebut and show that the content was verifiable. Rebuttal would be unlikely and effortful for a foreign defendant in this context. *See* Marc A. Franklin & Daniel J. Bussel, *The Plaintiff's Burden in Defamation: Awareness and Falsity*, 25 WM. & MARY L. REV. 825, 859 (1984).

who rallies others to engage in a politically contentious march, but whose political message is untainted by foreign influence, and he has had no contact with foreign-linked actors. Here, the message comes from within the community, under First Amendment protections. Even if the organizer stated mistruths and intended to cause social upheaval, this law would not touch him.[243] These examples show that what appears to be an impossible-to-define category at first, when carefully applying the definition's four prongs, is fully describable.

C. *Appropriate Mens Rea*

The statute's required mens rea is that the defendant acted knowingly or recklessly—no less. Like the standing principle, this test will likely narrow the law's use and direct suits toward the most egregious culprits: presumably foreign entities who create the disinformation or large media and online institutions that have the resources to know the source of their content.[244] The knowing or reckless standard is separate from the underlying requirement that foreign entities created or spread the disinformation with malicious intent and strategic aim. Thus, the mens rea is higher for targeting state actors because disinformation's very definition means showing that the state actors knew they were engaged in disinformation. The lower bar would also be hard to meet for, say, an outspoken American who

---

243 Taking this same community member example and reversing the facts slightly, such that the provocative statements that the organizer was repeating were from a foreign source, and the organizer knew their source and purpose, then again, this law *would* apply. In this variation, the foreign origins prong is met, and plaintiffs could likely overcome the defendant's First Amendment protections. *See infra* Section IV.F (discussing free speech).

244 This culpability standard fits neatly with the approach used in antiterrorism litigation, which showed that a knowing or reckless mens rea can be proven even without a smoking gun. *See, e.g.*, *In re* Terrorist Attacks on Sept. 11, 2001, 718 F. Supp. 2d 456, 489 (S.D.N.Y. 2010) ("The claimed wrongdoing of [Dubai Islamic Bank (DIB)] . . . does not relate to the performance of routine banking and financial services, or its use as a passive conduit through which monies were indirectly channeled to and from al Qaeda. Rather, the allegations indicate that DIB was an intentional, knowing and direct participant in providing money laundering services to al Qaeda, which allowed for direct funding of terrorist attacks. . . . DIB allegedly continued to provide banking and other financial services directly to Osama bin Laden and al Qaeda, in violation of accepted international banking standards adopted to prevent the illicit movement of funds to terrorists."), *aff'd on other grounds*, 714 F.3d 109 (2d Cir. 2013); *see also* Gill v. Arab Bank, PLC, 893 F. Supp. 2d 474, 486 (E.D.N.Y. 2012) ("The Bank beginning in the late 1990s knowingly maintained accounts for—and accepted wire transfers on behalf of—Hamas (or its proxies), well-known Hamas leaders, and other Hamas operatives, despite the facts that (1) Hamas was named as a beneficiary of wire transfers made, (2) the United States government determined that some individual account holders to whom transfers were made were Hamas-affiliated terrorists, and (3) some account holders to whom transfers were made were prominent members of the paramilitary side of Hamas.").

retweets dozens of foreign disinformation memes.[245] The plaintiffs would have to show that the retweeter was exposed to enough readily available reporting on the mistruth and foreign origins of those claims that he acted recklessly. As such, a person exercising reasonable care could not run afoul of the law through inattention.

Further assuring that this law is not abused, the plaintiff would have to prove the defendant's sufficient intent on all of the law's first three definitional prongs (the fourth prong, causing harm, would not be relevant at the intent phase). For example, in a suit against the serial retweeter, the plaintiff would have to show that the defendant knew or should have known that she was repeating false information (prong two), it originated from a foreign source (prong one), and that the foreign source intended strategic disruption (prong three).

A related, practical point is that a defined mens rea might result in a varying actus reus for future cases, as education about disinformation shifts. If technology enables automatic warning flags on dubious memes or questionable sources,[246] for instance, that which constitutes knowing amplification might change based on whether such a warning was issued and received. This law could naturally conform to society's changing norms.

There is a valid argument that far from reasonably limiting abuse, this burden actually makes pleading impossible—that it would require a smoking gun showing that the defendant considered that it was disinformation and acted anyway. If the framers agree with this concern, though it seems a misreading of the law, they might choose an alternative mens rea that borrows from defamation. Traditional defamation has a different intent standard depending on whether the defamatory statement involved a matter of public or private interest. If public, the defendant must have acted with malice or reckless disregard,[247] but if it is private, a defendant negligently failing to ascertain the mistruth is sufficient.[248] As to disinformation, this could mean a person might face liability if he failed to check the truth and

---

245 In the typology of actors, the serial retweeter would be an amplifier.

246 *See, e.g.*, Federico Guerrini, *Fake News: Could a New Online Rating System Help Fight Misinformation?*, FORBES (July 10, 2018, 2:01 PM), https://www.forbes.com/sites/federicoguerrini/2018/07/10/fake-news-could-a-new-online-rating-system-help-fight-misinformation/#5f7347ec66d6 [https://perma.cc/T3GW-2BW6] (describing, among other tools, Newsguard—a consumer-level AI technology that rates a website's trustworthiness automatically based on crowdsourced and curated data).

247 *See* RESTATEMENT (SECOND) OF TORTS § 580A (AM. L. INST. 1977); *see also* Gertz v. Robert Welch, Inc., 418 U.S. 323, 334 (1974) ("The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice' . . . .").

248 *See* RESTATEMENT (SECOND) OF TORTS § 580B.

origin of every statement before he posts it. This seems implausible in practice. Moreover, the reckless requirement described above is an achievable pleading standard. It is the right standard to apply in this law.

Setting the required mens rea at knowing or reckless compels a tougher question: whether news providers should receive more protection than others. It is well recognized that the press is a unique institution under the First Amendment,[249] but there is little case law interpreting what protections the free press clause actually adds.[250] With a few exceptions, the "protections offered to the institutional media have long been . . . no greater than those offered to others."[251] One consequence of this law is that news institutions might become obvious defendants. Plaintiffs would likely file claims against tech platforms, publications, or individual reporters, and some plaintiffs might have suffered no injury, but instead, be maliciously using the statute to hurt the press. This threat is magnified by already-existing public skepticism toward journalists.[252] With this in mind, holding a journalist or publisher to even a knowing standard could arguably be too low to avoid the risks. Perhaps the law should require a heightened, intentional mens rea specifically for the press.

In considering this risk, on one hand, journalists' greater vulnerability is balanced by greater resources and know-how in confirming information's source. Not only do journalists typically have the facilities and training to double-check a story's accuracy, they typically have an ethical duty to so.[253] Worryingly, creating a carveout for journalists overlooks the ease with which bad actors might take

---

249 The Constitution's free press clause states, "Congress shall make no law . . . abridging the freedom . . . of the press." U.S. CONST. amend. I, cl. 2.

250 The few speech-related protections unique to the press include: (1) near immunity in a libel context; (2) some protection for "reporters' claims that they had a constitutional privilege not to disclose their confidential news sources to a grand jury"; and (3) strong protections from government interference, be it from compulsion to publish certain stories, or prohibitions on publishing certain stories. Potter Stewart, *"Or of the Press,"* 26 HASTINGS L.J. 631, 635–36 (1975).

251 Eugene Volokh, *Freedom for the Press as an Industry, or for the Press as a Technology? From the Framing to Today*, 160 U. PA. L. REV. 459, 465 (2012).

252 *See* AMY MITCHELL, JEFFREY GOTTFRIED, GALEN STOCKING, MASON WALKER & SOPHIA FEDELI, PEW RSCH. CTR., MANY AMERICANS SAY MADE-UP NEWS IS A CRITICAL PROBLEM THAT NEEDS TO BE FIXED 6 (2019), https://www.journalism.org/wp-content/uploads/sites/8/2019/06/PJ_2019.06.05_Misinformation_FINAL-1.pdf [https://perma.cc/N2VR-HJX6] (noting a disproportionate percentage of registered Republicans expressing the most mistrust, creating partisan reasons to misuse this law because "[a] solid majority of Republicans and Republican-leaning independents (62%) say made-up news is a very big problem in the country today, compared with fewer than half of Democrats and Democratic-leaning independents (40%)").

253 SOC'Y PRO. JOURNALISTS, SPJ CODE OF ETHICS (2014), https://www.spj.org/ethicscode.asp [https://perma.cc/82RJ-3DQ3] ("Take responsibility for the accuracy of their work. Verify information before releasing it. Use original sources whenever possible.").

refuge in falsely proclaiming themselves press. A significant technique already present in foreign disinformation attacks is the creation of false news sites.[254] Requiring different treatment for the press would necessarily force the court into the dangerous territory of interpreting what journalism is.[255]

On the other hand, most journalists are required to work at breakneck speed.[256] The traditional factchecking expectations are not as strong as they once were,[257] and moreover, for freelance journalists lack the financial wherewithal to meet the same standards as, say, *The New York Times*.[258] There is also a theme in free press clause interpretation, in cases like *Gertz v. Robert Welch, Inc.*[259] and *New York Times Co. v. Sullivan*,[260] that seeks to grant journalists First Amendment "breathing space," creating the freedom reporters need to make occasional mistakes in order to adequately inform the public.[261]

The balance of these concerns is a delicate one, but it lays gently against heightened protections for journalists. As for breathing space, however true that claim is in broad strokes, that argument has limits. A judge might certainly weigh the media's value to society when exercising her discretion over a journalist's culpability as a defendant, but as Justice White once wrote, "Nothing in the central rationale

---

254 *See generally* Richard Fletcher, Alessio Cornia, Lucas Graves & Rasmus Kleis Nielsen, *Measuring the Reach of "Fake News" and Online Disinformation in Europe*, REUTERS INST., https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe [https://perma.cc/3RC6-W5CM] (recognizing and measuring the impact of fake news sites in France and Italy).

255 *See* David Abramowicz, *Calculating the Public Interest in Protecting Journalists' Confidential Sources*, 108 COLUM. L. REV. 1949, 1953–54 (2008) (discussing the difficulty of distinguishing journalists for legal purposes).

256 *See* Phyllis Furman, *Racing Against the Clock in the Newsroom, Then and Now*, SJR, https://www.groupsjr.com/racing-against-the-clock-in-the-newsroom-then-and-now [https://perma.cc/5825-2J22].

257 *See* Stephanie Fairyington, *In the Era of Fake News, Where Have All the Fact-Checkers Gone?*, COLUM. JOURNALISM REV. (Feb. 23, 2018), https://www.cjr.org/business_of_news/fact-checking.php [https://perma.cc/K49S-U8RX].

258 *See* Alec MacGillis, *The Hard Truth About Fact-Checking*, NEW REPUBLIC (Dec. 20, 2011), https://newrepublic.com/article/98760/the-hard-truth-about-fact-checking [https://perma.cc/5AC2-Z4U7] (describing journalists outsourcing fact-checking responsibilities).

259 *See* 418 U.S. 323, 342 (1974) ("[W]e have been especially anxious to assure to the freedoms of speech and press that 'breathing space' essential to their fruitful exercise.").

260 *See* 376 U.S. 254, 271–72 (1964) (also referring to breathing space).

261 *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 770 (1985) (White, J., concurring) (noting, without agreeing to the breathing space argument, that "[t]he press must therefore be privileged to spread false information, even though that information has negative First Amendment value and is severely damaging to reputation, in order to encourage the full flow of the truth, which otherwise might be withheld").

behind *New York Times* demands an absolute immunity from suits."[262] Moreover, the reckless mens rea is not an incredible burden. It is hard to imagine a reporter who does her job faithfully would not make some minimal effort to support an article's claims with facts. One could not fairly say that a journalist who confirms a typical quote once, but does not double or triple check it, always acts recklessly. Most professional or aspiring journalists would never need the protection that an intentional mens rea would afford.

But the greatest factor weighing against a heightened intent standard is how enemies might abuse it. While courts might mistake some upstart and legitimate news sites as propaganda, the greater danger is in attackers hiding behind the journalistic veil of established sources. Consider the tough cases of defining official state news entities like RT and China Daily. It would not be hard for such firms to use a heightened mens rea to shield their malicious acts. After all, it was a mainstream Russian news source, Russia One, that was responsible for the Lisa case—the false story about immigrant gang rapists in Germany.[263] For all these reasons, it seems prudent to avoid a special protection for journalists at the outset. Still, it is also fair that wise judges, acting on their discretion, would exercise stricter scrutiny in hearing a suit against CNN, for instance, versus one against a one-week-old website written in broken English.

D. *Establishing Standing and Causation*

What must the plaintiff do to meet her burdens on standing and causation? Does a plaintiff have standing by reading one article later exposed as propaganda? Can a reader who changed his presidential vote based on a series of false articles prove that those articles were the proximate cause of some harm?

For standing, the required level of injury is set in traditional Article III jurisprudence: the probabilistic test from *Lujan v. Defenders of Wildlife*.[264] "First, the plaintiff must have suffered an 'injury in fact,'—

---

262 *Id.* at 772. Justice White also noted that "breathing room for speakers can be ensured by limitations on recoverable damages; it does not also require depriving many public figures of any room to vindicate their reputations sullied by false statements of fact." *Id.* at 771.

263 *See supra* Introduction.

264 504 U.S. 555 (1992). The plaintiffs in *Lujan*, unlike ones making a claim under the proposed disinformation law, were seeking declaratory and injunctive relief. *See id.* at 559. In this sense, once they showed enough injury for standing, they would not need to show further harm to calculate damages. That makes this case simpler than a disinformation claim, in which a plaintiff who entered court based on a minimal injury would then still have to show the court

an invasion of a legally protected interest which is (a) concrete and particularized and (b) 'actual or imminent, not "conjectural" or "hypothetical."'"[265] Second, there must be a causal link between the injury and the disputed conduct—that is, the injury must be fairly traceable to the defendant's conduct and not the result of independent action by some third party. Third, the cited harm must be "likely," not "speculative." And fourth the injury must be "redress[able] by a favorable decision."[266]

In *Lujan*, plaintiffs did not establish standing because they could not prove imminent injury; environmental organizations whose members once traveled to and hoped to return to environmentally threatened areas were not injured by the United States withdrawing ecological funding in those areas.[267] The plaintiffs also failed to show redressability because the U.S. agencies that they sued provided less than ten percent of the foreign funding, there was nothing to indicate that the projects would be suspended without the money, and there was no indication that endangered species would be further harmed.[268] In the same Sixth Circuit case that dealt with mens rea above, *Crosby v. Twitter, Inc.*, the court applied a similar standing test in the terrorism context, and held that plaintiffs had not established standing at pleading because they had not offered enough facts on the causation prong to show that the attack was fairly traceable to Twitter's conduct.[269] Merely hosting provocative ISIS content on its platform was not enough.

One can see how the standing requirement might play out with the hypothetical disinformation-fueled rally in Section IV.B. First, the plaintiff would have to show an actual injury: anguish from merely watching the rally on TV is not enough, but attending and being injured, or if foreign agents coopted her into using her business services to support the rally, that would be enough. Second, the plaintiff would have to show that the disinformation was a proximate cause of the rally

how it could remedy her harm through a money reward. Questions of remedy, such as this, in some instances permit a court to dispose of a suit at the pleading stage if damages appear too speculative. *See, e.g.*, Harold H. Huggins Realty, Inc. v. FNC, Inc., 634 F.3d 787, 796–97 (5th Cir. 2011) (stating Lanham Act's five-factor prudential standing test in trademark violation cases). While setting damages is inarguably more complicated for disinformation claims, it is achievable. This Article addresses damages below. *See infra* Section IV.E.

265 *Lujan*, 504 U.S. at 560 (citations omitted).

266 *Id.* at 560–61 (citations omitted).

267 *See id.* at 563–64.

268 *See id.* at 571.

269 *See* 921 F.3d 617, 625 (6th Cir. 2019) ("Defendants do not proximately cause everything that an individual may do after viewing this endless content. Nor can Defendants foresee how every viewer will react to third party content on their platforms. This is especially true where independent criminal acts . . . are involved." (footnote omitted)).

taking place. Third, she must provide evidence of her physical or reputational damages; affidavits and receipts could do that. Finally, she must show that those injuries are redressable through money damages—a prong that will be consistently easy to meet under this statute because the very purpose of a money suit is to provide material redress.

As to causation, the statute borrows its standard from defamation law. The disinformation plaintiff, like in a defamation case, must show that the defendant's actions were a "substantial factor" in the resulting harm, but those actions need not be the sole cause.[270] By further incorporating a pure comparative negligence standard into this law, a plaintiff's contributory negligence or mistakes by other parties could not serve as a complete defense.[271] The factfinder would have to analyze the circumstances and decide what percentage of responsibility the defendant or others bear, and what amount falls onto the plaintiff themselves.[272] The plaintiff's own liability would not defeat liability, but if high enough, it might reduce causation so much that the judge would find it insubstantial enough to proceed beyond pleading. The adoption of a comparative negligence rule is likely essential if the law is to have any real-world effect. Since 2016, foreign disinformation purveyors have increasingly comingled their product with domestic actors, to hide their role and to magnify the legitimacy of their message.[273] More recent efforts have involved foreign states coopting local activists into posting the unfounded messages, or foreign actors directly supporting existing

---

270 *See* RESTATEMENT (SECOND) OF TORTS § 622A (AM. L. INST. 1977); *see also* Joseph v. Scranton Times, L.P., 89 A.3d 251, 267 (Pa. Super. Ct. 2014) ("The finding that there were other causes for the damage to Appellants' reputations certainly impacts the quantity of the damages for which Appellees are liable; however, that does not negate liability.").

271 *See* RESTATEMENT (SECOND) OF TORTS § 465 (AM. L. INST. 1965) ("The plaintiff's negligence is a legally contributing cause of his harm if, but only if, it is a substantial factor in bringing about his harm and there is no rule restricting his responsibility for it."); *id.* § 495 ("A plaintiff is barred from recovery if the negligence of a third person is a legally contributing cause of his harm, and the plaintiff has been negligent in failing to control the conduct of such person.").

272 *See id.* § 467 ("In several states general statutes applicable to all negligence actions, and in a great many others particular statutes applicable to certain types of cases . . . reduction of the damages to be recovered by the negligent plaintiff [occurs] in proportion to his fault.").

273 *See* Anne Applebaum, *The Science of Making Americans Hurt Their Own Country*, ATLANTIC (Mar. 19, 2021), https://www.theatlantic.com/ideas/archive/2021/03/russia-studied-how-get-americans-make-mistakes/618328 [https://perma.cc/EK3Y-8G5R]; *see, e.g.*, Julian E. Barnes, *Russian Disinformation Targets Vaccines and the Biden Administration*, N.Y. TIMES (Oct. 18, 2021), https://www.nytimes.com/2021/08/05/us/politics/covid-vaccines-russian-disinformation.html [https://perma.cc/847Z-23W9] (discussing foreign disinformation about Covid-19 vaccines spread on conservative websites).

extremists to promote homegrown societal division.[274] Contemporary disinformation campaigns, to abuse a phrase, often take a village.[275]

Imagine the causation prong in practice. An average voter exposed to a multitude of disinformation who claimed she therefore chose a candidate that she might not otherwise have preferred would likely be unable to muster the necessary evidence to tie her vote substantially to one defendant. Contrast this with a voter who claimed that a single, foreign-funded, local troll posted false information about polling sites on election day, leading to long lines and ultimately disenfranchising her. Here, even if other people reposted the false message and the voter could have waited longer in line, evidence like news reports and her employer's strict late-attendance policy would likely be enough to meet the substantial factor test. On the far end, although the comparative negligence calculation would be exceedingly hard, it seems Hillary Clinton would also have a plausible shot at proving causation in her 2016 run based on available evidence: the Senate Russia report, news reports, and polls showing the effect of disinformation on voters.

E. *Assessing Damages*

The challenge of assessing damages is two-fold: first, measuring the types of harm that disinformation might cause; and second, determining an appropriate remedy for that harm.

First, when measuring disinformation's harm, antiterrorism suits unfortunately offer less guidance.[276] Unlike a terrorist attack, disinformation cannot sever limbs. Disinformation's worst material harm would likely be financial. Otherwise, a court must look to nonmaterial harm. This proposed statute allows plaintiffs to plead both

---

274 *See* Nina Jankowicz, *How an Anti-Trump Flash Mob Found Itself in the Middle of Russian Meddling*, POLITICO (July 5, 2020, 7:00 AM), https://www.politico.com/news/magazine/2020/07/05/how-an-anti-trump-flash-mob-found-itself-in-the-middle-of-russian-meddling-348729 [https://perma.cc/QB8Z-NV56] ("Rather than simply creating fake accounts, Russian operatives are also infiltrating authentic activism and using American voices to turn us against one another."); Kevin Roose, Sheera Frenkel & Nicole Perlroth, *Tech Giants Prepared for 2016-Style Meddling. But the Threat Has Changed*, N.Y. TIMES (Sept. 22, 2020), https://nyti.ms/3dBfky5 [https://perma.cc/H3CQ-4V4Z] ("In one Facebook influence campaign in Africa last year, the Russian group appeared to pay locals to attend rallies and write favorable articles about its preferred candidates.").

275 *See generally* HILLARY RODHAM CLINTON, IT TAKES A VILLAGE AND OTHER LESSONS CHILDREN TEACH US (1996) (employing the phrase "it takes a village").

276 The Antiterrorism Act allows civil penalties by "[a]ny national of the United States injured in his or her person, property, or business by reason of an act of international terrorism." Wultz v. Islamic Republic of Iran, 755 F. Supp. 2d 1, 41 (D.D.C. 2010) (citing 18 U.S.C. § 2333(a) (2020)).

types. As a concrete example, take the Lisa case, in which Russian disinformation compelled Germans to protest the local police.[277] Under the anti-disinformation statute, shop owners at the protest site could have argued financial harm by showing diminished receipts that day and testimony from repeat shoppers who said that the protests kept them away. The city could prove harm by showing overtime expenses for police assigned to the protest. The police chief could have offered evidence of time and money he spent to publicly defend himself against false accusations. Each of these injuries would be measurable.

Plaintiffs could also make nonmaterial claims. Here, plaintiffs could draw lessons from other torts, such as defamation and similar privacy invasions.[278] In those cases, plaintiffs may offer evidence of reputational harm,[279] public exposure,[280] and mental anguish.[281] For example, a plaintiff seeking damages for slander might testify and offer witnesses to corroborate how the statements affected him emotionally, turned the community against him, fueled backlash at work, and caused physical angst.[282] To put this in a disinformation context, consider the political response to the 2020 George Floyd killing and subsequent protests in which some conservative activists sought to paint the Black Lives Matter movement as violent.[283] Russian and Chinese disinformation trolls contributed to that one-sided portrayal.[284] Members of actually peaceful groups accused of violence might show

---

277 *See* Rutenberg, *supra* note 16.

278 *See* Stanley Ingber, *Rethinking Intangible Injuries: A Focus on Remedy*, 73 CALIF. L. REV. 772, 827–32 (1985) (discussing contemporary judicial approach in defamation law to determine remedy).

279 *See* Rosenblatt v. Baer, 383 U.S. 75, 92 (1966) (Stewart, J., concurring).

280 *See* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1003 (1964) ("The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity."). *See generally* Roe v. Wade, 410 U.S. 113 (1973); Griswold v. Connecticut, 381 U.S. 479 (1965).

281 *See, e.g.*, Time, Inc. v. Firestone, 424 U.S. 448, 460–61 (1976); Gertz v. Robert Welch, Inc., 418 U.S. 323, 350 (1974).

282 *See, e.g.*, Williams v. First Advantage LNS Screening Sols., Inc., 238 F. Supp. 3d 1333, 1350 (N.D. Fla. 2017) (finding slander plaintiff who sought compensatory damages from a credit agency that provided incorrect reports to two prospective employers provided sufficient evidence based on his and his mother's testimony that he was highly upset about the prospects of future employment because of the erroneous reports, and he suffered physical distress such as insomnia, headaches, and dyspepsia).

283 *See* Kevin Liptak, *Trump Stokes Tensions over George Floyd Protests Before Calling for Calm*, CNN (May 29, 2020, 11:10 AM), https://www.cnn.com/2020/05/29/politics/donald-trump-george-floyd-protests/index.html [https://perma.cc/JQ7E-TBM3].

284 *See* Mark Scott, *Russia and China Target U.S. Protests on Social Media*, POLITICO (June 1, 2020, 4:12 PM), https://www.politico.com/news/2020/06/01/russia-and-china-target-us-protests-on-social-media-294315 [https://perma.cc/6KBP-4NZR].

reputational harm attributable to the disinformation with documentation of their opponents' tweets, for instance, reposting and spreading those disinformation claims.[285]

The second issue then is the appropriate penalty: how to assign a dollar value to the harm. This statute aims to deter frivolous lawsuits by setting fair damage limits. Tort law offers a menu of possible ways to calculate loss. It is helpful here to divide the harm from disinformation into primary and secondary costs.[286] The primary costs are the result of the direct injury, which for disinformation might be financial harm from business losses, data breach, or property damage (if the disinformation results in other parties taking physical action). Courts normally remedy these costs through compensatory damages. Measuring these costs are straightforward using financial statements, receipts, etc. Secondary costs include the nonmaterial harms cited above, such as reputational and emotional, which are necessarily harder to measure. Courts compensate these costs with punitive damages. Punitive damages that far exceed compensatory grew controversial and prompted a tort reform backlash in the 1990s.[287] And yet, in 2008, as Congress further expanded anti-terrorism protections, it amended the FSIA statutes to expressly allow punitive damages.[288] Judges and juries typically calculate punitive damages in one of five ways,[289] but in lieu of exploring the options in depth, it suffices to note which technique the Antiterrorism Act uses: a multiple of compensatory damages and, specifically, treble damages.[290] Therefore, whatever primary costs the

285 In such instances, this proposed statute benefits the plaintiff beyond actual defamation by overcoming FSIA constraints, allowing suits against the foreign disinformation creator rather than the domestic amplifier.

286 *See* Steven R. Salbu, *Developing Rational Punitive Damages Policies: Beyond the Constitution*, 49 FLA. L. REV. 247, 272 (1997) (describing the primary and secondary costs distinction as applied in other tort claims).

287 *See* Michael Rustad & Thomas Koenig, *The Historical Continuity of Punitive Damages Awards: Reforming the Tort Reformers*, 42 AM. U. L. REV. 1269, 1275–76 (1993); George L. Priest, *Lawyers, Liability, and Law Reform: Effects on American Economic Growth and Trade Competitiveness*, 71 DENV. U. L. REV. 115, 115 (1993) (the threat of civil penalties imposes a tax on U.S. companies that impairs their global competitiveness).

288 *See* National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-81, § 1083(a)(1), 122 Stat. 3 (2008). Previously, only compensatory damages were available. Congress amended FSIA to authorize certain plaintiffs to pursue a federal cause of action "for personal injury or death caused by" extrajudicial killing and to recover "economic damages, solatium, pain and suffering, and punitive damages." 28 U.S.C. § 1605A(c) (2020).

289 The five ways to measure punitive damages are: (1) to reflect the seriousness of the infraction; (2) to supplement inadequate compensatory damages; (3) to reflect the defendant's financial need; (4) as a multiple of compensatory damages; and (5) subject to the statutory caps. Salbu, *supra* note 286, at 281.

290 18 U.S.C.A. § 2333(a) (stating that the victims or family members "shall recover threefold the damages he or she sustains and the cost of the suit").

plaintiff proves, for which the court would award compensatory damages, the court may add three times as much as an additional punitive remedy.

The proposed disinformation law aims for a damages amount sufficient to create an effective deterrent and to remunerate the victim without enabling unfair windfalls prompting false suits. Accordingly, at the outset, it uses a maximum award of treble punitive damages plus compensatory. That amount has proven broadly effective in balancing the motivation and costs to parties in antiterrorism suits.[291] One might criticize the analogy here because the direct costs from most terrorist attacks are far greater than in a disinformation claim. But the lesser relative harm and, therefore, punishment in this context is expressly the purpose of treble damages: if disinformation hurts less, any given claim should impose less liability. Limiting damages also discourages misuse of this statute. Finally, because disinformation's harm can be widespread, even though any one lawsuit might not impose great costs, the bulk of suits or a class action might have the same effect on the defendants and better spread the wealth to persons harmed.[292]

F. *First Amendment Considerations*

The proposed statute defies the biggest challenge to regulating disinformation: First Amendment conflicts. In fact, it overcomes two hurdles: malicious actors misusing it as a weapon against legitimate speech and culpable defendants claiming free speech as a valid defense.

First, as to avoiding misuse, this statute demands a pleading standard high enough that it would deter frivolous suits against speech that plaintiffs merely dislike. As already described, the required mens rea, causation, and harm showings will largely constrain this statute's use to its designed purpose. It is true that incidents of misuse remain possible, even inevitable, but what stands in favor of this law is that the First Amendment harms from other disinformation solutions are worse. This statute does not impose blanket bans on certain types of speech or create opaque standards for acceptable speech by social media

---

[291] *See* Pugh v. Socialist People's Libyan Arab Jamahiriya, 530 F. Supp. 2d 216, 265, 274 (D.D.C. 2008) (assigning compensatory damages to victims of Flight 772 bombing in § 2333 claim); Melanie Kirkpatrick, *Terror's Tailwind*, WALL ST. J. (July 2, 2017, 5:00 PM), https://www.wsj.com/articles/terrors-tailwind-1499029226 [https://perma.cc/XH4M-FRMH] (noting that Libya, "in 2009, paid $1.5 billion to the U.S. Treasury to compensate all victims of Libyan acts of terrorism" and the "Flight 772 families each received about $10 million").

[292] *See* Ingber, *supra* note 278, at 775 (arguing that a properly constructed damages remedy functions like "social insurance [and] would accomplish such a compensation goal much more efficiently than the present tort system").

platforms' self-appointed boards. It checks the process through the adversarial process and oversight by judges. If anything, the valid criticism against this proposal is that it is too onerous. It could leave much disinformation unchecked. But as the Supreme Court has said, "[E]rroneous statement is inevitable in free debate, and . . . it must be protected if the freedoms of expression are . . . to 'survive.'"[293]

Second, this statute would survive a defendant's First Amendment challenge. Even though First Amendment exceptions are narrow,[294] two factors in the law—the requirement for a foreign source and the foreign actor's malicious intent—ensure that plaintiffs can succeed: foreign defendants would lack First Amendment protection entirely, and speech with malicious intent might be so likely to incite unrest or violence that silencing it would survive a court's heightened scrutiny. Here, a different line of antiterrorism legislation again provides a useful roadmap: material support.[295] Litigation around that law reveals the First Amendment exception into which disinformation rightfully falls.[296] Even where a court applies heightened scrutiny, proven disinformation will likely be unprotected.[297]

Material support for terrorism is prohibited under 18 U.S.C. § 2339A and § 2339B. The Court has litigated its First Amendment concerns in *Holder v. Humanitarian Law Project* (*HLP*) and its subsequent line of cases.[298] The issue in *HLP* was whether mere speech, advocacy for a terrorist group's goals, can be fungible and constitute material benefit to the terrorists. Importantly, the Court decided that

---

293 New York Times Co. v. Sullivan, 376 U.S. 254, 271–72 (1964) (quoting NAACP v. Button, 371 U.S. 415, 433 (1963)).

294 *See supra* Section II.B (discussing the First Amendment challenges to countering disinformation).

295 *See* 18 U.S.C.A. § 2339B (2020).

296 *See* Holder v. Humanitarian L. Project, 561 U.S. 1, 39 (2010). The Court, of course, has interpreted the First Amendment to extend even to speech advocating illegal conduct. *See* Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

297 *See* Ashcroft v. Free Speech Coal., 535 U.S. 234, 237 (2002). Case law suggests that the imminence required under *Brandenburg* is a stringent standard for offenses involving "advocacy." *See, e.g.*, *id.* at 236 ("[T]he mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it, absent some showing of a direct connection between the speech and imminent illegal conduct." (citations omitted)).

298 561 U.S. 1, 26 (2010) ("Congress has not . . . sought to suppress ideas or opinions in the form of 'pure political speech.' Rather, Congress has prohibited 'material support,' which most often does not take the form of speech at all. And when it does, the statute is carefully drawn to cover only a narrow category of speech to, under the direction of, or in coordination with foreign groups that the speaker knows to be terrorist organizations."); *see also* United States v. Ghayth, 709 F. App'x 718, 723–24 (2d Cir. 2017) ("Far from 'pure speech,' Abu Ghayth's words provided material support to Al Qaeda by spreading its message to the world and encouraging others to join its terrorist cause."), *cert. denied*, 138 S. Ct. 1450 (2018).

the issue was speech itself and not otherwise prohibited conduct.[299] In *HLP*, the plaintiffs provided legal advice and other types of expertise in support of allegedly lawful activities of two designated terrorist groups. The Court found that in applying § 2339B, a "demanding standard" of scrutiny should apply.[300] While the Court did not define what it meant by "demanding," it placed that measure somewhere between the intermediate and strict scrutiny tests.[301] And in analyzing the support that the plaintiffs provided the groups—training in use of humanitarian and international law, as well as political advocacy—the Court held that by even indirectly empowering terrorists to commit more crimes, the plaintiffs were conferring a measurable, illegal contribution.[302] In other words, even with mere speech, plaintiffs were furthering illegal terrorist conduct. And though this material support statute was a content-based restriction, legitimate government interests outweighed the harm of imposing restrictions in this instance.

Turning to the disinformation statute, two conditions would defeat a defendant's First Amendment argument. First, if the defendant were a foreign state actor, the target would likely have no First Amendment protection. "The Bill of Rights is a futile authority for the alien seeking admission for the first time to these shores."[303] First Amendment protections do not extend to foreign actors if they are speaking into America from abroad or have entered illegally and are deportable.[304] The First Amendment also offers no refuge for noncitizens interfering in core civic functions like elections.[305] And U.S. citizens have only a

---

299 *See HLP*, 561 U.S. at 27–28. "The material support law now stands alone as the only content-based measure upheld by a majority of the Supreme Court." Zick, *supra* note 162, at 942.

300 *HLP*, 561 U.S. at 28.

301 *See id.* at 27–28.

302 *See id.* at 39.

> Given the sensitive interests in national security and foreign affairs at stake, the political branches have adequately substantiated their determination that, to serve the Government's interest in preventing terrorism, it was necessary to prohibit providing material support in the form of training, expert advice, personnel, and services to foreign terrorist groups, even if the supporters meant to promote only the groups' nonviolent ends.

Id. at 36.

303 Kwong Hai Chew v. Colding, 344 U.S. 590, 596 n.5 (1953) (quoting Bridges v. Wixon, 326 U.S. 135, 161 (1945) (Murphy, J. concurring)) (recognizing that the First Amendment does not apply to a noncitizen outside of the United States).

304 *See, e.g.*, *id.*

305 Courts have approved legal restrictions on political contributions (a form of expression) by people who are not citizens or permanent residents, which would include individuals in America on temporary work, student, tourist, or other nonimmigrant visas. *See* 52 U.S.C. § 30121 (2020); Bluman v. Fed. Election Comm'n, 800 F. Supp. 2d 281, 288 (D.D.C. 2011), *aff'd*, 565 U.S.

limited First Amendment right to receive and distribute foreign materials inside the United States.[306] A plaintiff without any constitutional barrier could use this law to sue a foreign speaker, be it a state or state subsidiary. That leaves one set of likely defendants unprotected.

Second, if a plaintiff instead sued a U.S. resident under this statute, an American amplifier for instance, the statute's factual mistruth and malicious intent prongs would still enable it to survive a court's scrutiny. In that scenario, depending on the facts, the speech would either be entirely unprotected, or regulatable subject to heightened scrutiny.[307]

The speech might be entirely unprotected because the factual mistruth prong will often place the defendant's actions in the same category as defamatory statements. There, the speaker lacks First Amendment protection if he acted with actual malice, meaning "knowledge that [the statement] was false or with reckless disregard of whether it was false or not."[308] Actual malice can be a hard standard to prove and perhaps more so in the disinformation context. In one slander case, the South Carolina Supreme Court held that a police chief had not shown a reporter's actual malice in publishing an opinion column that said the chief took bribes, even though the chief alleged that the reporter failed to investigate the source of an anonymous call that sparked the story and the reporter had expressed ill will toward the police chief.[309] In contrast, the Virginia Supreme Court held that a TV station had shown actual malice by airing a report accusing a doctor of sexual assault, because the TV station knew that a source had retracted one of the statements on which the story was based, and the medical board had cleared the doctor of accusations.[310] For disinformation, to meet the actual malice standard, if the defendant were a public figure who used disinformation to tar the plaintiff, for instance, that plaintiff

1104 (2012). The government may also deny citizens' access to foreign speakers on U.S. soil for any "facially legitimate and bona fide reason" under its immigration power. *See* Kleindienst v. Mandel, 408 U.S. 753, 770 (1972).

306 *See, e.g.*, Meese v. Keene, 481 U.S. 465, 480 (1987) (permitting limits on distribution of foreign political propaganda).

307 The government in *HLP* mentioned but did not fully brief the argument that the speech in that case should have been wholly unprotected under one of the theories in this paragraph, for instance, seditious conspiracy. The Court, as a result, did not rule on that question. *See* 561 U.S. at 27 n.5.

308 New York Times Co. v. Sullivan, 376 U.S. 254, 280 (1964). The actual malice protection applies only for statements about public figures or private figures involving matters of public interest if the latter person is seeking punitive damages. Otherwise, negligent mistruth is sufficient. *See, e.g.*, Phila. Newspapers, Inc. v. Hepps, 475 U.S. 767, 770 (1986).

309 *See* Elder v. Gaffney Ledger, 533 S.E.2d 899, 904–05 (S.C. 2000).

310 *See* WJLA-TV v. Levin, 564 S.E.2d 383, 392 (Va. 2002).

would need to show more than recklessness on the defendant's part; she must show that the defendant should have known it was a lie. This might require proof that the public figure had seen reliable evidence to the contrary or knew that the underlying disinformation was untrustworthy. With discovery, and for domestic defendants, this is not an impossible burden—but it is steep.

If the plaintiff cannot overcome First Amendment protection based on falsity and actual malice, she might do so based on the defendant having advocated violence or unrest. As discussed in Section II.B, First Amendment exceptions emerge with speech that is tantamount to or leads to conduct legitimately proscribed, punished, or regulated under other statutes.[311] The distinction a court must draw is whether the speech is pure advocacy, or whether it violated or compelled another to violate a law.[312] An example of disinformation that itself constitutes illegal speech is statements that qualify as seditious conspiracy, that is speech conspiring to use force to overthrow the government.[313] In one such case, the Second Circuit upheld the conviction of a lecturer at a Virginia Islamic center for inducing others to levy war.[314] Another example of unprotected speech in the antiterrorism context are true threats. "'True threats' encompass those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals . . . [though the] speaker need not actually intend to carry out the threat."[315] In *United States v. Viefhaus*, the Tenth Circuit rejected a First Amendment appeal in a conviction for making a bomb threat, holding that the defendant's speech crossed the threshold from political rhetoric to criminal threat when he stated that fifteen cities would be bombed.[316] Thus, examples

311 *See, e.g.*, United States v. Varani, 435 F.2d 758, 762 (6th Cir. 1970) ("[S]peech is not protected by the First Amendment when it is the very vehicle of the crime itself."); *see also* Brandenburg v. Ohio, 395 U.S. 444, 456 (1969) (Douglas, J., concurring) (noting "speech . . . brigaded with action" was not protected by the First Amendment).

312 *See Brandenburg*, 395 U.S. at 448 ("'[T]he mere abstract teaching . . . of the moral propriety or even moral necessity for a resort to force and violence, is not the same as preparing a group for violent action and steeling it to such action.' A statute which fails to draw this distinction impermissibly intrudes upon the freedoms guaranteed by the First and Fourteenth Amendments." (citations omitted) (majority opinion) (quoting Noto v. United States, 367 U.S. 290, 297–98 (1961))).

313 *See* 18 U.S.C. § 2384 (2020).

314 United States v. Rahman, 189 F.3d 88, 116–17 (2d Cir. 1999).

315 Virginia v. Black, 538 U.S. 343, 359–60 (2003) (citations omitted).

316 168 F.3d 392, 396 (10th Cir. 1999) (the Government charged defendant with 18 U.S.C. § 844(e) (2020)). Similarly, in *United States v. Williams*, the Eighth Circuit rejected a First Amendment challenge to 18 U.S.C. § 35(b) (conveying false information about bombing a

of disinformation that would avoid First Amendment barriers under the seditious conspiracy or true threat exceptions might include foreign disinformation advocating and enabling violent insurrection or calls to stage a rally where the actor pits sides prone to imminent violence against each other, like in the instance of the IRA promoting simultaneous pro- and anti-Islam marches in Texas.[317]

This proposed statute, by requiring the plaintiff to show that the defendant had both intended to and successfully inflicted harm, incentivizes plaintiffs to target speech that falls into a fully unprotected category.[318] But even if the harm was nonmaterial, the defendant claimed the law was restricting her expression of a viewpoint, and a court applied heightened scrutiny to the statute itself,[319] the statute's intent prong would lessen the defendant's constitutional interests as weighed against society's concern for security and civic trust. The Court in *HLP* applied demanding scrutiny to § 2339B's content-based speech and found it constitutional.[320] This standard is something more than intermediate scrutiny—inquiring whether the contested law (1) advances important government ends; (2) is substantially related to advancing those ends; and (3) is not substantially more burdensome than necessary[321]—but less than strict scrutiny—the restriction (1) "furthers a compelling interest"; and (2) "is narrowly tailored to achieve

commercial aircraft) and 18 U.S.C. § 844(e) (conveying a threat and false information in interstate commerce about the destruction of life and property by explosives) because the statutes "legitimately criminalize true threats and not protected expressive activity" and are "not examples of the government 'orchestrat[ing] public discussion through content-based mandates.'" 690 F.3d 1056, 1061–64 (8th Cir. 2012) (citation omitted).

317 *See* Martin J. Riedl et al., *Researchers Reverse-Engineer 2016 Texas Protest Organized by Russian Internet Research Agency*, TECH POL'Y PRESS (May 31, 2021), https://techpolicy.press/researchers-reverse-engineer-2016-texas-protest-organized-russian-internet-research-agency [https://perma.cc/EUL4-SAUW].

318 Such speech would effectively have no First Amendment protection. *See* Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) ("There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. . . . It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.").

319 *See* R. Randall Kelso, *The Structure of Modern Free Speech Doctrine: Strict Scrutiny, Intermediate Review, and "Reasonableness" Balancing*, 8 ELON L. REV. 291, 293–95 (2016) (describing the various levels of scrutiny a court might apply).

320 *See* Holder v. Humanitarian L. Project, 561 U.S. 1, 28 (2010).

321 *See* Kelso, *supra* note 319, at 293; *see also* Burdick v. Takushi, 504 U.S. 428, 434 (1992) ("A court . . . must weigh 'the character and magnitude of the asserted injury to the rights protected by the First and Fourteenth Amendments that the plaintiff seeks to vindicate' against 'the precise interests put forward by the State as justifications for the burden imposed by its rule,' taking into consideration 'the extent to which those interests make it necessary to burden the plaintiff's rights.'" (quoting Anderson v. Celebrezze, 460 U.S. 780, 789 (1983)).

that interest."[322] Whether tested facially or as-applied, the disinformation statute falls within those standards and survives the challenge. As for important government ends, whether the court made the assessment itself or looked to see if Congress had done so,[323] the need to prevent foreign meddling that leads to election interference or social unrest, for instance, are core societal needs, akin to the national security concerns expressed in *HLP* with terrorism. The law is substantially related to those ends in that it applies to speech strategically designed to undermine society, and it is strictly limited in its use against protected speech. Also, while the statute regulates content, it curtails only that speech which is false and furthers criminal purposes. Finally, if a court weighed minimal burden, that test is met because of the law's difficult pleading requirements, limiting the likely frequency of suits. An as-applied challenge would necessarily be fact dependent, but this statute easily withstands most free speech claims that a defendant could muster.

Considering the material support, statute as precedent strongly illustrates that even though the terrain is fragile, this proposed law, properly administered, would appropriately balance First Amendment and national security interests.

CONCLUSION

Picture next year's Thanksgiving dinner. You are sitting around the holiday table with friends and family. You talk about the kids, travel, and football. Then someone says, "Of course, we elected Obama, and he was an immigrant Muslim," and you realize it was no joke. Or your uncle says, "George Bush had a plan to let Black people die in Katrina—I've seen the data." The conversation stops. Or worse, someone across the table begins to argue. When lies become truth, community falters, even inside our own homes.

If we trace back to the source of mistruth, we can stanch the flow of harmful ideas. It is at that stage, far from the dinner table, outside of personal or even publisher's control, that a citizen army is needed. This Article's proposed statute is a government-enabled tool to help individuals strike back. And like the idiomatic Dutch boy with his finger in the dike, one person alone will not fix the disinformation problem,

---

322 *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340 (2010).

323 *See* Randall v. Sorrell, 548 U.S. 230, 249 (2006) ("[A]n appellate court has an obligation to 'make an independent examination of the whole record' in order to make sure that 'the judgment does not constitute a forbidden intrusion on the field of free expression.'" (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 285 (1964))).

but with many victims arguing their private right in court, the combined effort could be enough to force bad actors to retreat.

This Article defined disinformation, described its historic roots, and showed why it is a greater threat now than ever. It noted potential solutions and showed why none had fully met disinformation's challenges or could do so alone. It proposed a new solution: a private right of action to claim money damages against those who knowingly disseminate mistruth. Finally, it highlighted analogous antiterrorism laws that paved the path for this law to follow, then element by element, showed how the law would overcome obstacles on which the other solutions had faltered.

Even if this analysis does not close the door on every concern, it presents a largely turnkey response. It helps focus the debate and perhaps seeds new solutions where gaps remain. Disinformation is a systemic threat: its harms are sinister in that each occurrence looks minor, but its cumulative damage is stark. That threat will grow with time, or become worse if policymakers act unwisely in fighting it. A private right of action is a unique and powerful tool to unleash.