Features Essay

The International Law of Rabble Rousing*

Hendrick Townley† and Asaf Lubin††

I. INTRODUCTION

It was noon on an ordinary sunny spring day in May, but the scene was not as it should have been outside the Islamic Da'wah Center in downtown Houston, Texas.

On one side of the street stood approximately ten protestors. Bearing confederate flags and "White Lives Matter" banners, they had gathered that day for an event titled "Stop Islamification of Texas" organized by the Heart of Texas, a Facebook group celebrating the "homeland of guns, BBQ and [your] heart" and boasting 250,000 followers.[1]

---

* The authors wish to thank Barrie Sander for insightful comments on a previous draft of this Essay.
† Hendrick Townley is a software engineer and a student fellow at the Information Society Project at Yale Law School. He graduated from Yale College with a B.S. in Computer Science.
†† Asaf Lubin is an Affiliate at the Berkman Klein Center for Internet and Society at Harvard University, Visiting Fellow at the Information Society Project at Yale Law School, and Visiting Scholar at the Federmann Cybersecurity Research Center at Hebrew University of Jerusalem. This research was supported in part by funding from the William and Flora Hewlett Foundation under grant 2018-7277.
[1] *See, e.g.*, Claire Allbright, *A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest.*, TEX. TRIBUNE (Nov. 1, 2017), https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-

On the other side of the street were more than fifty counter protesters, who mounted a lively response with the help of a loudspeaker. They told reporters they had come because of yet another Facebook event: "Save Islamic Knowledge," which had been created by United Muslims of America, a Facebook group 370,000 followers strong with the tagline "I'm a Muslim, and I'm proud."[2]

As the "dueling rallies" stared each other down and the incident "eventually escalated into confrontation and verbal attacks,"[3] an active police presence kept both groups apart.[4]

There was no violence, but violent overtones colored the incident nonetheless. An event post had encouraged the anti-Islam protestors "to bring their firearms to the rally," and one protestor was seen with an AR-15 rifle slung over his shoulder.[5] The counter protestors displayed an enormous banner depicting Hitler holding a gun to his head and the exhortation: "FOLLOW YOUR LEADER—KILL YOURSELF."[6]

Representatives of the Islamic center itself had no prior knowledge of the protests and had not played a part in organizing either gathering, leaving reporters on their own to puzzle over the scene in front of them.[7]

What none of those present could have known was that both social media groups, United Muslims of America and Heart of Texas, would be named by Special Counsel Robert Mueller in a 2018 indictment as agents of the Kremlin-linked Russian Internet Research Agency (IRA).[8] Both protests had been teed up that afternoon thanks to the handiwork of one foreign entity operating thousands of miles away (and merely $200 worth of social media advertisement spending).[9]

There are a number of malicious tactics that have emerged as especially potent, subversive threats to democracy in the cyber age. "Fake news" content is spread across social media platforms by networks of bots, and promoted by ill-

---

russian-page-l/; Mike Glenn, *A Houston Protest, Organized by Russian Trolls*, HOUSTON CHRONICLE (Feb. 20, 2018), https://www.houstonchronicle.com/local/gray-matters/article/A-Houston-protest-organized-by-Russian-trolls-12625481.php.

2 Allbright, *supra* note 1; Glenn, *supra* note 1.

3 Allbright, *supra* note 1.

4 Glenn, *supra* note 1; Scott Shane, *How Unwitting Americans Encountered Russian Operatives Online*, N.Y. TIMES (Feb. 18, 2018), https://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html.

5 Glenn, *supra* note 1.

6 *Russian Trolls Organized Protests in Houston*, CNN (Jan. 26, 2018), https://www.cnn.com/videos/cnnmoney/2018/01/26/russian-trolls-houston-protests-facebook-orig-mss.cnn.

7 *See* Glenn, *supra* note 1.

8 Indictment ¶ 34, United States v. Internet Research Agency LLC, No. 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018).

9 *See* Allbright, *supra* note 1.

intentioned or incautious media outlets and even some State officials.[10] State-sponsored doxing of political leaders seeks to influence free and open democratic elections in Western nations.[11] The possibility of widespread "deep fakes"—artificially generated but lifelike images, video, or audio—threatens to change forever public trust in basic sources of information.[12] Equally alarming is how governments, businesses, and individuals are now under constant threat of debilitating cyberattacks by malicious online hackers.[13]

A burst of international law scholarship in recent years has devoted itself to characterizing these practices and crafting legal and policy solutions to address them.[14] At the center of these analyses stands the realization that while the practices seem to run counter to foundational principles of international law,[15] they have mostly frustrated precise legal definition and evaded enforcement

---

[10] *See* Adam Mosseri, *Working to Stop Misinformation and False News*, FACEBOOK (Apr. 6, 2017), https://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news; *Tackling Online Disinformation*, EUR. COMM'N, https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation (last updated Sept. 13, 2019); Joint Declaration On Freedom Of Expression and "Fake News", Disinformation And Propaganda, HRC, U.N. Doc. FOM.GAL/3/17 (Mar. 3, 2017) [hereinafter Joint Declaration on "Fake News"], https://www.osce.org/fom/302796?download=true.

[11] *See* Bruce Schneier, *The Rise of Political Doxing*, VICE (Oct. 28, 2015), https://www.vice.com/en_us/article/z43bm8/the-rise-of-political-doxing (discussing a doxing operation against former CIA director John O. Brennan); *see also* Robert Chesney, *State-Sponsored Doxing and Manipulation of the U.S. Election: How Should the U.S. Government Respond?*, LAWFARE (Oct. 21, 2016), https://www.lawfareblog.com/state-sponsored-doxing-and-manipulation-us-election-how-should-us-government-respond.

[12] *See generally* Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1757-58 (2019) ("We . . . provide the first comprehensive survey of these [deep-fake] harms and potential responses to them.").

[13] *See, e.g.*, Christopher Bing & Sarah N. Lynch, *U.S. charges North Korean Hacker in Sony, WannaCry Cyberattacks*, REUTERS (Sept. 6, 2018), https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W (discussing the oft-cited North Korean hacking of Sony Pictures); Dave Weinstein, *Hackers Hold Baltimore Hostage*, WALL ST. J. (May 30, 2019), https://www.wsj.com/articles/hackers-hold-baltimore-hostage-11559256722 (discussing the recent hacking incident that afflicted the city of Baltimore)).

[14] *See, e.g.*, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0] (a manual produced by a group of international experts on behalf of the NATO Cooperative Cyber Defence Centre of Excellence proposing rules to govern below the threshold of use of force cyber operations); Björnstjern Baade, *Fake News and International Law*, 29 EUR. J. INT'L L. 1357 (2018); Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565 (2017); Duncan Hollis, *The Influence of War; the War for Influence*, 32 TEMP. INT'L & COMP. L.J. 31 (2018); Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT'L SEC. J. 146 (2018); Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law*, 95 TEX. L. REV. 1579 (2016); Barrie Sander, *Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections*, 18 CHINESE J. INT'L L. 1 (2019); Michael N Schmitt, *Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30 (2018); Claire Wardle & Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, COUNCIL OF EUR. (2017), https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c; *Faking News: Fraudulent News and the Fight for the Truth*, PEN AM. (Oct 12, 2017), https://pen.org/wp-content/uploads/2017/11/2017-Faking-News-11.2.pdf [hereinafter *Faking News*].

[15] One of the central principles of international law is the obligation to strengthen friendly relations which was adopted by G.A. Res 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Oct. 24, 1970) [hereinafter Friendly Relations Declaration], and recognized as reflective of customary international law in Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (Nov. 26) [hereinafter Military and Paramilitary Activities].

attempts despite their sudden intensity.[16] Indeed, international law has been slow to adapt to the remote and non-kinetic nature of modern-day cyber transgressions, exacerbating significant "grey areas" of legal uncertainty.[17] Moreover, fundamental human rights, including the freedom of expression, provide strong reason to avoid excessive, potentially oppressive regulation of a battlespace entirely centered around communication and communications technologies.[18]

Within the theater of modern information warfare there exists a particularly devious, and previously unnamed, practice that existing legal literature has so far mostly ignored. We call this practice—exemplified in the introductory narrative—*rabble-rousing*: the simultaneous, two-sided amplification of content in support of directly contradictory stances on controversies of national significance. The goal of these operations is to sow mistrust and aggravate divisions within a target populace.

The tactic has become an especially potent weapon thanks to the widely present technologies of the cyber age, including social media platforms and automated "bot" capabilities.[19] This strategy is distinct both from the injection of "fake news" into public discourse—as it need not involve false information—and from doxing and hacking—as it has no obviously illegal component under domestic law nor does it target a single individual.

This Essay offers an account of rabble-rousing, a novel information warfare operation worthy of its own classification, and explores the extent to which contemporary international law and available technologies are capable of addressing the threat that this tactic poses to public world order.

This Essay proceeds as follows. Part I provides a definition of rabble-rousing strategies, highlighting the ways by which they are uniquely defined from other forms of information warfare. It then proceeds to highlight the dangers associated with the practice.

Part II moves to examine whether rabble-rousing can be recognized as an internationally wrongful act under the traditional paradigms of public international law. It looks at the prohibitions on coercive intervention, transboundary harm, and subversive propaganda as well as the principle of

---

[16] *See, e.g.*, Ohlin, supra note 14, at 1579 ("To the layperson, the Russian hacking constituted an impermissible (and perhaps) shocking interference in the American political process . . . [t]he problem arises when one attempts to translate that commonsense intuition into legal discourse."); Chesney & Citron, *supra* note 12, at 42 ("To some extent, this is a question of setting law enforcement priorities and allocating resources accordingly. Here, the track record is not promising.").

[17] *See generally* Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L. L. ONLINE 1, 3 (2017) ("[I]dentif[ying] certain critical grey zones of international law that are susceptible to exploitation when conducting cyber operations.").

[18] *See* Faking News, *supra* note 14, at 24.

[19] *See* Adrian Chen, *The Agency*, N.Y. TIMES (Jan. 1, 2015), https://www.nytimes.com/2015/06/07/magazine/the-agency.html (exposing the influence of the Kremlin-linked Internet Research Agency "employing hundreds of Russians to post pro-Kremlin propaganda online under fake identities, including on Twitter.").

sovereignty and the human rights to self-determination and freedom of expression[20] in order to determine the legality of rabble-rousing operations under international law. This Part highlights the limits of traditional interpretations of the above legal regimes and proposes how certain adaptations to the law could potentially better capture the examined phenomenon.

Part III assesses current technological capabilities and proposes policy solutions, which will be necessary for States to practically defend against this activity regardless of whether or not wrongfulness can be established. Part IV concludes the argument.

Ultimately, we hope that this Essay will serve as a call-to-action for scholars and practitioners to expand on their existing taxonomies of the informational theater of conflict, and to promote nuanced solutions that take all considerations into account.

II. INTRODUCING RABBLE-ROUSING: A TWO-FACED TROLL

A. What Is Rabble-Rousing?

Escaping the focus of scholarly attention up until now is a very particular and ingeniously devious method of sowing discord by "playing both sides against the middle" online. For the purpose of this Essay, this practice is defined as rabble-rousing—a coordinated operation to conduct widespread, simultaneous amplification of both opposing sides of a nationally divisive issue.[21]

This practice is best conveyed illustrated by example. In addition to the opening narrative, we here provide several examples of varying intensity, in chronological order. This collection of examples is the first time these events have been brought together under the umbrella of such a focused category of information operations.

Over a nine month period between January and October 2016, hundreds of thousands of tweets referencing shootings and the Black Lives Matter movement in the United States were posted by accounts linked to the IRA. Analysis of this

---

[20] We recognize that one could have also considered the right to political participation. However, a violation of the right could only be argued in the limited scenario where rabble-rousing causes undue influence in an election or referendum (*see* U.N. Hum. Rts. Comm., General Comment 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service (Art. 25), U.N. Doc. CCPR/C/21/Rev.1/Add.7, ¶ 19 (Jul. 12, 1996)). Similarly, we have excluded from our analysis, for reasons of space, the preliminary discussion around the extraterritorial scope of application of those human rights.

[21] In addition to "rabble-rousing" various other phrases were considered including "double-faced amplification" and "two-sided trolling." Ultimately, we settled on "rabble-rousing" as the best phrase to encapsulate the core purpose of the practice: to amplify and aggravate tensions and divides among a populace on a widespread scale. Note, part of the international illegality of rabble-rousing would depend on the ability to attribute the practice back to a responsible State (as distinguished from the operation of private hackers). There are significant hurdles in establishing attribution in cyberspace, and this short analysis cannot begin to address this point fully. For further reading see Monica Hakimi, *Introduction to Symposium on Cyber Attribution*, 113 AM. J. INT'L L. UNBOUND 189 (2019) and the other contributions to the symposium.

content demonstrated that the agency simultaneously amplified both left- and right-leaning discussions.[22]

On November 12, 2016, the IRA organized two rallies in New York within the very same day—one to "show your support for President-Elect Donald Trump" and the other titled "Trump is NOT my President."[23] These findings were reported in the February 2017 indictment filed by special prosecutor Robert Mueller, which found that the IRA "used false U.S. personas to organize and coordinate U.S. political rallies in support of then president-elect Trump, while simultaneously using other false U.S. personas to organize and coordinate U.S. political rallies protesting the results of the 2016 U.S. presidential election."[24]

In the fall of 2017, as nationwide controversy erupted across the United States over professional football players kneeling in protest during the national anthem, Russian trolls amplified hashtags on either side of the divide in popular opinion.[25] Senator Lankford conveyed that U.S. intelligence personnel shared with Senate leaders the fact that Russian actors "were taking both sides of the argument this weekend . . . to try to raise the noise level of America and make a big issue seem like an even bigger issue as they are trying to push divisiveness in this country."[26]

In 2018, researchers discovered that Russian social media accounts "stoked the [U.S. vaccination] debate by tweeting pro- and anti-vaccine messages in an apparent attempt to sow division."[27] Analysis of #VaccinateUS, "a Twitter hashtag designed to promote discord using vaccination as a political wedge issue," revealed that twitter accounts identified as Russian trolls paid roughly "equal attention to pro- and anti-vaccination arguments."[28]

All of these examples share in common having a Russian agent as the actor and the U.S. populace as the victim. This should not come as a surprise given

---

[22] Leo G. Stewart, et al., *Examining Trolls and Polarization with a Retweet Network*, Proceedings of WSDM workshop on Misinformation and Misbehavior Mining on the Web (MIS2) (2018), https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf (evidence suggests "RU-IRA troll accounts . . . [fed] content into both sides of an information network characterized by divergent and competing frames").

[23] *See* Indictment ¶ 57, United States v. Internet Research Agency, *supra* note 8; Alicia Parlapiano & Jasmine C. Lee, *The Propaganda Tools Used by Russians to Influence the 2016 Election*, N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html.

[24] *Id.*

[25] Andrew Beaton, *How Russian Trolls Inflamed the NFL's Anthem Controversy*, WALL ST. J. (Oct. 22, 2018), https://www.wsj.com/articles/how-russian-trolls-inflamed-nfls-anthem-controversy-1540233979.

[26] Dustin Volz, *Senator Says Russian Internet Trolls Stoked NFL Debate*, REUTERS (Sept. 27, 2017), https://www.reuters.com/article/us-usa-congress-cyber-russia/senator-says-russian-internet-trolls-stoked-nfl-debate-idUSKCN1C237J.

[27] Carolyn Y. Johnson, *Russian Trolls and Twitter Bots Exploit Vaccine Controversy*, WASH. POST (Aug. 23, 2018), https://www.washingtonpost.com/science/2018/08/23/russian-trolls-twitter-bots-exploit-vaccine-controversy.

[28] David A. Broniatowski, et al., *Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate*, 108 AM. J. PUB. HEALTH 1378 (2018).

that the Russian government has funded an initiative called Project Lakhta dedicated to launching rabble-rousing attacks against the United States.[29]

Although most of the publicly reported evidence centers around U.S.-Russian relations, there is no reason that rabble-rousing attacks should be limited to the interplay between these two countries. Indeed, examples that break this mold—while lesser known—do exist.

For example, in 2019, an analysis of Russian influence in Germany demonstrated that "both official Russian government media and unofficial pro-Russian channels" not only showed strong support for "the far-right Alternative for Germany [AfD] party" but also "appeared to amplify messages from AfD's staunchest opponents, left-wing anti-fascists."[30] This serves to "underscore what analysts say is Russia's true interest—sowing political discord in democracies, regardless of ideology."[31]

Furthermore, the Chinese government pays hundreds of thousands of its citizens to manipulate public opinion through online commenting – an effort that has been dubbed "the 50 Cent army."[32] In 2012, the celebrated Chinese artist and activist Ai Weiwei interviewed one such paid commenter, who said of the group's online commenting strategy: "Most of the time we're debating with ourselves . . . [the aim of arguing both sides of a debate] is to anger netizens and divert the anger and attention . . . to me."[33]

---

[29] *See* Steven Melendez, *DOJ Charges Russian Accountant with Targeting 2018 Midterms*, FAST COMPANY (Oct. 19, 2018), https://www.fastcompany.com/90254282/what-is-project-lakhta-russian-accountant-charged-with-targeting-2018-midterms ("The operation allegedly generated divisive social media posts, targeting audiences on both sides of issues like immigration, LGBT rights, gun control, and the Confederate flag.").

[30] Matt Apuzzo & Adam Satariano, *Russia Is Targeting Europe's Elections. So Are Far-Right Copycats.*, N.Y. TIMES (May 12, 2019), https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html.

[31] *Id.* Another example involves alleged Russian rabble-rousing operation in Canada in relation to the controversy surrounding an addition to the Keystone Oil Pipeline. *See* Roberta Rocho, *Data Sheds Light on how Russian Twitter Trolls Targeted Canadians*, CBC (Aug. 3, 2018), https://www.cbc.ca/news/canada/russian-twitter-trolls-canada-targeted-1.4772397.

[32] Henry Farrell, *The Chinese Government Fakes Nearly 450 Million Social Media Comments a Year. This is Why.*, WASH. POST (May 19, 2016), https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why.

[33] Ai Weiwei, *China's Paid Trolls: Meet the 50-Cent Party*, NEW STATESMAN AM. (Oct. 17, 2012), https://www.newstatesman.com/politics/politics/2012/10/china's-paid-trolls-meet-50-cent-party. Observers have found a "high level of coordination in the timing and content in these posts" suggesting the approach described to Ai Weiwei is representative of a larger trend. Gary King, et al., *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*, 111 AM. POL. SCI. REV. 484, 485 (2017). That being said, most research suggests that China's overall online strategic goal is not to amplify division, but instead to "cheerlead" and promote Chinese values and policies. *See Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion*, Recorded Future Blog (Mar. 6, 2019), https://www.recordedfuture.com/china-social-media-operations/; *See also Information Operations Directed at Hong Kong*, TWITTER SAFETY (Aug. 19, 2019), https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html ("disclosing a significant [Chinese] state-backed information operation" discrediting pro-democracy protestors in Hong Kong).

Since 2016, cybersecurity analysts have found that "campaigns tied to various governments" around the world have taken a page from the Russian "playbook for spreading disinformation on social media,"[34] including in the form of rabble-rousing. In summer 2018, documents were leaked from the Venezuelan Interior Ministry detailing the country's "plans for developing a government backed 'troll army.'"[35] The report describes separate squadrons dedicated to amplifying pro-government positions as well as opposing those positions.[36] In Fall 2018, a "new influence network" originating in Iran was detected on Facebook where it had impacted at least a million users across the United States and Britain. The Iranian posts "meant for British users took both sides in the country's political debates."[37] In the same year, the CEO of social media intelligence company, Zignal Intelligence, spoke of increasing activity of bot networks amplifying "both sides" of issues to "sow discord within Western culture" although he was unable to identify the origin of these activities.[38]

In all of these instances, foreign nations have been involved in taking advantage of publicly available online discourse tools to simultaneously drum up support for directly contradictory stances on controversies of national significance. Despite the deluge of literature concerning misinformation and online manipulation, rabble-rousing has never been identified as its own standalone practice.[39]

B. The Danger of Rabble-Rousing

At the heart of rabble-rousing is the amplification of simultaneously contradictory themes. The absurdity of such an expression was illustrated humorously and incisively by Representative Noah Sweat's 1952 speech

---

[34] Sheera Frenkel et al., *Russia's Playbook for Social Media Disinformation Has Gone Global*, N.Y. TIMES (Jan. 31, 2019), https://www.nytimes.com/2019/01/31/technology/twitter-disinformation-united-states-russia.html.

[35] Michael Riley et al., *A Global Guide to State-Sponsored Trolling*, BLOOMBERG (July 19, 2018), https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook.

[36] *See Proyecto de Formación del Ejército de Trolls Venezuela* [Plan for the Development of the Troll Army of Venezuela], MINISTERIO DEL PODER POPULAR [INTERIOR MINISTRY] 5 (2017), https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/data/Ejercito_De_Trolls_Venezuela.pdf. This document is part of a pool of sources collected by Bloomberg as part of its Global Guide to State-Sponsored Trolling.

[37] Mike Isaac & Sheera Frenkel, *Facebook Removes Iranian Network That Was Spreading Disinformation*, N.Y. TIMES (Oct. 26, 2018), https://www.nytimes.com/2018/10/26/technology/facebook-removes-iranian-network-that-was-spreading-disinformation.html.

[38] *How Bots Amplify Hoaxes and Propaganda on Social Media*, VOX (Aug. 2, 2018), https://www.vox.com/2018/8/2/17636264/josh-ginsberg-zignal-bot-recode-decode.

[39] For a general overview of state-sponsored trolling efforts, *see generally* Samantha Bradshaw & Philip N. Howard, *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*, COMPUTATIONAL PROPAGANDA PROJECT (2018), https://blogs.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf; Carly Nyst & Nick Monaco, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, INST. FOR THE FUTURE 23-44 (2018), http://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf (providing in-depth case studies of "state-sponsored trolling"); Maeve Shearlaw, *From Britain to Beijing: How Governments Manipulate the Internet*, GUARDIAN (Apr. 2, 2015), https://www.theguardian.com/world/2015/apr/02/russia-troll-factory-kremlin-cyber-army-comparisons.

regarding the legalization of alcoholic beverages (which later became known as the *if-by-whiskey* logical fallacy):

> I want you to know that I do not shun controversy. On the contrary, I will take a stand on any issue at any time, regardless of how fraught with controversy it might be. You have asked me how I feel about whiskey. All right, here is how I feel about whiskey:
>
> If when you say whiskey you mean the devil's brew, the poison scourge, the bloody monster, that defiles innocence, dethrones reason, destroys the home, . . . *then certainly I am against it*. But, if when you say whiskey you mean the oil of conversation, . . . the sale of which pours into our treasuries untold millions of dollars, which are used to provide tender care for our little crippled children, our blind, our deaf, our dumb . . . ; to build highways and hospitals and schools—*then certainly I am for it*.
>
> *This is my stand. I will not retreat from it. I will not compromise*.[40]

In taking both sides, Representative Sweat deceptively does not take any side. He instead leans into the existing controversy and amplifies confusion. Mississippi was the last State to go wet, and whiskey was the most controversial issue of the day. By simultaneously making the case for both, Sweat "lampoon[ed] legislators' reticence to take a position on liquor."[41]

Our analysis identifies parallel characteristics inherent to rabble-rousing. But unlike Sweat's speech, which openly and absurdly draws attention to its self-contradiction, the posts produced by bots and trolls are written in mass and obscure their ultimate intentions. They are not comical devices aimed at triggering changes of policy. Rather, they are real and scary assaults on social cohesion masquerading as legitimate expression.

The destabilizing force represented by rabble-rousing is immense and worthy of our utmost attention. The practice interferes with public discourse and pollutes the "processes of collective will formation" that are crucial for proper democratic functioning.[42] Rabble-rousing capitalizes on the phenomenon of group polarization whereby the exchange of arguments within a group results in individuals drifting further apart ideologically and adopting more extreme positions than they held previously.[43] Sunstein has shown how the algorithms at the base of search engines and social media profiles may be utilized to intensify incidents of group polarization.[44]

---

[40] *Judge Noah Sweat of Mississippi Shows How to Straddle a Fence with Satiric Flair*, *in* LEND ME YOUR EARS: GREAT SPEECHES IN HISTORY 954-55 (William Safire ed., 2004) (emphasis added).
[41] Orley Hood, *On June 3, Soggy's Speech Will Come to Life*, CLARION LEDGER (May 25, 2003), https://archive.is/20120714122102/http://orig.clarionledger.com/news/0305/25/oorley.html#selection-601.0-601.43.
[42] CHRIS TENOVE ET AL., DIGITAL THREATS TO DEMOCRATIC ELECTIONS: HOW FOREIGN ACTORS USE DIGITAL TECHNIQUES TO UNDERMINE DEMOCRACY 8-10 (2018).
[43] CASS R. SUNSTEIN, INFOTOPIA: HOW MANY MINDS PRODUCE KNOWLEDGE 92-96 (2006).
[44] *Id.* at 97-98.

This amplification of divisiveness today is a great threat, and western democracies with open societies encouraging the free flow of information and the discourse of conflicting ideas and identities are especially vulnerable.[45] Democracies across the world wrestle with unifying increasingly diverse nations of peoples and immigrants under the auspices of an open society.[46] Rabble-rousing wears at the fabric of open societies, slowly, but surely, eroding the very foundations of democracy itself.

The international legal order is dependent on unions coalescing around sets of higher values. The very existence of international law as the law of nations is dedicated to connecting the disparate countries of the world around common principles of cooperation and peace. A practice that, at its very core, seeks to cleave tribes further apart, must be gravely antithetical to a vision of a shared life exercised "in peace with one another as good neighbors," as is manifested in the U.N. Charter's preamble.

C. Why Rabble-Rousing?

Several authors have put forward taxonomies in order to distinguish between various forms of information and cyber operations.[47] Broadly speaking, rabble-rousing falls under the diverse umbrella category of cyber influence operations: the "deployment of resources for cognitive ends that foster or change a targeted audience's behavior" in the context of cyberspace."[48] Wardle and Derakhshan further distinguish between influence operations involving dis-information and mal-information. Whereas the former concerns *false* information "knowingly shared to cause harm," the latter concerns *genuine* information that is shared with the intention of causing harm.[49] On its face, rabble-rousing is simply an example of mal-information.

There are several characteristics that each of the provided examples share in common and which set rabble-rousing apart from other similar practices.

---

[45] *See* Herbert Lin & Jaclyn Kerr, *Influence Warfare and Manipulation*, *in* OXFORD HANDBOOK OF CYBERSECURITY 17-18 (forthcoming, 2019).

[46] *See, e.g.*, Joseph Nye, *Protecting Democracy in an Era of Cyber Information War*, HOOVER INSTITUTION (Nov. 13, 2018), https://www.hoover.org/research/protecting-democracy-era-cyber-information-war ("Autocracies are able to protect themselves by controlling information flows, while the openness of democracies creates vulnerabilities that autocracies can exploit via information warfare. Ironically, one cause of the vulnerabilities has been the rise of social media and mobile devices in which American companies have been the global leaders. Citizens voluntarily carry Big Brother and his relatives in their pockets. Along with big data and artificial intelligence, technology has made the problem of defending democracy from information warfare far more complicated than foreseen two decades ago.").

[47] *See, e.g.*, TENOVE, *supra* note 42, at 12-25; Lin & Kerr, *supra* note 45, at 9-11; Sander, *supra* note 14, at 5-14; Wardle & Derakhshan, *supra* note 14, at 20-22.

[48] *See* Hollis, *supra* note 14, at 36; s*ee also* Sander, *supra* note 14, at 7-14. Also referred to as "cyber-enabled information/influence warfare and manipulation"—"the deliberate use of information against an adversary to confuse, mislead, and perhaps to influence the choices and decisions that the adversary makes" —by Lin & Kerr, *supra* note 45, at 3.

[49] *See* Wardle & Derakhshan, *supra* note 14, at 5.

First, the two stances that are the subject of amplification are directly opposite and irreconcilable.[50] This stands in contrast to the more straightforward practice of amplifying a single theme or opinion—a very common tactic in today's cyber age.[51] One-sided amplification does not fall under the definition of rabble-rousing established for the purposes of this Essay. The contradictory nature of rabble-rousing is crucial to the legal analysis that will follow. For this reason, amplification operations more generally are not the main subject of our analysis either.

Second, there is no obviously illegal act either domestically or internationally since the social media platform functionality used in each instance is publicly available. This stands in contrast to political *doxing*, which typically involves the hacking of private computers to obtain sensitive information—a deliberate violation of domestic cyber and data security laws, such as the U.S. Computer Fraud and Abuse Act.[52]

Third, there is no immediate falsity of information. The rallies advertised really do take place and the views expressed in individual posts are not out of place with the opinions of many of those being influenced. This stands in contrast to the deliberate spread of false news stories, which has attracted much of the scholarly attention.[53]

Finally, rabble-rousing may amplify existing content and need not promote a specific policy agenda. This stands in contrast to State-sponsored propaganda, which is expressly engineered for the purpose of advancing specific political goals and ideas of interest to the sovereign manipulator.[54]

---

[50] One issue worth highlighting is when should two themes be considered clearly opposite. Consider, for example, the supporters of Bernie Sanders and Donald Trump respectively. Practically, speaking there are strong arguments to make for why amplifying both Sanders and Trump could result in divisiveness. Philosophically speaking, it is very difficult to make the case that supporting both candidates would have been irrational. After all, there is an unusual but logically consistent argument to make for supporting both Bernie *and* Trump. Therefore, if a bot is engaging in the simultaneous advertising of statements by both candidates, is it engaging in rabble-rousing? We leave this question open.

[51] *See generally*, Nyst & Monaco, *supra* note 39 (detailing seven case studies of state-sponsored trolling involving one-sided amplification). A bad actor can be effective in achieving the divisive results of rabble-rousing by only amplifying one-sided messages or themes. For example, an ongoing Iranian disinformation campaign, dubbed "Endless Mayfly" has promoted geopolitical and domestic discord since April 2016 by means of narratives entirely critical of Saudi Arabia. Thanks to "ephemeral disinformation" tactics the campaign avoided attribution for years, deceived mainstream media outlets, and engineered thousands of clicks on inauthentic news articles. Gabrielle Lim et al., *Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign*, CITIZEN LAB (May 14, 2019), https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign; *see also* FireEye Intelligence, *Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East*, FIREEYE (Aug. 21, 2018), https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html.

[52] 18 U.S.C. § 1030 (1986).

[53] *See* Baade, *supra* note 14; *Faking News*, *supra* note 14.

[54] It is worth mentioning that influence operations are not strictly unique to the digital world. Russia spread "fake news" manually before the rise of the internet, planting hoaxes about the United States inventing AIDS in third world developing countries such as India and monitoring their slow, but steady percolation into western media environments. *See e.g.*, *Soviet Influence Activities: A Report on Active*

These differences are important for three reasons. First, they enable rabble-rousing to sidestep the arguments most commonly employed against other forms of cyber information operations. Without being explicitly violent, or explicitly false, or explicitly political, it is not immediately obvious how to construct a legal position in opposition to the practice.

Second, the two-sided nature of rabble-rousing, which uniquely distinguishes the practice from amplification operations more generically, also presents a unique risk to democratic and liberal systems predicated on finding common ground and bridging differences. This serves as a strong motivating force for the forthcoming legal dissection of rabble-rousing, as we seek to determine what legal tools are available to protect our world order from corrosive assaults aimed at endangering that very order.

Third, the same quality of self-contradiction might justify prohibiting this unique information amplification practice. As we discuss later in the Essay, there is room to challenge the expressive value of such speech in a way that might not be as readily available against other forms of information warfare such as fake news, deep fakes, or propaganda.

III. THE LEGALITY OF RABBLE-ROUSING: A SQUARE PEG AMONG ROUND HOLES

Rabble-rousing, like many other below the threshold of the use of force information warfare tactics, proves to have the remarkable slippery ability of persistently evading legal characterization. In the first half of this section, this slipperiness will become increasingly clear. We approach the problem of rabble-rousing from a variety of perspectives drawn from an exploration of many different domains of international law. These domains include the prohibitions on coercive intervention, transboundary harm, and subversive propaganda as well as the principle of sovereignty and the human right to self-determination. We show that each of these international legal regimes fails to pin down the corrosive properties of rabble-rousing to any consistent concept of illegality.

It is only with an analysis of the unique contradictory nature of rabble-rousing in the context of international human rights law and the freedom of expression that we make any progress in unlocking a path towards conceptualizing the illegality of rabble-rousing.

A. Rabble-Rousing and the Principle of Non-Intervention

Almost every international legal scholar—in seeking to characterize the novel digital age disruptions previously introduced—has made an attempt to

---

Measures and Propaganda 1986-87, U.S. DEP'T STATE . (Aug. 1987), https://www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf. Nonetheless, it would be wrong to consider these practices in isolation from technology in this day and age. The internet and social media in particular have allowed the same acts to be committed at lower cost and risk and with greater speed and breath than ever before. *See* Sander, *supra* note 14, at 3-4 ("The contemporary technological landscape is particularly conducive to influence operations.").

apply the principle of non-intervention. This makes obvious sense. By the ordinary meaning of the term there is an intuitive sense that States responsible for these practices are "intervening" in the affairs of another. In this spirit, we will first attempt to describe rabble-rousing through the lens of the prohibition on intervention in the domestic affairs of other States. This Essay will reaffirm, as other scholars have, that the element of *coercion*, crucial to the definition of non-intervention, serves as the primary obstacle to a designation of illegality.

Although "the exact meaning of the principle remains unclear," there is wide consensus that any prohibited intervention must satisfy two conditions.[55] The two conditions are best summarized by the ICJ's ruling in the *Military and Paramilitary Activities* case: the intervention must be (1) "bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely [such as] the choice of a political, economic, social and cultural system, and the formulation of foreign policy" (the *Domaine Réservé* requirement); and (2) conducted via "forcible or dictatorial means" as evidenced by "the element of coercion, which forms the very essence of prohibited intervention" (the coercion requirement).[56] We analyze both of these conditions below.

1. Domaine Réservé

The first condition is commonly referred to as the condition of *domaine réservé* (reserved domain) "describ[ing] the areas of State activity that are internal or domestic affairs of a State." The scope of this notion is in considerable flux as "there are hardly any subject-matters or policy areas today that are inherently removed from the international sphere."[57] Nonetheless, there is a relatively simple argument to be made for rabble-rousing satisfying this first condition. In an open, democratic nation, the people are the ultimate deciders of the "political, economic, social and cultural system[s]," which govern their society. Platforms, both abstract and constructed, channeling speech, ideas and expression are the means by which a democratic people gradually converge on a consensus. Since rabble-rousing operations participate at scale alongside and in the same medium as active democratic discussion, there is sufficient reason to believe that "matters in which each State is permitted . . . to decide freely" may be involved. This is especially the case when rabble-rousing is utilized to interfere in the outcome of elections, as the Russian-American and Russian-German above-mentioned examples demonstrate.

2. Coercion

The ICJ identified coercion as being "particularly obvious in the case of an intervention which uses force."[58] Indeed, most traditional interpretations of the second condition, the coercive element, place a premium on physicality and

---

[55] Philip Kunig, *Prohibition of Intervention*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?prd=EPIL (last updated Apr. 2008).

[56] *See* Military and Paramilitary Activities, *supra* note 15, at 108; Kunig, *supra* note 55.

[57] Katja S. Ziegler, *Domaine Réservé*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398 (last updated Apr. 2013).

[58] *See* Military and Paramilitary Activities, *supra* note 15, at 108.

kinetic force. Of the four main forms of intervention identified by Kunig—military, economic, diplomatic and subversive—the latter serves as the closest match to the characteristics of rabble-rousing. Subversive intervention, consisting of "propaganda or other activities by one State with the intention of influencing the situation in another State," is prohibited if it "aim[s] to foment revolt or civil strife in another State or [is] devoted to assisting illegal and violent activities."[59] Revolt, civil strife and violent activities are all terms which demand real world physical effects. As our examples of rabble-rousing demonstrate, only rarely do these operations trigger actual physical violence or civil strife. Moreover, the ability to show a causal link, meeting all evidentiary requirements, between the perpetrating State and the rabble-rousing, and between the rabble-rousing and the potential violence is equally tenuous. This physical, kinetic standard is, therefore, too high to encompass most forms of rabble-rousing conducted online.

Tallinn Manual 2.0, an academic non-binding study of the international law of cyberspace produced by an international group of experts, adopted a lower standard for coercion. The experts "agreed that to be coercive . . . the acts concerned need not be physical in nature."[60] Instead, the intervention must be instrumental in "factually compelling" the actions of a target State.[61] Ohlin has similarly concluded that resulting physical violence is not a *sine qua non* of coercion. Instead the test is that the threat or coercive act be more than mere influence, but rather deprive the victim State of choice by making it "act in a way that it otherwise would not act."[62] This requirement, while setting a lower standard, still distinguishes coercive intervention "from persuasion, criticism, public diplomacy, propaganda, retribution, mere maliciousness, and the like in the sense that, unlike coercion, such activities merely influence the voluntary actions of the target State or seek no action on the part of the target State at all."[63] In this sense, a cyber operation not intended to change policy and make a government or a people take a certain course of action cannot meet the requisite coercive element.[64]

Even this lower bar would seem to exclude most instances of rabble-rousing. Generally speaking, rabble-rousing is not targeted at a Government being compelled to adopt a different policy. Rather, it aims to slowly sow mistrust in the institutions of the government, pushing people to pull at the threads of the communal fabric that makes up their society.

Ultimately, the amplification of contradictory hashtags seems more akin to "mere maliciousness"—a noise-producing program with a longer arc aimed at

---

[59] *See* Kunig, *supra* note 55, ¶ 24 (citing to the International Convention concerning the Use of Broadcasting in the Cause of Peace (Geneva, 1936)).
[60] *See* TALLINN MANUAL 2.0, *supra* note 14, at 318.
[61] *Id.* at 318-319. Note that the finding of the experts in *Tallinn Manual 2.0* has been recently criticized by a number of scholars as to its legal authority. *See, e.g.*, Dan Efroni and Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583 (2018).
[62] *See* Ohlin, *supra* note 14, at 1592. *See also* Schmitt, *supra* note 17, at 8.
[63] *See* TALLINN MANUAL 2.0, *supra* note 14, at 318-19.
[64] *Id.*

the gradual destabilization of governance through the upending of certain democratic processes. Each individual piece of amplified content thus lacks the necessary coercive elements that would seem to be required to constitute a prohibited intervention. The ICJ's *Oil Platforms* decision does open the door for combining operations, which individually might not meet the required threshold, to examine whether their aggregate effect does cross the line.[65] This is indeed promising, although the problem here is one of timing. By the time the aggregate effect of each of these rabble-rousing tactics could potentially be said to rise to the level of coercion under an *Oil Platforms* theory, it is likely to already be too late. Long-lasting irrevocable harms would have already been caused to the societies targeted.

Given the high bar set by the element of coercion, some scholars have suggested a variety of means to sidestep this condition altogether. Kilovaty suggests that the non-intervention principle should be augmented to cover a degree of "disruptiveness" as a suitable alternative to the outdated requirement of a "coercion element."[66] In implementing this standard, however, we simultaneously risk the adoption of an over-encompassing definition that would capture a whole gamut of legitimate contemporary interstate interferences in the dragnet (such as lawful countermeasures, sanctions, diplomatic downgrading, public condemnations, and other international shaming-and-blaming techniques).

Ohlin, looking entirely beyond the non-intervention norm for alternatives *sans* coercion, argued that the usurpation of an inherently government function "does not require the element of coercion" but does qualify as a prohibited international act.[67] The international group of experts behind *Tallinn Manual 2.0* also adopted this position.[68] Even if we were to accept their approach, rabble-rousing would seem to fall short of this standard. In the rabble-rousing context, the perpetrator takes advantage of publicly available technological tools to manipulate the algorithms of privately held social media platforms to

---

[65] Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, 191-92, ¶ 64 (Nov. 6). The Court did not reject the United States theory that a series of alleged attacks attributed to Iran could be read "cumulatively" to reach the threshold of an armed attack. *Id.* Far from it, the Court instead examined the evidence surrounding each individual attack and concluded that even together they do not constitute an armed attack. *Id.* With regards to its international acceptance, David Kretzmer has noted in 2013 that "[t]he accumulation of events theory has not gained general acceptance in the international community. There are, however, signs that with the growing awareness that transnational terrorist attacks present states with a serious problem, it is not as widely rejected as it was in the past." *See* David Kretzmer, *The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum*, 24 EUR. J. INT'L L. 235, 244 (2013); *See also* J. Francisco Lobo, *One Piece at a Time: The 'Accumulation of Events' Doctrine and the 'Bloody Nose' Debate on North Korea*, LAWFARE (Mar. 16, 2018, 7:00 AM), https://www.lawfareblog.com/one-piece-time-accumulation-events-doctrine-and-bloody-nose-debate-north-korea ("[T]he accumulation of events doctrine has more support in both theory and practice . . . [and] has been relied upon by several states"). If we were to accept this theory as customary, then "the whole . . . [can be] greater than the sum of its parts," or, in other words, "low-level uses of force may in the aggregate produce a higher-level armed attack." *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 211 (6th ed., 2017). Adopting this model, we can similarly imagine a case where low-levels of noise-producing information operations may in the aggregate result in a higher-level coercive intervention.

[66] *See* Kilovaty, *supra* note 14, at 167-69.

[67] *See* Ohlin, *supra* note 14, at 1593.

[68] *See* TALLINN MANUAL 2.0, *supra* note 14, at 24.

strategically influence public discourse. As such, rabble-rousing does not seem to qualify as such usurpation as it does not involve commandeering governmental functions.[69]

B. Rabble-Rousing, the Principle of Self-Determination, and the Prohibition on Subversive Propaganda

The practice of rabble-rousing is also not covered by the principle of self-determination or as subversive propaganda. Modern international law recognizes the right of a people to decide their own destiny in the international order by freely determining their political status.[70] The Declaration on Principles of International Law Concerning Friendly Relations, which was recognized as customary by the ICJ, declares a similar positive right of people "freely to determine . . . their political status," as well as pursue "economic, social and cultural development" all "without external interference."[71] This principle finds its historical underpinnings in the work of Grotius, who acknowledged that "whenever two peoples are united, their rights will not be lost but will be shared in common."[72]

But what are these "rights . . . shared in common"? Professor and diplomat Philip Marshall Brown argued that it was a "mutual guarantee between nations, great and small, of their legal right to a separate existence in order to realize their own aspirations and destinies."[73] He further considered this right "the solid rock of international law."[74] Ohlin has argued, in the context of the alleged Russian interference in U.S. elections, that where a foreign nation utilizes cyber means to substitute its sovereign will for that of the targeted nation, such an act would constitute a violation of the principle of self-determination.[75]

The principle of self-determination of peoples, if adopted in such an expansive way, might encompass some forms of rabble-rousing (for example, where the rabble-rousing can be sufficiently shown to have influenced election results). Nonetheless, this analysis cannot put to rest the lingering issue of coercion (or lack thereof). Although there is no formalized requirement of "coercion" for self-determination violations, the norm "does not have an absolute

---

[69] An interesting line of inquiry would be to examine whether the governments of western democracies have an obligation to ensure the existence of free and secure forums for public discussion. Is providing a marketplace for ideas, and protecting it from potential abuse, an "inherently governmental function"? If so, are private social media platforms already usurping this function? Within the limits of this Essay we leave these questions open.

[70] *See, e.g.*, Case Concerning East Timor (Port. v. Austl.), Judgment, 1995, I.C.J. 90, ¶ 29 (June 30) (concluding that the assertion that the right of peoples to self-determination has an *erga omnes* character "is irreproachable"); Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 167, ¶ 156 (July 9).

[71] *See* Friendly Relations Declaration, *supra* note 15, pmbl. Similarly, Antonio Cassese's study of self-determination concluded that this provision applies broadly to "the whole population" of each State as opposed to the traditional context of a distinct group within a population attempting to create a new State. ANTONIO CASSESE, SELF-DETERMINATION OF PEOPLES: A LEGAL REAPPRAISAL 65 (1995).

[72] HUGO GROTIUS, ON THE LAW OF WAR AND PEACE 173 (Stephen C. Neff ed., Cambridge Univ. Press 2012) (1625).

[73] Phillip Marshall Brown, *The Rights of States Under International Law*, 26 YALE L.J. 85, 87 (1916).

[74] *Id.*

[75] *See* Ohlin, *supra* note 14, at 1594-1597.

character" either.[76] It would seem reasonable to require some degree of coercion or usurpation to be carried from the principle of non-intervention and applied in the principle of self-determination. Without some kind of legal litmus test, the principle of non-intervention will become meaningless, as it would be overtaken by a limitless principle of self-determination. In other words, if we were to rely on self-determination as an independent legal category subject to violation, we would have to also adopt, for the sake of maintaining consistency, a prescriptive policy which harmonizes the two principles.[77]

Rabble-rousing may further rise to the level of "subversive propaganda"—that is, communication "aimed at destabilizing State institutions by influencing nationals of another State towards insurrection, revolt, or civil strife."[78] Evidentiary issues will arise proving that each individual tweet or post constituted such subversion.[79] If subversion is established, it is well-settled in international law that such propaganda is prohibited. Vattel wrote as early as 1863 that it is "unlawful for Nations to do any act tending to create trouble in another state, to stir up discord, to corrupt its citizens, to alienate its allies."[80] UNGA Resolution 290 of 1949 on the "Essentials for Peace," which reflects custom, further calls on all nations "to refrain from any threats or acts, direct or indirect, aimed at . . . fermenting civil strife and subverting the will of the people."[81] Nonetheless, there are frequent violations of this rule as guilty States "find plenty of excuses for the communication complained of—denial that the offensive words had ever been uttered, claim that they were justified retaliation, reprisal, or self-defense, or that the communicator was not under the legal control of the State"[82] (as States generally deny extending the prohibition to communications made by private individuals).[83] Ultimately, the international law of propaganda seems to offer rhetorical promise but minimal avenues for practical international enforcement.

C. Rabble-Rousing and the Territorial Sovereignty

Rabble-rousing, in line with other information warfare and below the threshold of the use of force cyber tactics, triggers the question of the relevance and applicability of the principle of sovereignty. Then-UK Attorney General

---

[76] Daniel Thürer & Thomas Burri, *Self-Determination*, MAX PLANCK ENCYCLOPEDIA PUBL. INT'L L., https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e873 (last updated Dec. 2008).

[77] *See, e.g.*, Int'l Law Comm'n, Rep. on the Work of its Fifty-Eighth Session, U.N. Doc. A/61/10; GAOR, 61st Sess., Supp. No. 10 (2006) (describing the principle of harmonization in the following way: "when several norms bear on a single issue they should, to the extent possible, be interpreted so as to give rise to a single set of compatible obligations.").

[78] Eric De Brabandere, *Propaganda*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 10, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e978 (last updated Nov. 2012).

[79] *But cf.* the "accumulation of events" theory above discussed, *supra* note 65 and accompanying text.

[80] EMMERICH DE VATTEL, THE LAW OF NATIONS ¶ 18 (Chitty ed., 1863).

[81] GA Res. 290 (IV) at ¶ 3. For further reading on the customary nature of the prohibition on subversive propaganda, *see* Arthur Larson, *The Present Status of Propaganda in International Law*, 31 L. & CONT. PROBL. 439, 445-47 (1966).

[82] *See* John B. Whitton, *Hostile International Propaganda and International Law*, 398 ANN. AM. ACAD. POL. & SOC. SCI. 14, 18 (1971).

[83] *See* Eric De Brabandere, *supra* note 76, at ¶ 32.

Jeremy Wright made a statement in May 2018 about his Government's position on the application of the principle of territorial sovereignty in cyberspace. In his comments, Wright suggested that as a matter of international law it is not currently possible to extrapolate from the general principle of sovereignty "a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention."[84] In other words, Wright's position would seek to apply the same problematic set of tests of coercion and usurpation so to limit the scope of sovereignty violations in cyberspace. Nothing below those high standards could ever be considered a violation, certainly not mere acts of rabble-rousing. Wright's position runs counter to that of the international group of experts who drafted *Tallinn Manual 2.0*. They believe that a violation of sovereignty may occur in cases where a cyber attack results in a physical damage or loss of functionality, irrespective of issues of usurpation or coercion.[85] A minority of the experts even took the view that other forms of below-the-threshold cyber intrusions might violate sovereignty.[86] In so doing the drafters relied on the principle of respect for territorial sovereignty that was introduced by the ICJ in the *Nicaragua* case.[87]

This legal clash is a microcosm of a broader active debate in the literature as to whether all infringements upon sovereignty, even outside the cyber context, could ever trigger actual violations of international law.[88] A minority of scholars seem to take the view that the principle of sovereignty informs only primary rules of conduct, rather than itself operating as a binding legal rule.[89]

But even if we were to escape the threshold problem and adopt the majority view that sovereignty violations are internationally wrongful, there is still the unresolved debate around the proper application of territorial sovereignty in cyberspace. This is especially true considering that rabble-rousing rarely triggers any tangible and identifiable harm within the territory of the targeted State; rather, rabble-rousing seems to be involved in a far murkier gradual unraveling of social ties.

D. Rabble-Rousing and the Prohibition on Transboundary Harm

---

[84] *See* Jeremy Wright QC MP, *Cyber and International Law in the 21st Century*, GOV.UK (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. *Cf.* the recent statements by both the French and Dutch governments, adopting an opposite view on the application of the principle of sovereignty in cyberspace, as summarized here: Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis*, JUST SECURITY (Oct. 14, 2019), https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/; Michael Schmitt, *France's Major Statement on International Law and Cyber: An Assessment*, JUST SECURITY (Sept. 16, 2019), https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment.

[85] *See* TALLINN MANUAL 2.0, *supra* note 14, at 20.

[86] *See id*., at 21 (though none of the examples offered bear any resemblance to rabble-rousing).

[87] *See* Military and Paramilitary Activities, *supra* note 15, ¶ 251.

[88] The American Journal of International Law Unbound hosted a symposium on the topic in 2017. *See* Tom Ginsburg, *Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0*, 111 AM. J. INT'L L. UNBOUND 205 (2017).

[89] *See* Gary P. Corn and Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207 (2017).

Can rabble-rousing be considered a prohibited transboundary harm? Customary international law on the prevention of transboundary harm traces its origins to the *Trail Smelter* arbitration; there, the arbitral panel stated in dicta that "[n]o state has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence."[90] The *Trail Smelter* maxim, often referred to as the doctrine of *sic utere tuo ut alienum non laedas* ("use your property in such a way that you do not injure that of others"), was expanded upon by the ICJ in its *Corfu Channel* decision, in which it stated that it is "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[91]

While there is obvious appeal in trying to capture the illegality of rabble-rousing through the maxim of *sic utere*, the principle would rarely be applicable. This is because of reasons already illuminated: rabble-rousing does not always manifest itself in clearly identifiable and detectible harms, and even if it did, there would rarely be "clear and convincing evidence" to support the causal link between the perpetrating State, the online acts of rabble-rousing, and those alleged harms.

E. Rabble-Rousing and International Human Rights Law

At first glance, international human rights law (IHRL) would seem only to further complicate any attempts to articulate the dangers of rabble-rousing from a legal perspective. IHRL defines freedom of expression expansively. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) includes the "right to seek, receive and impart information and ideas of all kinds *regardless of frontiers*."[92] General Comment 34 of the Human Rights Committee, interpreting Article 19, is clear to extend the "frontiers" of expression to "every form of idea and opinion capable of transmission to others" including "all forms of . . . electronic and internet-based modes of expression."[93]

Because IHRL so firmly protects freedom of expression, it gives policy makers strong reason not to over-regulate rabble-rousing and other practices. Indeed, there are quite a number of think tanks and academic institutions, both progressive and libertarian, that share the view that government regulation of content moderation on social media is both dangerous and futile.[94]

---

[90] Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941).
[91] Corfu Channel Case (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 21-22 (Apr. 9).
[92] U.N. Human Rights Committee, General Comment No. 34: Freedoms of Opinion and Expression (Art. 19 of the ICCPR), U.N. Doc. CCPR/C/GC/34, ¶ 11 (Sept. 12, 2011) [hereinafter General Comment No. 34].
[93] *Id.*, ¶ 12.
[94] *See, e.g.*, John Samples, *Why the Government Should Not Regulate Content Moderation of Social Media*, CATO INST. (Apr. 9, 2019), https://www.cato.org/publications/policy-analysis/why-government-should-not-regulate-content-moderation-social-media; Niam Yaraghi, *Regulating Free Speech on Social Media is Dangerous and Futile*, BROOKINGS (Sept. 21, 2018), https://www.brookings.edu/blog/techtank/2018/09/21/regulating-free-speech-on-social-media-is-dangerous-and-futile.

However, analysis of the unique self-contradictory behavior of this practice opens the door for an argument as to what expressive value rabble-rousing has, if any. This allows us, at the end of this section, to make a paradigm shift away from a presumption against government action and creates the opportunity for States to freely take mitigating steps against rabble-rousing as needed.

Despite the expansiveness of the right to freedom of expression, it is equally "beyond doubt that both freedom of expression and freedom of information are not absolute."[95] Under the European Convention on Human Rights, for example, freedom of expression can be curtailed if necessary in a democratic society to protect other legitimate interests, including national security, territorial integrity, or public safety. In *Erbakan v. Turkey* (2006) the European Court of Human Rights acknowledged that it may be considered necessary "to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance . . . provided that any . . . 'restrictions' . . . are proportionate to the legitimate aim pursued."[96]

Still, the ruling concluded with the finding that the Turkish prime minister's speech emphasizing "division between 'believers' and 'non-believers'" did not present "a 'present risk' and an 'imminent danger.'" As a result, the criminal proceedings instituted as a result of those expressions were not "reasonably proportionate" and *did* constitute a violation of the European convention. Given that rabble-rousing does not explicitly or necessarily promote physical violence or ethnic tensions one might expect to encounter similar objections to attempts to limit it under existing IHRL.

Given our modern day understanding of disinformation, special attention is given to balancing the concern for its destabilizing effects with the inherent value of expression. In 2017, the Special Rapporteurs on Freedom of Expression and Opinion from the UN Human Rights Council (UNHRC), the Organization of American States (OAS) and the African Commission on Human and Peoples' Rights adopted a Joint Declaration on "Fake News," Disinformation and Propaganda. In the declaration, the Special Rapporteurs acknowledge both the risk that disinformation may "interfere with the public's right to know" and also the risk that "prohibitions on disinformation may violate international human rights standards [of freedom of expression]."[97]

Careful consideration of rabble-rousing's aggregate effect, however, leads one to question what expressive value rabble-rousing serves. In amplifying directly contradictory statements simultaneously, perhaps rabble-rousing is conceding that it is expressing nothing at all. Consider the NFL example for rabble-rousing provided in Part I. Each individual tweet or hashtag expresses an opinion for or against the act of NFL players kneeling in protest. Amplifying both tweets at once is to express neither support for, nor disapproval of, the

---

[95] Eric De Brabandere, *supra* note 78, ¶ 9.
[96] Erbakan v. Turkey, Eur. Ct. H.R., App. No. 59405/00, ¶ 56 (July 6, 2006).
[97] *See* Joint Declaration on "Fake News," *supra* note 10, at 1.

protesting athletes. It is logically irreconcilable to express both positions in one breath. Doing so is nothing more than an action with the function of emphasizing division amongst the individuals it reaches. Attempting to conduct two contradictory acts at once belies the operation's true intention to sow discord instead of expressing opinion.[98]

There is an inauthenticity to rabble-rousing that flows from this simultaneous expression of opposites. There is an indirect element of misrepresentation inherent in rabble-rousing when it is employed at the scale that can be achieved by a State-organized effort targeted at social media. The scale of the campaign may be too broad for any one citizen to comprehend with the evidence they are exposed to on their own. To some the perpetrating State, through its proxies, is expressing that it supports the kneeling players. To others that very State expresses that it supports the NFL. Both expressions are misleading because in actuality the State believes in neither. Therefore, each individual instance of amplification that constitutes an act of rabble-rousing is disingenuous.

Given the analysis of its contradictory nature, rabble-rousing does more than attach itself at the hip to the fate of the "fake news" and misinformation debate within international legal scholarship. So long as the two stances are irreconcilable opposites, a rabble-rouser's intent to sow discord is without ambiguity. This stands in contrast to the vast majority of misinformation and amplification cases online and elsewhere where it is impossible to truly separate the content's immediate act of expression (perhaps in support of a particular political position) from the content's higher-level purpose of fostering tension and division.

This Essay therefore opens the question of whether rabble-rousing deserves any protection at all under IHRL if we can determine conclusively that the intent is functional and not expressive. Rabble-rousing, as a form of speech, may not be *illegal* under modern-day IHRL, but the reasoning developed above suggests we should push the bounds of existing jurisprudence so to ensure that it's not *protected* either. Normally, restrictions on possibly malicious acts conducted via communication platforms are only allowed if they meet the high standard set to overcome freedom of expression concerns enshrined within Article 19.[99] If we consider excluding rabble-rousing from within Article 19's aura of protection, the door is opened for victim States themselves to prohibit this narrowly defined and carefully scoped practice as needed.

---

[98] *See Russian Trolls Are Flooding Social Media with Messages Meant to Increase Tensions in U.S.*, NPR (Feb. 21, 2018), https://www.npr.org/2018/02/21/587731730/russian-trolls-are-flooding-social-media-with-messages-meant-to-increase-tension.

[99] A clear three-part test has been established for restrictions on the freedom of expression: [1.] "the restrictions must be "provided by law"; [2.] they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3 ["respect of the rights or reputations of others;" "protection of national security, . . . public order, . . . public health or morals"]; and [3.] they must conform to the strict tests of necessity and proportionality." General Comment No. 34, *supra* note 92, at ¶ 22.

IV. RABBLE-ROUSING AND TECHNOLOGY: FIGHTING FIRE WITH FIRE?

International law, at least in its present state, does not offer a satisfying resolution to the problem of rabble-rousing. The principles of non-intervention, self-determination, and the protection of territorial sovereignty seem to fail to capture this phenomenon. Similarly, the prohibitions on subversive propaganda and transboundary harm offer more rhetorical than practical help in mitigating the risks associated with rabble-rousing. The human right to freedom of expression could evolve to deny protections to rabble-rousing speech, but such development has yet to occur. In the absence of sufficient legal responses, democracies around the world must look to non-legal measures to ensure the integrity of their electoral systems and civil societies and to actively mitigate the corrosive effects of operations such as rabble-rousing. This section explores how various technological approaches may be deployed to combat rabble-rousing tactics.

To understand what solutions might be effective, it is first necessary to understand how exactly technological transformations to our information landscape have enabled a phenomenon like rabble-rousing to arise in the first place.

Rabble-rousing is directly enabled by the radically transformed information and communication landscape that is dominant today thanks to the Internet and social media. Only a few years ago, the costs to speech were measured by the day for sending mail, by the dollar for costly international telephone calls, and by the years of experience needed to achieve a position lofty enough to command a wide audience. We are several worlds away from the modes in which public discourse took place a hundred years ago, when politicians stood on soap boxes and the possession of a printing press was the only way to reach the people on a mass scale.[100] It is impossible to imagine that rabble-rousing could take place under those conditions.

Today, on the other hand, the public activity and conversations of Internet users a world away are readily accessible making it straightforward for foreign actors to evaluate the cultural and societal divisions that are ripe for exploitation by rabble-rousing.[101]

Barriers to communication, whether they be speed, cost, reputation or publishing authorities, have been dramatically reduced, enabling anyone to reach a nationwide audience in a fraction of a second. Determined, well-resourced actors can flood forums for public discussion producing overwhelming amounts

[100] James A Dewar, *The Information Age and the Printing Press: Looking Backward to See Ahead*, RAND (1998), https://www.rand.org/content/dam/rand/pubs/papers/2005/P8014.pdf.
[101] Wasim Ahmed, *Using Twitter as a Data Source: An Overview of Social Media Research Tools*, LSE IMPACT BLOG (May 8, 2017), https://blogs.lse.ac.uk/impactofsocialsciences/2017/05/08/using-twitter-as-a-data-source-an-overview-of-social-media-research-tools-updated-for-2017.

of content to sway conversations in their favor.[102] Moreover, we have direct access to individuals through microtargeting technology refined for advertisement purposes.[103] As a result, State actors are well-equipped to influence different subsections of a target populace as required for rabble-rousing.

Anonymity shields online bad actors. Facebook and Google have given up on actively enforcing proper identification as simple as using one's "real" name.[104] Many online platforms for expression, including Reddit, Twitter and news site commenting services, do not require users to reveal their physical identities at all while expressing themselves online using these platforms. Clouded online identities allow rabble-rousing to dupe everyday Internet users into "perceiv[ing] a seemingly spontaneous groundswell of public opinion" and make formal attribution by law enforcement more difficult.[105]

Finally, there is evidence that the news feeds and curation algorithms, which are necessary to make sense of the overwhelming amount of online data available to Internet users, allow divisive, inflammatory content to spread even faster. Professor Zeynep Tufekci theorized that video recommendations made by YouTube lead its users to "content that is more extreme than what they started with — or to incendiary content in general."[106] Others have found that although most social media users are moderate, "[m]embers of a tiny but highly followed network core . . . post links to sources that are more politically extreme" and which "are responsible for the majority of tweets received overall due to their popularity and activity."[107] Simply put, "[s]ocial media platforms are vulnerable to trolling because they are designed to maximize engagement and sell ads, rather than provide structured deliberative forums."[108] This allows bad actors "[to] gain disproportionate influence in setting the agenda of public discussion by framing issues in controversial ways that may go viral."[109] This is fertile ground for rabble-rousing.

Ideas for practical solutions to overcome these vulnerabilities are hard to come by and successful implementations are even rarer. Research suggests that "[c]itizens with less digital literacy are less able to assess trustworthiness or origins of digital messaging and are more prone to manipulation," however there

---

[102] Andrew Roth, *Pro-Putin Bots are Dominating Russian Political Talk on Twitter*, WASH. POST (Jun. 20, 2017), https://www.washingtonpost.com/world/europe/pro-putin-politics-bots-are-flooding-russian-twitter-oxford-based-studysays/2017/06/20/19c35d6e-5474-11e7-840b-512026319da7_story.html.
[103] *See* TENOVE, *supra* note 42, at 19-22; Thomas B. Edsall, *Let the Nanotargeting Begin*, N.Y. TIMES (Apr. 15, 2012), https://campaignstops.blogs.nytimes.com/2012/04/15/let-the-nanotargeting-begin/; Natasha Singer, *'Weaponized Ad Technology': Facebook's Moneymaker Gets a Critical Eye*, N.Y. TIMES (Aug. 16, 2018), https://www.nytimes.com/2018/08/16/technology/facebook-microtargeting-advertising.html.
[104] Eva Galperin, *2011 in Review: Nymwars*, ELECTRONIC FRONTIER FOUND. (Dec. 26, 2011), https://www.eff.org/deeplinks/2011/12/2011-review-nymwars.
[105] *See* Nyst & Monaco, *supra* note 39, at 51.
[106] Zeynep Tufekci, *YouTube, the Great Radicalizer*, N.Y. TIMES (Mar. 10, 2018), https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.
[107] Jesse Shore et al., *Network Structure and Patterns of Information Diversity on Twitter*, MIS Q. 1 (2016).
[108] *See* TENOVE, *supra* note 42, at 41.
[109] *Id.*

are disagreements about what digital media literacy entails and what forms of education are most important.[110] Moreover, experts argue that putting the onus on individuals, instead of tech companies, ISPs, and governments, is misguided.[111]

Other scholars theorize that technology companies bear "the sole ability to curb the practice and effects of State-sponsored harassment campaigns" given their proximity to the problem and the rapid pace of technological advancement.[112] Potential steps include developing more robust capabilities to detect activity linked to "state-linked accounts" and "bots" and to make this activity readily identifiable by ordinary users.[113]

Some measures already taken by companies to curb unwanted and damaging content have been less than successful. For example, "fact checking bots, [and] algorithms that flag unreliable sources" potentially "amplif[ied]" the unwanted misinformation "and increased its potency."[114] Greater success was had by technology companies targeting the economic motives for producing unwanted content, such as Google and Facebook banning certain websites from their advertising services.[115]

Carefully engineered algorithmic curation can be effective at dampening unwanted content while still allowing high quality content to rise to the surface. In 2009, Reddit, the popular discussion website, released a new "Best" metric for sorting comments under its posts to ensure that comments made very early on in the discussion didn't get an unfair advantage.[116] Carefully crafting online forums for public discourse is a difficult but necessary exercise for any Internet platform.[117] Perhaps, there are similar metric changes to be made to dampen incendiary, divisive content and to boost more moderate online voices.

In the absence of, or alongside, any effective long-term solutions, States may have no option but to adapt by developing proactive institutions responsible for pushing back against manipulative information campaigns. When implemented incorrectly, such institutions may only add bureaucratic baggage to a system already inept at countering disinformation. The European Union's Rapid Alert System, an "ambitious effort" launched in 2019 to "sound alarms about Russian propaganda" and to provide an "an early-warning system" for

---

[110] *Id.* at 36-37.
[111] *Id.* at 38.
[112] *See* Nyst & Monaco, *supra* note 39, at 50.
[113] *Id.* at 51.
[114] *See* TENOVE, *supra* note 42, at 42.
[115] Nick Wingfield et al., *Google and Facebook Take Aim at Fake News Sites*, N.Y. TIMES (Nov. 14, 2016), https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html.
[116] Randall Munroe, *Reddit's New Comment Sorting System*, UPVOTED REDDIT BLOG (Oct. 15, 2009), https://redditblog.com/2009/10/15/reddits-new-comment-sorting-system.
[117] *See, e.g.*, Jennifer Forestal, *The Architecture of Political Spaces: Trolls, Digital Media, and Deweyan Democracy*, 111 AM. POL. SCI. REV. 149 (2017).

member States, has been derided for its inability to take any meaningful action.[118]

In the best case scenario, however, these institutions serve as powerful tools for nations to maintain a robust online presence and to proactively combat disinformation. In Finland, a country "unusually resistant to the wider information war waged by Moscow," officials believe that "their country's strong public education system, long history of balancing Russia, and a comprehensive government strategy allow it to deflect coordinated propaganda and disinformation."[119] In 2015, the Finish prime minister publicly acknowledged the problem of Russian information operations and created a program to train government officials in identifying and understanding disinformation.[120] Jed Willard, Director of the Franklin Delano Roosevelt Center for Global Engagement at Harvard, was hired to help develop this policy and training program for the Finnish government. In his words, "the best way to respond is less by correcting the information, and more about having your own positive narrative and sticking to it."[121]

Sweden adopted a similar strategy beginning in 2016. The Swedish Civil Contingencies Agency's task force for guarding against election interference was empowered to take decisive action and has trained thousands of government officials, political party members, journalists and election administrators on "spotting foreign influence campaigns."[122] Ahead of national elections in 2018 Sweden mailed twenty-page leaflets "resembling a wartime government communiqué" to its citizens educating them on Russian information operations that might interfere with the elections.[123] Moreover, the Swedish government has "a 24/7 line of communication with social-media companies" allowing government officials to "report fake pages or accounts" immediately.[124] Other States that have created institutions to proactively combat adverse information operations include Israel, Ukraine, Estonia, Latvia and Lithuania.[125]

---

[118] Matt Apuzzo, *Europe Built a System to Fight Russian Meddling. It's Struggling.*, N.Y. TIMES (July 6, 2019), https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html ("[A]n inside joke was circulating in Brussels about the Rapid Alert System: It's not rapid. There are no alerts. And there's no system.").

[119] Reid Standish, *Why Is Finland Able to Fend Off Putin's Information War?*, FOREIGN POLICY (Mar. 1, 2017), https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war.

[120] *Id.*

[121] *Id.*

[122] Chris Good, *Ahead of Election, Sweden warns its voters against Foreign Disinformation*, ABC NEWS (Sept. 8, 2018), https://abcnews.go.com/International/ahead-election-sweden-warns-voters-foreign-disinformation/story?id=57694373.

[123] *Id.*

[124] *Id.*

[125] Greg Keeley, *Combatting Russian Information Warfare—in the Baltics*, THE HILL (Apr. 9, 2018), https://thehill.com/opinion/technology/382245-combatting-russian-information-warfare-in-the-baltics; Shearlaw, *supra* note 39; Aliya Sternstein, *Estonia's Lessons for Fighting Russian Disinformation*, CHRISTIAN SCIENCE MONITOR (Mar. 24, 2017), https://www.csmonitor.com/World/Passcode/2017/0324/Estonia-s-lessons-for-fighting-Russian-disinformation.

V. CONCLUSIONS

This Essay lays the foundations for understanding the practice of rabble-rousing in order to ultimately limit the likelihood that it may be used to sow societal mistrust and to unravel the fabric that binds us together. Rabble-rousing is distinct from other cyber information operations due to its unique self-contradictory nature. This quality presents a distinct risk to democracies and the international world order, which depend on cooperation and the search for common understanding.

As is the case for amplification operations more generally, it is very difficult to find a plausible international legal lens through which the corrosive properties of rabble-rousing may be decisively viewed as prohibited. Nonetheless, even if rabble-rousing will be difficult to prohibit as a matter of law, there is reason to believe it should not be protected. The two-sided nature of rabble-rousing in the context of the human right to freedom of expression suggests that there is not much expressive value in the practice worthy of protection.

Rabble-rousing is made possible thanks to several distinct shifts in our information landscape at the hands of technological change. Given the lack of legal remedies, technological solutions may be necessary for States looking to combat rabble-rousing and mitigate its harmful effects.

This Essay opens up the possibility for more work along many different fronts. There are theoretical concerns, as international legal scholarship and international consensus-building is needed to account for the unique damaging properties of amplification operations in the digital age, including rabble-rousing. From a practical standpoint, all of this work will be for naught without focused studies concerning the efficacy of various technological strategies which seek to stave off rabble-rousing and other divisive information operations. These two agendas should be pursued in tandem, and theoreticians and technologists must work together to promote them.