ARTICLE

SUING RUSSIA:

HOW AMERICANS CAN FIGHT BACK AGAINST RUSSIAN INTERVENTION IN AMERICAN POLITICS

William J. Aceves[*]

ABSTRACT

The evidence of Russian intervention in American politics is overwhelming. In the midst of the 2016 US presidential campaign, a growing number of inflammatory social media posts addressing various political topics emerged on Facebook, Instagram, and Twitter. These posts supported the candidacy of Donald Trump, condemned the influx of refugees and migrants, and promoted racial divisions in the United States. Through clicks, likes, shares, and retweets, these messages reached millions of Americans. But, these messages did not originate in the United States; they were drafted and disseminated through inauthentic social media accounts created and controlled by the Internet Research Agency, an obscure foreign corporation with direct contacts to the Russian government. This propaganda campaign was part of Project Lakhta, a Russian operation designed to undermine American democracy.

In response, the US government filed criminal indictments against several Russian nationals and corporations implicated in Project Lakhta. Social media companies released thousands of files that document Russian intervention and purged many of these inauthentic accounts.

---

* William J. Aceves is the Dean Steven R. Smith Professor of Law at California Western School of Law. Gabor Rona offered helpful comments on earlier drafts of the manuscript. Andrea Alberico, Regina Calvario, Sara Emerson, Lillian Glenister, Warsame Hassan, Ash Kargaran, and Stacey Zumo provided excellent research assistance. All errors and opinions are the author's sole responsibility.

This Article proposes a different response—one that directly targets the Russian government. Because its actions violated numerous international norms, Russia is subject to proceedings before several international human rights bodies. And, significantly, these proceedings can be brought by the very people who were the targets of the Russian campaign—the American people.

I. INTRODUCTION

In the midst of the 2016 US presidential campaign, thousands of inflammatory social media posts emerged on Facebook, Instagram, and Twitter.[1] These posts supported the candidacy of Donald Trump and denounced Hillary Clinton, condemned the influx of refugees and migrants, and promoted racial divisions in the United States. Many used offensive stereotypes, virulent tropes, and violent imagery to convey their inflammatory messages. The messages were sent by social media accounts from several groups, including Secured Borders, Being

1. *See generally* Paul M. Barrett et al., NYU Stern Center, Combating Russian Disinformation: The Case for Stepping Up the Fight Online (2018); KATHLEEN HALL JAMIESON, CYBER-WAR: HOW RUSSIAN HACKERS AND TROLLS HELPED ELECT A PRESIDENT (2018); Paris Martineau, *How Instagram Became the Russian IRA's Go-To Social Network*, WIRED (Dec. 17, 2018), https://www.wired.com/story/how-instagram-became-russian-iras-social-network/ [https://perma.cc/K668-2RHM].

Patriotic, Heart of Texas, and Stop A.I. [All Invaders].[2] Through clicks, likes, shares, and retweets, these messages reached millions of Americans.[3] But, these messages did not originate in the United States; they were drafted and disseminated through inauthentic social media accounts controlled by the Internet Research Agency, an obscure foreign corporation with direct contacts to the Russian government.[4]

The work of the Internet Research Agency was part of a larger propaganda campaign authorized by the Russian government known as Project Lakhta.[5] Project Lakhta was designed to influence the 2016 US presidential campaign by supporting the candidacy of Donald Trump.[6]

---

2. Elizabeth Dwoskin, *How Russian Content Ended Up on Pinterest*, WASH. POST (Oct. 11, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/11/how-russian-content-ended-up-on-pinterest/?noredirect=on&utm_term=.10f3818ac6a8 [https://perma.cc/25XZ-WAB6]**;** Yochai Benkler et al., *Are the Russians Coming?*, *in* NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 235, 241 (Yochai Benkler et al. eds., 2018).

3. *See* Gillian Cleary, *Twitterbots: Anatomy of a Propaganda Campaign*, SYMANTEC (June 5, 2019), https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation [https://perma.cc/SR8U-8LBB]; Bruce Schneier, *Toward an Information Operations Kill Chain*, LAWFARE (Apr. 24, 2019), https://www.lawfareblog.com/toward-information-operations-kill-chain [https://perma.cc/Z8D2-LVPS].

4. *See generally* JONATHAN MASTERS, COUNCIL FOR. REL., RUSSIA, TRUMP, AND THE 2016 U.S. ELECTION (2018), https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election [https://perma.cc/PT8C-3LSQ]; April Glaser, *What We Know About How Russia's Internet Research Agency Meddled in the 2016 Election*, SLATE (Feb. 16, 2018), https://slate.com/technology/2018/02/what-we-know-about-the-internet-research-agency-and-how-it-meddled-in-the-2016-election.html [https://perma.cc/YLK7-R4ZK]; Krishnadev Calamur, *What is the Internet Research Agency?*, THE ATLANTIC (Feb. 16, 2018), https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/ [https://perma.cc/UF2B-8RYT]; David E. Sanger, *Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says*, N.Y. TIMES (Jan. 6, 2017), https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html [https://perma.cc/8CDC-V6FP].

5. Lee Ferran, *What you Need to Know About the Indictment on Russian Influence*, ABC NEWS (Feb. 20, 2019), https://abcnews.go.com/Politics/indictment-russian-influence/story?id=61147179 [https://perma.cc/4TWD-5KDB]; Charlie Osborne, *Project Lakhta: Russian National Charged with US Election Meddling*, ZDNET (Oct. 22, 2018), https://www.zdnet.com/article/russian-national-charged-with-us-election-meddling/ [https://perma.cc/GR6C-LRBW]; Sadie Gurman & Byron Tau, *U.S. Charges Russian With Trying to Influence 2018 Midterms*, WALL ST. J. (Oct. 19, 2018), https://www.wsj.com/articles/u-s-says-china-russia-iran-trying-to-intervene-with-elections-1539973093 [https://perma.cc/EH3C-4BEY]; Adam Goldman, *Justice Dept. Accuses Russians of Interfering in Midterm Elections*, N.Y. TIMES (Oct. 19, 2018), https://www.nytimes.com/2018/10/19/us/politics/russia-interference-midterm-elections.html [https://perma.cc/6W32-NFYK].

6. Scott Shane, *These Are the Ads Russia Bought on Facebook in 2016*, N.Y. TIMES (Nov. 1, 2017), https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html [https://perma.cc/3KQW-TETM]; Jane Mayer, *How Russia Helped Swing the Election for*

It was also designed to manipulate the US political system and undermine the democratic process.[7] And, it continued after the 2016 election, echoing the Trump administration's populist agenda.[8] In historical terms, this was a propaganda campaign; in modern terms, it was information warfare. Regardless of how it is captioned, Russia's online campaign was systematic, pernicious, and affected human rights in the United States on a massive scale.[9] It undermined the right of individuals to be free from racial and ethnic discrimination. It violated religious freedom and demeaned religious minorities. It also affected the right of individuals to vote and to hold opinions without interference.

In response, the US government has filed criminal indictments against several Russian nationals and corporations implicated in Project Lakhta.[10] These charges addressed violations of federal election laws, identity theft, foreign agent registration requirements, and conspiracy. The US military has also conducted cyber operations against the Internet Research Agency and other Russian targets.[11] Project Lakhta was even an integral part of Special Counsel Robert Mueller's investigation and subsequent report on Russian interference in the 2016 presidential election.[12] Legislation has been proposed in

---

Trump, THE NEW YORKER (Oct. 1, 2018), https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump [https://perma.cc/84DE-FPD8]; Scott Shane & Mark Mazzetti, *The Plot to Subvert an Election*, N.Y. TIMES (Sept. 20, 2018), https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html [https://perma.cc/8HPL-ALRS].

7. *See, e.g.*, Bruce Zagaris, *Russian Indicted for Cybercrime and Interfering with 2016 and 2018 Elections*, 34 INT'L ENF. L. REP. 561, 562 (2018).

8. *Id*. at 561.

9. *See infra* Pt IV.

10. *See, e.g.*, United States of America v. Elena Alekseevna Khusyaynova, No. 1:18-MJ-464, (E.D. Va. Sept. 28, 2018); United States of America v. Internet Research Agency, No. 18-cr-0032 (DLF), (D.D.C. Feb. 16, 2018).

11. Ben Buchanan, *What to Make of Cyber Command's Operation against the Internet Research Agency*, LAWFARE (Feb. 28, 2019), https://www.lawfareblog.com/what-make-cyber-commands-operation-against-internet-research-agency# [https://perma.cc/H9XK-LTUE]; Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html [https://perma.cc/YF9D-WTK5].

12. ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION (Mar. 24, 2019), https://www.documentcloud.org/documents/5955118-The-Mueller-Report.html

Congress to address Russian intervention.[13] In addition, social media companies have released thousands of files that document Russian intervention and have purged many of these inauthentic accounts.[14] They have also revised their policies to make it more difficult for foreign governments to undertake similar propaganda campaigns.[15]

This Article proposes a different response—one that directly targets the Russian government. This Article frames Russia's actions and the ensuing harms as human rights issues.[16] Because its actions violated numerous international norms, Russia is subject to

---

[https://perma.cc/UXJ6-YU8H] [hereinafter MUELLER REPORT]; Letter from William P. Barr, U.S. Att'y Gen., to the Hon. Lindsey Graham, Chairman, Comm. on the Judiciary, United States Senate, et al. (Mar. 24, 2019), https://www.npr.org/2019/03/24/706351394/read-the-justice-departments-summary-of-the-mueller-report [https://perma.cc/E6RJ-KMKR]. *See generally* David A. Graham, *No One Wants to Talk About Mueller's Most Definitive Conclusion*, THE ATLANTIC (May 30, 2019), https://www.theatlantic.com/ideas/archive/2019/05/no-one-wants-talk-about-muellers-most-important-conclusion/590674/ [https://perma.cc/TUT3-T8S7]. Alina Polyakova, *What the Mueller Report Tells Us About Russian Influence Operations*, BROOKINGS (Apr. 18, 2019), https://www.brookings.edu/blog/order-from-chaos/2019/04/18/what-the-mueller-report-tells-us-about-russian-influence-operations/ [https://perma.cc/XBV2-LW6E].

13. *See, e.g.*, Jordain Carney, *Senate Passes Bill to Deny Entry for Individuals Who Meddle in U.S. Elections*, THE HILL (June 3, 2019, 8:21 PM), https://thehill.com/blogs/floor-action/senate/446763-senate-passes-bill-to-deny-entry-for-individuals-who-meddle-in-us [https://perma.cc/5K3C-GW62].

14. Kelvin Chan, *Facebook Shuts Hundreds of Russia-Linked Pages, Accounts Over "Inauthentic Behavior,"* USA TODAY (Jan. 17, 2019), https://www.usatoday.com/story/tech/2019/01/17/facebook-shuts-down-hundreds-russia-linked-pages-accounts/2603319002/ [https://perma.cc/2SUT-LKKG]; Nicholas Fandos & Kevin Roose, *Facebook Identifies an Active Political Influence Campaign Using Fake Accounts*, N.Y. TIMES (July 31, 2018), https://www.nytimes.com/2018/07/31/us/politics/facebook-political-campaign-midterms.html [https://perma.cc/JQ85-ZYRF].

15. *See, e.g.*, Paresh Dave, *Facebook Defends Russia Response, Updates Plan to Curb Misbehavior*, REUTERS (Nov. 15, 2018), https://www.reuters.com/article/us-facebook-content/facebook-defends-russia-response-updates-plan-to-curb-misbehavior-idUSKCN1NK2MO [https://perma.cc/PTN5-Y8Q7].

16. *See* Scott J. Shackelford, *Should Cybersecurity Be a Human Right? Exploring the "Shared Responsibility" of Cyber Peace*, 55 STAN. J. INT'L L 155, 165 (2019); Carly Nyst & Nick Monaco, *State-Sponsored Trolling: How Governments are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, INST. FOR THE FUTURE, 46 (2018) available at http://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf [https://perma.cc/V22A-8W9T]; *Helsinki Summit: A Review of Vladimir Putin's Record of Human Rights Violations and Attacks on Democratic Institutions,* HUM. RTS. FIRST (July 18, 2018), available at https://www.humanrightsfirst.org/sites/default/files/factsheet-Putin-July-2018.pdf [https://perma.cc/H9ZF-7W3K]; Scott J. Shackelford, *Human Rights and Cybersecurity Due Diligence: A Comparative Study*, 50 U. MICH. J. L. REFORM 859, 860 (2017); Gabor Rona & Lauren Aarons, *State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace*, 8 J. NAT'L SECURITY L. & POL'Y 503, 504 (2016).

proceedings before several international human rights bodies.[17] These proceedings can overcome the unique challenges of cyber propaganda campaigns.[18] And, significantly, these proceedings can be brought by the very people who were the targets of the Russian campaign—the American people.[19]

In fact, there is no other viable mechanism for pursuing these claims against Russia. There is no indication the United States will pursue claims against Russia in any international tribunal. Some scholars have questioned whether Russia's actions even violate US sovereignty.[20] Other scholars have acknowledged the perceived shortcomings of international law and have proposed new regimes to address state liability in cyberspace.[21] Civil claims against the Russian government in US courts would face significant challenges, both for jurisdictional and substantive reasons. In the United States, civil proceedings against Russia would be governed by the Foreign Sovereign Immunities Act, and case law indicates such lawsuits would be unsuccessful.[22] While criminal indictments have been issued in the United States against the Internet Research Agency and several other

17. *Cf.* 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, 50 (2018) (proposing the need for an international response to address disinformation campaigns).

18. Kristen E. Eichensehr, *Decentralized Cyberattack Attribution*, 113 AM. J. INT'L L. UNBOUND 213, 217 (2019).

19. While this Article focuses on the ability of U.S. citizens (or permanent residents) to pursue claims against Russia, similar proceedings could be initiated by citizens of any country who are able to claim victim status.

20. Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30 (2018); Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1 (2017); Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579 (2017); William Banks, *State Responsibility and Attribution of Cyber Intrusions after* Tallinn 2.0, 95 TEX. L. REV. 1487, 1501 (2017).

21. *See* Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 637 (2018). *But see* Bjornstjern Baade, *Fake News and International Law*, 29 EUR. J. INT'L L. 1357, 1365 (2018) (arguing that the 1936 International Convention on the Use of Broadcasting in the Cause of Peace can offer mechanisms for addressing the modern challenges of "fake news").

22. 28 U.S.C. § 1602. *See, e.g.*, Democratic National Committee v. The Russian Federation, 2019 WL 3423536, at *1 (S.D.N.Y. 2019). *See generally* Doe v. Ethiopia, 851 F.3d 7 (D.C. Cir. 2017). *But see* Benjamin Kurland, *Sovereign Immunity in Cyberspace: Towards Defining a Cyber-Intrusion Exception to the Foreign Sovereign Immunities Act*, 10 J. NAT'L SECURITY L. & POL'Y 255, 263 (2019); Scott A. Gilmore, *Suing the Surveillance States: The (Cyber) Tort Exception to the Foreign Sovereign Immunities Act*, 46 COL. HUM. RTS. L. REV. 227, 233 (2015).

Russian entities, these proceedings do not directly involve the Russian government and may not be effective in deterring Russia's actions.[23] And, of course, the First Amendment would provide significant protection to speech-related activities in any civil or criminal proceedings in US courts.[24] Claims against the Russian government in Russia would also be futile.[25] Claims against US social media companies such as Facebook and Twitter would not address Russia's responsibility or hold it accountable.[26] Accordingly, international human rights bodies may offer the only viable mechanism for pursuing direct accountability against Russia.

II. THE INTERNET RESEARCH AGENCY AND PROJECT LAKHTA

The Internet Research Agency began operations in 2013 from a small building in the Primorsky district of St. Petersburg, Russia.[27]

---

23. *See* Chimène I. Keitner, *Attribution by Indictment*, 113 AM. J. INT'L L. UNBOUND 207, 208-09 (2019).

24. *See, e.g.*, Philip M. Napoli, *What If More Speech is No Longer the Solution: First Amendment Theory Meets Fake News and the Filter Bubble*, 70 FED. COMM. L.J. 55, 59 (2018); Erwin Chemerinsky, *False Speech and the First Amendment*, 71 OKL. L. REV. 1, 6 (2018); Louis W. Tompros et al., *The Constitutionality of Criminalizing False Speech Made on Social Networking Sites in a Post-Alvarez, Social Media-Obsessed World*, 31 HARV. J. L. & TECH. 65, 85 (2017); Brittany Vojak, *Fake News: The Commoditization of Internet Speech*, 48 CAL. W. INT'L L.J. 123, 144 (2017); Garrett Epps, *Does the First Amendment Protect Deliberate Lies?*, THE ATLANTIC (Aug. 16, 2016), https://www.theatlantic.com/politics/archive/2016/08/does-the-first-amendment-protect-deliberate-lies/496004/ [https://perma.cc/54M2-V58M].

25. In Russia, the nature of these claims and corruption within the judiciary ensure that such claims would be unsuccessful. *See generally* OLGA ROMANOVA, CARNEGIE MOSCOW CTR., THE PROBLEM WITH THE RUSSIAN JUDICIARY (2018), https://carnegie.ru/commentary/75316 [https://perma.cc/XZ5W-HUFE]; MARIA POPOVA, POLITICIZED JUSTICE IN EMERGING DEMOCRACIES: A STUDY OF COURTS IN RUSSIA AND UKRAINE (2012).

26. Moreover, there are significant hurdles in bringing such claims against social media companies. *See generally* Force v. Facebook, Inc., 304 F. Supp. 3d 315 (E.D.N.Y. 2018); Cohen v. Facebook, 252 F. Supp. 3d 140 (E.D.N.Y. 2017).

27. *See generally* April Glaser, *What We Know About How Russia's Internet Research Agency Meddled in the 2016 Election*, SLATE (Feb. 16, 2018), https://slate.com/technology/2018/02/what-we-know-about-the-internet-research-agency-and-how-it-meddled-in-the-2016-election.html [https://perma.cc/TA37-8274]; Polina Rusyaeva & Andrei Zakharov, *Investigation of RBC: How the "Factory of Trolls" Worked in the Elections in the United States*, RBC MAG. (Oct. 17, 2017), https://www.rbc.ru/magazine/2017/11/59e0c17d9a79470e05a9e6c1 [https://perma.cc/4GS8-4LPA]; Adrian Chen, *The Agency*, N.Y. TIMES MAG. (June 2, 2015), https://www.nytimes.com/2015/06/07/magazine/the-agency.html [https://perma.cc/4977-6GFL].

After an aggressive recruitment period, the Agency moved to a larger, four-story office building.[28] By 2015, the Agency employed hundreds of workers, most of whom were responsible for generating online content.[29] Workers were well-paid by Russian standards and were offered bonuses for excellent work as well as corresponding fines for underperformance.[30] According to its former employees, workers were required to post new content daily.[31] They worked twelve-hour shifts and were responsible for generating both new content as well as commenting on content drafted by other workers.[32] When engaged in online activity, workers would use an Internet proxy service to hide their IP addresses.[33] Content decisions were made by managers who reviewed web traffic and statistical reports to assess project impact. Workers would then receive detailed instructions on what issues to address.[34] While online contents initially focused on Russian topics—the war in Ukraine, Russian politics, and the economy—they soon began addressing US politics, including the 2016 presidential election.[35]

The Internet Research Agency operated as part of Project Lakhta, a broad-ranging Russian propaganda campaign.[36] Project Lakhta was

---

28. SETH HETTENA, TRUMP/RUSSIA: A DEFINITIVE HISTORY 191 (2018); Garrett M. Graff, *Inside the Mueller Indictment: A Russian Novel of Intrigue*, WIRED (Feb. 20, 2018), https://www.wired.com/story/inside-the-mueller-indictment-a-russian-novel-of-intrigue/ [https://perma.cc/5E4A-S3T2].

29. Rusyaeva & Zakharov, *supra* note 27. Neil MacFarquhar, *Inside the Russian Troll Factory: Zombies and a Breakneck Pace*, N.Y. TIMES (Feb. 18, 2018), https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html [https://perma.cc/DQ2U-RX63].

30. P.W. SINGER & EMERSON T. BROOKING, LIKE WAR: THE WEAPONIZATION OF SOCIAL MEDIA 111-149 (2017); Chen, *supra* note 27.

31. MacFarquhar, *supra* note 29.

32. SINGER & BROOKING, *supra* note 30, at 110-16.

33. Chen, *supra* note 27.

34. *Id*.

35. *See generally* DIANA PILIPENKO & TALIA DESSEL, CTR. FOR AM. PROGRESS, FOLLOWING THE MONEY: TRUMP AND RUSSIA-LINKED TRANSACTIONS FROM THE CAMPAIGN TO THE PRESIDENTIAL INAUGURATION (2018), https://cdn.americanprogress.org/content/uploads/2018/12/22043523/FollowTheMoney-report2.pdf [https://perma.cc/4F2T-DE76]; Julia Ioffe, *What Russian Journalists Uncovered About Russian Election Meddling*, THE ATLANTIC (Dec. 30, 2017), https://www.theatlantic.com/international/archive/2017/12/russia-hackers-journalism-press-freedom-troll-factory/549422/ [https://perma.cc/3L65-B8S2].

36. Lakhta is a historic area located in the Primorsky district of St. Petersburg. *See generally* Sadie Gurman & Byron Tau, *U.S. Charges Russian with Trying to Influence 2018 Midterms*, WALL ST. J. (Oct. 19, 2018), https://www.wsj.com/articles/u-s-says-china-russia-iran-trying-to-intervene-with-elections-1539973093 [https://perma.cc/EH3F-6PWY]; Garrett

designed to develop and spread misinformation campaigns on various issues, including misinformation on political candidates.[37] It operated with a multi-million dollar budget funded by Yevgeniy Viktorovich Prigozhin, a wealthy Russian executive with close connections to Vladimir Putin and the Russian government.[38] Specific funding for the Internet Research Agency was funneled through companies controlled by Prigozhin, including Concord Management and Consulting LLC.[39]

The connections between the Russian government and the propaganda campaign were identified in the January 2017 report—*Assessing Russian Activities and Intentions in Recent US Elections*—prepared by the Director of National Intelligence.[40] While the full report was highly classified, a shorter declassified report described Russian activities and intentions during the 2016 presidential elections. The declassified report revealed multiple actors within the Russian government were involved in ordering and managing the campaign. Significantly, the report indicated Russian President Vladimir Putin had ordered the propaganda campaign to target the US presidential election.[41] In addition, the report determined that Russia's intelligence services conducted cyber operations against targets associated with the 2016 election and that Russia's state-run propaganda machine contributed to the campaign.[42]

Russian connections were also recognized by the House Permanent Select Committee on Intelligence in its March 2018 report—*Report on Russia's Active Measures*.[43] The report described

---

M. Graff, *Russian Trolls are Still Playing Both Sides—Even with the Mueller Probe*, WIRED (Oct. 19, 2018), https://www.wired.com/story/russia-indictment-twitter-facebook-play-both-sides/ [https://perma.cc/83LM-YSAJ].

37. Criminal Complaint at 4, United States v. Khusyaynova, No. 1:18-MJ-464 (E.D. Va. Sept. 28, 2018).

38. Nick Allen & Rozina Sabur, *US Charges Russian Woman Elena Khusyavnova with Interfering in US Elections*, THE TELEGRAPH (Oct. 19, 2018), https://www.telegraph.co.uk/news/2018/10/19/us-charges-russian-womanelena-khusyaynova-interfering-us-elections/ [https://perma.cc/P4T8-5EED].

39. Khusyaynova Criminal Complaint, *supra* note 37, at 4-5.

40. OFFICE OF THE DIR. OF NAT'L INTELL., ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (2017) [hereinafter 2017 NATIONAL INTELLIGENCE REPORT].

41. *Id.* ii.

42. *Id*. ii-iii.

43. HOUSE PERM. SELECT COMM. ON INTELL., REPORT ON RUSSIA'S ACTIVE MEASURES (2018), https://www.hsdl.org/?view&did=809811 [https://perma.cc/PH35-R5HP] [hereinafter HPSCI REPORT].

the campaign as multi-faceted and designed to affect the United States.[44]

> The Russian active measures campaign against the United States was multifaceted. It leveraged cyberattacks, covert platforms, social media, third-party intermediaries, and state-run media. Hacked material was disseminated through this myriad network of actors with the objective of undermining the effectiveness of the future administration. This dissemination worked in conjunction with derisive messages posted on social media to undermine confidence in the election and sow fear and division in American society.[45]

The Committee confirmed that Russia's social media posts were generated "to promote divisive social and political messages across the ideological spectrum."[46] The Senate Select Committee on Intelligence ("SSCI") issued a similar report establishing an explicit connection between the Russian government and the propaganda campaign.[47]

The details of Project Lakhta, as well as the connections between the Internet Research Agency and the Russian government, were described in two federal criminal filings. On February 16, 2018, the Justice Department filed a criminal indictment against the Internet Research Agency, Concord Management & Consulting, Concord Catering, Yevgeniy Prigozhin, and twelve other Russian nationals.[48] The indictment alleged the defendants were foreign agents engaged in a conspiracy to influence the US elections.[49] The Internet Research Agency was described as a Russian organization "engaged in operations to interfere with elections and political processes."[50] Concord Management & Consulting and Concord Catering were

---

44. *Id.* at 11-37.

45. *Id.* at 2.

46. *Id.* at 33.

47. SENATE SELECT COMM. ON INTELL., THE INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS (2018), https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf [https://perma.cc/KK34-8BPS] [hereinafter SSCI REPORT]. The SSCI released a highly redacted follow-up report in July 2019. SENATE SELECT COMM. ON INTELL., REPORT ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION (2019), https://assets.documentcloud.org/documents/6214172/Senate-Intelligence-Committee-report-on-Russian.pdf [https://perma.cc/G8T5-B3G40].

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

49. *Id*. at 4.

50. *Id.* at 2.

identified as Russian corporations connected to the Russian government. Collectively, these entities were part of Project Lakhta, which was described as a foreign interference operation targeting the United States and other countries.[51]

On September 28, 2018, the Justice Department filed a criminal complaint against a Russian national, Elena Khusyaynova, for her alleged role as the Chief Accountant for Project Lakhta.[52] The complaint described Project Lakhta as a plan to engage in "information warfare against the United States of America" by creating "fictitious social media personas, pages, and groups designed to attract US audiences and to address divisive US political and social issues."[53] According to the complaint, Khusyaynova "managed the budgeting and payment of expenses associated with social media operations, web content, advertising campaigns, infrastructure, salaries, travel, office rent, furniture, and supplies, and the registration of legal entities used to further Project Lakhta activities."[54]

The Khusyaynova complaint provided numerous examples of how Project Lakhta's social media campaign was designed "to sow division and discord in the U.S. political systems."[55] It described how some posts sought to promote social unrest over race and social justice issues. For example, the following image was posted on the Facebook account of "Rachell Edison," an inauthentic social media account created through Project Lakhta.[56] It was designed to gain support from

51. *Id.* at 6-7.

52. Press Release, Dep't of Justice, Russian National Charged with Interfering in U.S. Political System (Oct. 19, 2018), https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system [https://perma.cc/5LB6-GN8N]. While the complaint was filed on Sept. 28, 2018, it remained sealed until Oct. 19, 2018.

53. Criminal Complaint at 6, United States v. Khusyaynova, No. 1:18-MJ-464 (E.D. Va. Sept. 28, 2018).

54. *Id*. at 5.

55. *Id*. at 6.

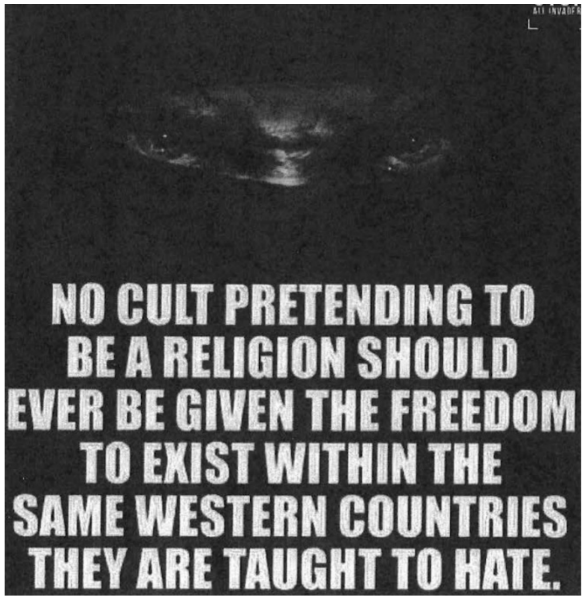
56. *Id*. at 23.

individuals who criticized the Black Lives Matter movement and similar groups opposed to police violence.[57]

The post included the following comments: "Whatever happens, blacks are innocent. Whatever happens, it's all guns and cops. Whatever happens, it's all racists and homophobes. Mainstream Media."[58]

Other social media posts targeted religious minorities for discrimination. This Facebook post appeared on the Facebook account of "Bertha Malone," another inauthentic account created through Project Lakhta.[59] Its text indicates that it was designed to gain support from individuals who were critical of Islam and Muslims.

57. *Id*.
58. *Id*.
59. *Id*. at 31.



The post included the following comment: "Damn right! And we all know which cult we need to kick out of America."[60]

In addition, social media posts targeted foreign nationals for discriminatory treatment. The following post also appeared on the "Bertha Malone" Facebook page.[61] Its text indicates that it was designed to gain support from individuals who were critical of immigrants.

60. *Id*.
61. *Id*. at 29.

This post included the following comment: "Stop separating families! Deport them all, including their anchor babies! And spend saved money on Americans who really need it, for example our homeless Vets."[62]

Because Project Lakhta operated through social media, there is an extensive record of its operations. Each of the affected social media companies—Facebook, Twitter, and Google—have released some of this information to the general public.[63] They have also released additional information to the US government, including the Senate Select Committee on Intelligence. In 2018, the SSCI shared this data with two private research groups, the Computational Propaganda Research Project and New Knowledge, in order to generate an independent assessment of the Russian social media campaign.[64] These groups released their reports in December 2018. According to SSCI Chair Richard Burr, "[t]his newly released data demonstrates how aggressively Russia sought to divide Americans by race, religion and ideology, and how the IRA actively worked to erode trust in our

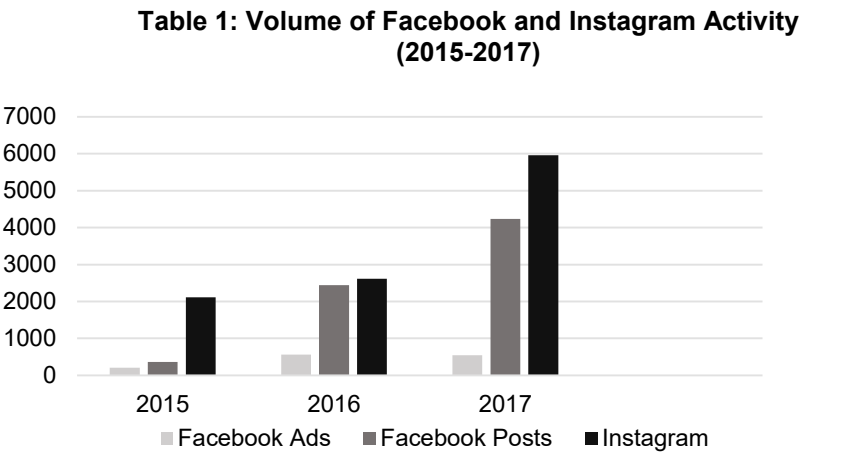
62. *Id*.

63. *See, e.g.*, *How Are We Working to Protect Election Security on Facebook?,* FACEBOOK (last visited Oct. 10, 2019), https://www.facebook.com/help/1991443604424859 [https://perma.cc/DX2R-NMAD]; Elias Groll, *Zuckerberg: We're in an "Arms Race" with Russia and AI Will Save Us*, FOR. POL'Y (Apr. 10, 2018), https://foreignpolicy.com/2018/04/10/zuckerberg-facebook-were-in-an-arms-race-with-russia-but-ai-artificial-intelligence-will-save-us/ [https://perma.cc/7SRH-DV52].

64. The Computational Propaganda Research Project is affiliated with Oxford University, and New Knowledge is a private cybersecurity company.

democratic institutions. Most troublingly, it shows that these activities have not stopped."[65] SSCI Vice Chair Mark Warner echoed this assessment, noting that "[t]hese reports demonstrate the extent to which the Russians exploited the fault lines of our society to divide Americans in an attempt to undermine and manipulate our democracy. These attacks against our country were much more comprehensive, calculating and widespread than previously revealed."[66]

The report prepared by the Computational Propaganda Research Project provided extensive details regarding the breadth of the social media campaign. Table 1 describes the volume of social media activity within Facebook and Instagram generated by the Internet Research Agency between 2015 and 2017.[67]



Facebook ads and posts are listed separately because they reflect distinct methods for disseminating information to users. According to

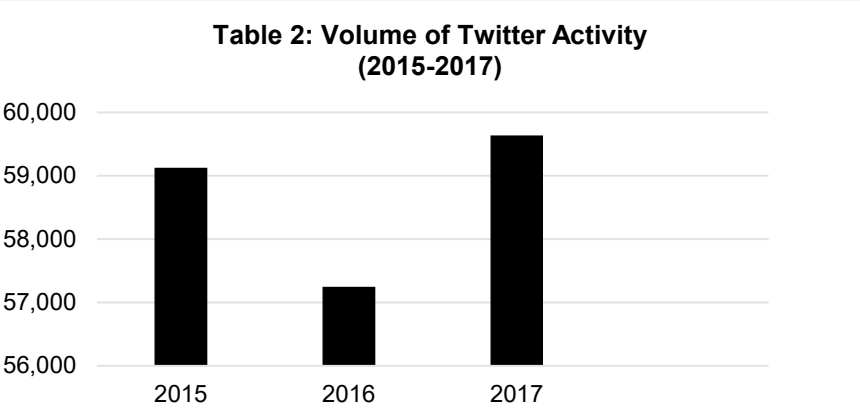
65. Press Release, Intelligence Committee, New Reports Shed Light on Internet Research Agency's Social Media Tactics (Dec.17, 2018), https://www.intelligence.senate.gov/press/new-reports-shed-light-internet-research-agency's-social-media-tactics [https://perma.cc/99Z3-PT2L].

66. *Id*.

67. PHILIP N. HOWARD ET AL., COMPUTATIONAL PROPAGANDA RESEARCH PROJECT, THE IRA, SOCIAL MEDIA AND POLITICAL POLARIZATION IN THE UNITED STATES, 2012-2018, at 5 (2018). In Table 1, the first column from the left indicates the number of Facebook ads; the second column from the left indicates the number of Facebook posts; the third column from the left indicates Instagram activity.

this data, social media activity increased significantly between 2015 and 2017. In fact, it peaked after the 2016 presidential election.

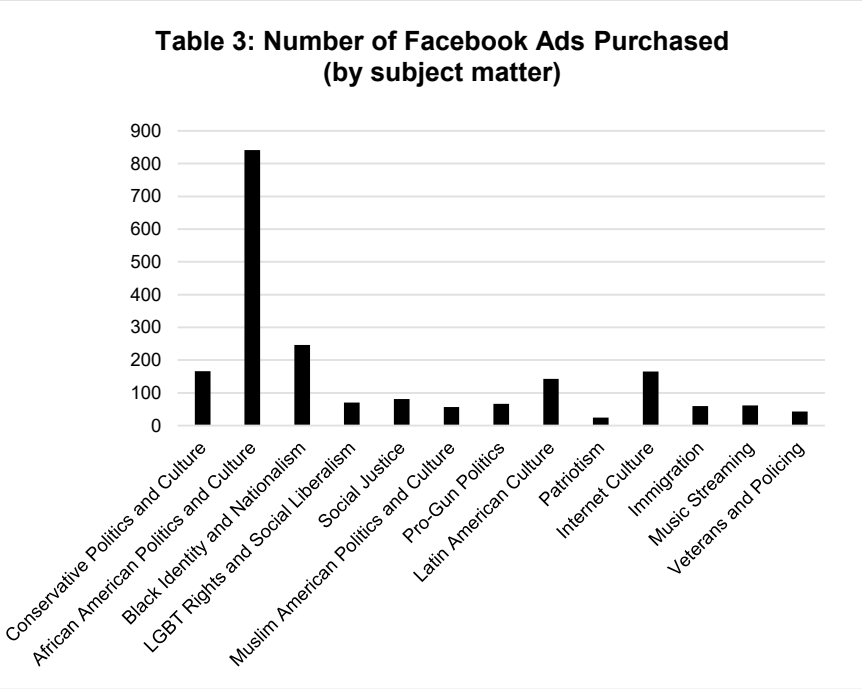
Table 2 describes the volume of social media activity on Twitter generated between 2015 and 2017.[68] Twitter's functionality allowed for more extensive messaging than Facebook or Instagram.



The Computational Propaganda Research Project determined that Project Lakhta sought to generate conflict and division in American society. It did so in several ways. First, it encouraged African American voters to boycott the presidential elections or follow the wrong voting procedures.[69] Second, it encouraged right-wing voters to be more extreme and confrontational.[70] And third, it spread "sensationalist, conspiratorial, and other forms of junk political news and misinformation to voters across the political spectrum."[71]

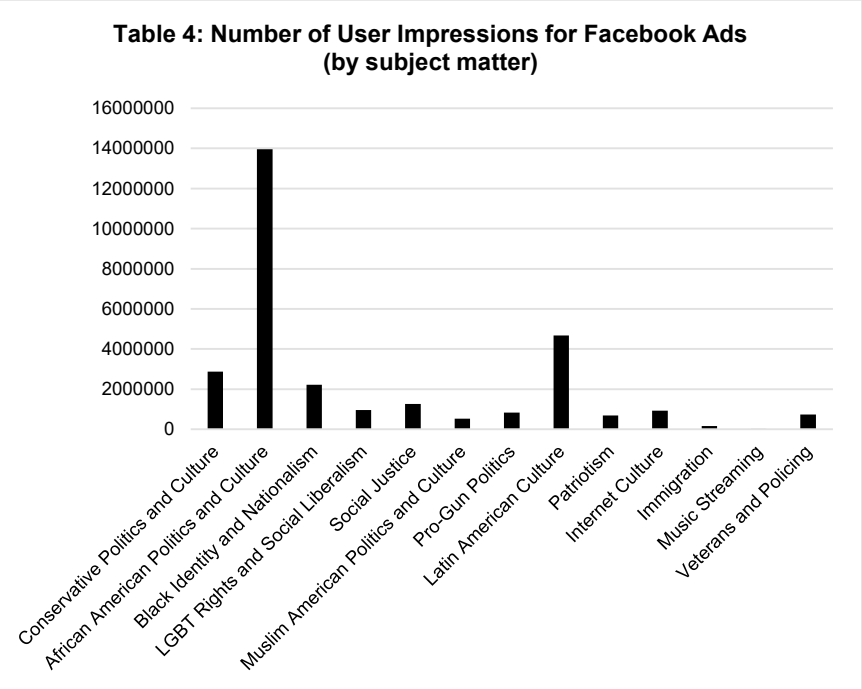
Table 3 identifies the top thirteen issue areas for Facebook ads purchased by the Internet Research Agency.[72] As evidenced in the data, the largest number of ad purchases involved the subject of race.

68. *Id*. at 5.
69. *Id*. at 3.
70. *Id*.
71. *Id*.
72. *Id*. at 23.



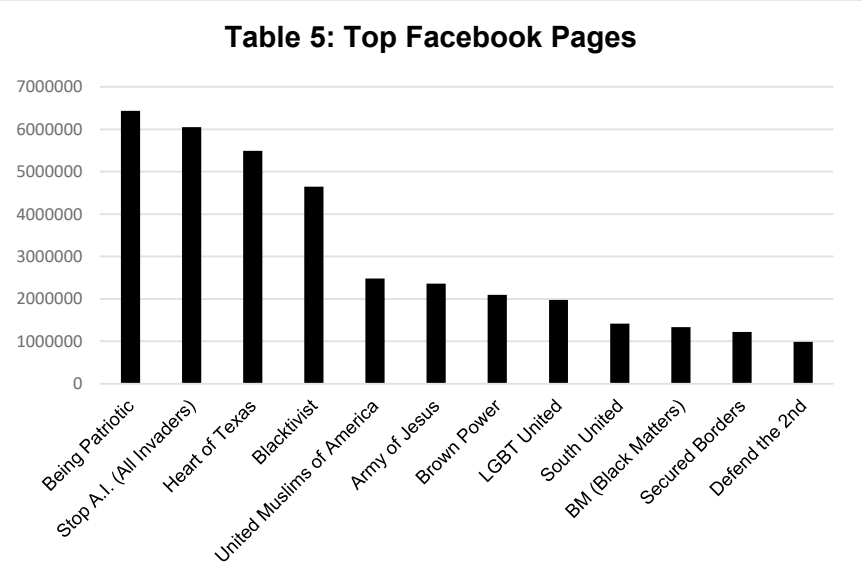
While Table 3 identifies the number of Facebook ads purchased, Table 4 indicates the impact of these ads. Specifically, it identifies the number of user impressions for these pages.[73] The most popular ads, as reflected in user impressions, were also related to race.

73. *Id*. at 23. A user impression represents the number of ad placements on a user's computer, tablet, or telephone.



Finally, Table 5 presents the top twelve Facebook pages created by the Internet Research Agency.[74] Many of these pages focused on race and minority groups, including Blacktivist, Black Matters ("BM"), Brown Power, and United Muslims of America.[75] A significant number, including the top three Facebook pages, were openly critical of minority groups and several supported white nationalism.[76]

74. *Id*. at 35.
75. *Id*. at 33-35.
76. *Id*.



The 2018 report prepared by New Knowledge confirmed that the Russian government, through the Internet Research Agency, orchestrated a massive and targeted social media campaign against the United States.[77] The report highlights the following key points:

- Social media operations targeted prominent political figures.
- There were extensive anti-Hillary Clinton operations.
- There was a clear bias for Donald Trump.
- Operations promoted both secessionist and insurrectionist movements in the United States to sow discord at the local, state, and federal levels.
- Operations promoted voter suppression.
- Operations targeted the African American community.[78]

Significantly, the report indicated that Russia's efforts are ongoing.[79]

In March 2019, Special Counsel Robert Mueller released his long-awaited *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. The report is unequivocal that "[t]he

77. RENEE DIRESTA ET AL., NEW KNOWLEDGE, THE TACTICS AND TROPES OF THE INTERNET RESEARCH AGENCY 3 (2018).

78. *Id*. at 7-10.

79. *Id*. at 7, 99.

Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[80] It refers to the Russian interference operations as "active measures" (активные мероприятия), which is "a term that typically refers to operations conducted by Russian security services aimed at influencing the course of international affairs."[81] While significant portions of the Mueller report were redacted, the released material highlights the connections between the Internet Research Agency and the Russian government.[82] The report described the structure of the Internet Research Agency and its funding and oversight.[83] It provided detailed descriptions of the Internet Research Agency's social media campaign, which included active measures using Facebook, Twitter, YouTube, Instagram, and Tumblr.[84] It also described the connections between Concord Management & Consulting and the Russian government.[85] While the Mueller report clearly establishes the Russia connection, the US government has been forced to be more circumspect in describing this connection due to pending litigation involving Concord Management.[86]

In sum, there is clear evidence of direct connections between the Russian government, Project Lakhta, and the Internet Research Agency. Significantly, these connections reveal that Project Lakhta was initiated and directed by Russian political leadership and its intelligence community.

III. RUSSIA'S RESPONSIBILITY FOR PROJECT LAKHTA

Under international law, state responsibility only exists for actions that can be attributed to state actors.[87] There are several ways in which attribution can be established, and these principles are set forth in the Articles on State Responsibility prepared by the International Law

80. MUELLER REPORT, *supra* note 12, at 1.
81. *Id*. at 14.
82. *Id*. at 1, 4, 9, 14.
83. *Id*. at 15-19.
84. *Id*. at 19-35.
85. *Id*. at 14, 16-19.
86. United States v. Concord Mgmt. & Consulting LLC, No. 18-cr-32-2 (DLF) slip op. at 3 (D.D.C. July 1, 2019).
87. *See generally* Helmut Philipp Aust, Complicity and the Law of State Responsibility (2011); James Crawford et al., The Law of International Responsibility (2010).

Commission.[88] For example, attribution is established when a state organ "exercises legislative, executive, judicial or any other function."[89] In other words, the actions of government entities can give rise to state responsibility under international law. In addition, the conduct of persons or entities that are exercising elements of governmental authority can be considered acts of the state even if these persons or entities are not state organs.[90] Attribution also exists "if a person or group of persons is in fact acting on the instruction of, or under the direction or control of, that State in carrying out the conduct."[91] And even when the conduct is not otherwise attributable to a state under these principles, such conduct may still be attributable when the state "acknowledges and adopts the conduct in question as its own."[92]

International law also recognizes that states must adhere to the principle of due diligence and the obligation to prevent transboundary harm.[93] It is a basic precept of customary international law that can be traced to the seminal *Trail Smelter* arbitration decision, which noted that a state "owes at all times a duty to protect other states against injurious acts by individuals from within their jurisdiction."[94] It was reaffirmed by the International Court of Justice in the *Corfu Channel* case, where the Court held that states must not knowingly allow their "territory to be used for acts contrary to the rights of other States."[95] This is a duty of prevention that informs the analysis of attribution for harm that emanates from a state's territory. Thus, a state may be held responsible for acts occurring in its territory that it knew about, or should have known about, and "failed to take appropriate steps."[96]

88. Int'l Law Comm'n, Rep. on the Work of Its Fifth-Third Session, U.N. Doc. A/56/10 (2001) [hereinafter SR Articles]; *see generally* JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART (2013).

89. SR Articles, *supra* note 88, art. 4.

90. *Id*. art. 5.

91. *Id*. art. 8.

92. *Id*. art. 11.

93. *See generally* DUNCAN FRENCH & TIM STEPHENS, ILA STUDY GROUP ON DUE DILIGENCE IN INTERNATIONAL LAW (FIRST REPORT) (2014); Robert P. Barnidge, Jr., *The Due Diligence Principle under International Law*, 8 INT'L COMM. L. REV. 81 (2006); Riccardo Pisillo-Mazzeschi, *The Due Diligence Rule and the Nature of the International Responsibility of States*, 35 GERM. Y.B. INT'L L. 9 (1992).

94. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (Perm. Ct. Arb. 1941).

95. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

96. Diplomatic and Consular Staff (United States v. Iran), Judgment, 1980 I.C.J. 3, 31-32 (May 24).

Accordingly, states may be held responsible for harms that emanate from their own territory even if they did not authorize such harms.[97]

While attribution for acts in cyberspace poses some unique challenges, these principles are equally applicable in the virtual world.[98] In fact, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare applies the principles of state responsibility and attribution to cyber operations.[99] While the Tallinn Manual 2.0 is not a legally binding document, it offers a contemporary application of traditional state responsibility and attribution rules to cyber operations. It does so in several ways. Consistent with the Articles on State Responsibility, the Tallinn Manual 2.0 indicates that cyber operations conducted by state organs, or by non-state actors that functioned under state direction or control, are attributable to that state.[100] Cyber operations conducted by a non-state actor are attributable to a state if such operations were engaged in "pursuant to its instructions or under its direction or control" as well as if the state "acknowledges and adopts the operations as its own."[101]

At a broader level, the Tallinn Manual 2.0 recognizes the due diligence principle.[102] Accordingly, "[a] State must exercise due

97. *See generally* Beatrice A. Walton, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law*, 126 YALE L.J. 1460 (2017); Russell Buchan, *Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm*, 21 J. CONFLICT & SEC. L. 431 (2016).

98. *See generally* Berenice Boutin, *Shared Responsibility for Cyber Operations*, 113 AM. J. INT'L L. 197 (2019); Barrie Sander, *Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections*, 18 CHINESE J. INT'L L. 1 (2019); OFF. DIR. NAT'L INTELL., A GUIDE TO CYBER ATTRIBUTION (2018); Crootof, *supra*, note 21, at 572; Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169 (2017); Jon R. Lindsay, *Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack*, 1 J. CYBERSECURITY 53 (2015); Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481 (2015).

99. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 17 (2017) [hereinafter TALLINN MANUAL 2.0]. *See generally* Dan Efrony & 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); Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. INT'L L.J. 735 (2017).

100. TALLINN MANUAL 2.0, *supra* note 99, at 87, 94 (Rule 15 – Attribution of cyber operations by State organs).

101. *Id*. at 94 (Rule 17 – Attribution of cyber operations by non-State actors).

102. Some commentators have argued the Tallinn Manual 2.0 did not go far enough in applying the principle of due diligence to cyber operations. *See* Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 INT'L & COMP. L.Q. 643 (2018). This is, in fact, a highly disputed area. *See, e.g.*, Eric Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer*, 95 TEX. L. REV. 1555 (2017); Peter Margulies,

diligence in not allowing its territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[103] Significantly, the Tallinn Manual 2.0 also recognizes that "international human rights law is applicable to cyber-related activities."[104] In such cases, "a State must: (a) respect the international human rights of individuals; and (b) protect the human rights of individuals from abuse by third parties."[105]

There is overwhelming evidence that Russia conducted a sophisticated campaign to influence the US political system in connection with the 2016 presidential election and, more broadly, to undermine the democratic process in the United States.[106] Russian involvement in the social media campaign was first identified by the Director of National Intelligence in the January 2017 report, *Assessing Russian Activities and Intentions in the Recent US Elections*.[107] In its March 2018 *Report on Russia's Active Measures*, the House Permanent Select Committee on Intelligence concurred with the earlier assessments of the intelligence community and found them "to be based on compelling facts and well-reasoned analysis."[108] These findings were echoed in the July 2018 report of the Senate Select Committee on Intelligence, which also supported the intelligence community's assessment and findings on Russian involvement.[109]

The February 2018 federal indictment of the Internet Research Agency provides more details on the role of the Russian government.[110] It described how corporations with direct connections to the Russian government provided funding to the Internet Research Agency.[111] It also described how these organizations sought to hide their Russian connections. In addition to the Internet Research Agency, several

---

Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, 14 MELB. J. INT'L L. 496 (2013).

103. TALLINN MANUAL 2.0, *supra* note 99, at 30 (Rule 6 – Due diligence (general principle)).

104. *Id*. at 182 (Rule 34 – Applicability).

105. *Id*. at 196 (Rule 36 – Obligations to Respect and Protect International Human Rights); *see also* Rona & Aarons, *supra* note 16, at 503.

106. *See supra* Part II.

107. 2017 NATIONAL INTELLIGENCE REPORT, *supra* note 40, at ii-iii.

108. HPSCI REPORT, *supra* note 43, at 22.

109. SSCI REPORT, *supra* note 47, at 1.

110. Indictment at 2-4, United States v. Internet Research Agency L.L.C., No. 1:18-cr-00032-DLF, (D.D.C. Feb. 16, 2018).

111. *Id*. at 6.

individuals with close contacts to Vladimir Putin were also indicted for their role in the social media campaign.[112] The October 2018 federal indictment of Elena Khusyaynova offered even more details on the Russian connection to Project Lakhta and the work of the Internet Research Agency.[113]

Under international law, Project Lakhta and the actions of the Internet Research Agency are attributable to Russia. These operations were directly authorized by President Putin and the Russian government.[114] Thus, they can be attributed to Russia because the Internet Research Agency was acting under Russia's direction and control. As noted by the International Law Commission, "[t]he attribution to the State of conduct in fact authorized by it is widely accepted in international jurisprudence."[115] This principle is reiterated in the Tallinn Manual 2.0, which indicates that cyber operations conducted by a non-state actor are attributable to a state if such operations were conducted "pursuant to its instructions or under its direction or control" as well as if the state "acknowledges and adopts the operations as its own."[116] Because Project Lakhta was specifically authorized by the Russian government, it is irrelevant that the Internet Research Agency is a private corporation or that it may have operated outside the official structure of the Russian government.[117] Russia can also be held responsible for failing to comply with the principle of due diligence and the prevention of transboundary harm.[118]

The Russian government has denied any connections to Project Lakhta or the Internet Research Agency. Elena Khusyaynova has not

---

112. Neil MacFarquhar, *Oligarch Tied to Troll Factory Earned Nickname "Putin's Cook*," N.Y. TIMES, (Feb. 16, 2018), https://www.wral.com/meet-yevgeny-prigozhin-the-russian-oligarch-indicted-for-interfering-in-the-u-s-elections/17347516/ [https://perma.cc/ECE7-R7J9].

113. Criminal Complaint at 4-5, United States v. Khusyaynova, No. 1:18-MJ-464 (E.D. Va. Sept. 28, 2018).

114. 2017 NATIONAL INTELLIGENCE REPORT, *supra* note 40, at ii; *see also* Calamur, *supra* note 4.

115. INTERNATIONAL LAW COMMISSION, DRAFT ARTICLES ON RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, WITH COMMENTARIES 47 (2008).

116. TALLINN MANUAL 2.0, *supra* note 99, at 94 (Rule 17 – Attribution of Cyber Operations by Non-State Actors).

117. Applying the principles of the Tallinn Manual 2.0 reinforces this conclusion because Russia failed to comply with the due diligence principle. It allowed the Internet Research Agency to function within its territory and to engage in cyber operations that affected "the rights of, and produce[d] serious adverse consequences" for the United States. TALLINN MANUAL 2.0, *supra* note 99, at 30.

118. *See* Crootof, *supra* note 21, at 571-73.

responded to the criminal charges brought against her, although this is not surprising since she is in Russia and unlikely to be extradited to the United States.[119] In contrast, Concord Management and Consulting has vigorously defended itself and has challenged its federal indictment on multiple grounds.[120]

IV. SUING RUSSIA

Russia has ratified several international agreements that require it to respect human rights. These include the Convention on the Elimination of all Forms of Racial Discrimination ("CERD"), the International Covenant on Civil and Political Rights ("ICCPR") as well as its Optional Protocol, and the European Convention on the Protection of Human Rights and Fundamental Freedoms ("ECHR").[121]

---

119. Quinta Jurecic, *Where in the World is Elena Khusyaynova?*, LAWFARE, Oct. 26, 2018, https://www.lawfareblog.com/where-world-elena-khusyaynova [https://perma.cc/U48H-R6ND]. Soon after she was indicted, Khusyaynova appeared on a Russian media outlet to deny the allegations and profess her innocence.

120. *See, e.g.*, United States v. Concord Management & Consulting LLC, 2019 WL 2247792 (D.D.C. 2019); United States v. Concord Management & Consulting LLC, 347 F. Supp. 3d 38 (D.D.C. 2018); United States v. Concord Management & Consulting LLC, 317 F. Supp. 3d 598 (D.D.C. 2018). A Russian media company has even filed a civil lawsuit against Facebook alleging several causes of action arising out of Facebook's decision to delete its account and online presence. Federal Agency of News LLC v. Facebook Inc., Case No. 5:18-cv-07041-SVK (N.D. Cal. 2018). The Federal Agency of News ("FAN") is a Russian corporation located in St. Petersburg, Russia. Its lawsuit alleges violations of the First Amendment, federal and state civil rights laws, breach of contract, and breach of the implied covenant of good faith and fair dealing. *Id*. at 10-18. While FAN has been linked to Project Lakhta and the Internet Research Agency, the complaint firmly rejected any such connections. Kartikay Mehrotra, *Facebook's Fake News War Has Russian Site Crying Censorship*, BLOOMBERG, (Nov. 20, 2018), https://www.bloomberg.com/news/articles/2018-11-20/facebook-is-sued-by-russian-news-agency-over-blocked-account [https://perma.cc/465N-E4A6]. And yet, when Elena Khusyaynova was indicted, she appeared on the Federal Agency of News to deny the allegations. But soon after filing the lawsuit, FAN was placed on a sanctions list established by the State Department and the Treasury Department in response to Russian intervention in the 2016 presidential election. Kevin Poulsen, *Russian Trolls' Lawsuit Against Facebook Hits a Wall*, DAILY BEAST, (Feb. 28, 2019), https://www.thedailybeast.com/russian-trolls-lawsuit-against-facebook-hits-a-wall?source=articles&via=rss [https://perma.cc/X8QH-HF880].

121. International Convention on the Elimination of all Forms of Racial Discrimination Dec. 21, 1965, 660 U.N.T.S. 195 [hereinafter CERD]; International Covenant on Civil and Political Rights Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; Optional Protocol to the International Covenant on Civil and Political Rights Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR Optional Protocol]; Convention for the Protection of Human Rights and Fundamental Freedoms Nov. 4, 1950, ETS No. 005 [hereinafter ECHR]. Russia ratified CERD in 1969. *See Parties to the International Covenant on the Elimination of all Forms of Racial Discrimination*, U.N. TREATY COLLECTION, (last visited Oct. 10, 2019), available at

A common feature of the CERD, ICCPR, and ECHR is the establishment of a corresponding institutional body.[122] The CERD Committee and the ICCPR's Human Rights Committee have broad powers, including the ability to assess state self-reporting on treaty compliance, to serve as review bodies to adjudicate claims of treaty noncompliance, and to conduct independent investigations to study the status of human rights in member states. The European Court of Human Rights functions exclusively as a review body that adjudicates claims of state noncompliance with the ECHR.

While these three treaty bodies have their own procedures and submission requirements, they all share a common feature: they allow individuals to bring claims (also referred to as communications or complaints) against member states.[123] These treaty bodies are empowered to review these submissions and issue decisions (also referred to as opinions or observations) that determine whether a state has violated its obligations under the respective treaty regime. Unlike most international tribunals, these human rights bodies are victim-centered—they empower individuals to bring claims against states and seek accountability from these states.[124] Russia has accepted the competence of the CERD Committee and the Human Rights

---

https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-2&chapter=4&clang=_en [https://perma.cc/4UTF-R3PB]. Russia ratified the ICCPR in 1973. *See Parties to the International Covenant on Civil and Political Rights*, U.N. TREATY COLLECTION, (last visited Oct. 10, 2019), https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND [https://perma.cc/WT7A-GCVP]. Russia ratified the ECHR in 1998. *See Parties to the Convention for the Protection of Human Rights and Fundamental Freedoms*, U.N. TREATY COLLECTION, (last visited Oct. 10, 2019), https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/005/signatures?p_auth=zWPjjBnD [https://perma.cc/LND3-KNL5].

122. *See, e.g.*, COURTNEY HILLEBRECHT, DOMESTIC POLITICS AND INTERNATIONAL HUMAN RIGHTS TRIBUNALS: THE PROBLEM OF COMPLIANCE 4-10 (2014); YUVAL SHANY, ASSESSING THE EFFECTIVENESS OF INTERNATIONAL COURTS 253 (2014); UN HUMAN RIGHTS TREATY BODIES: LAW AND LEGITIMACY 320 (Helen Keller & Geir Ulfstein eds., 2012); GUDMUNDUR ALFREDSSON ET AL., INTERNATIONAL HUMAN RIGHTS MONITORING MECHANISMS 35, 487, 617 (2d rev. ed. 2009).

123. *See generally* SARAH JOSEPH & MELISSA CASTAN, THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS: CASES, MATERIALS, & COMMENTARY (3d ed. 2014); WILLIAM A. SCHABAS, THE EUROPEAN CONVENTION ON HUMAN RIGHTS: A COMMENTARY (2014); PATRICK THORNBERRY, THE INTERNATIONAL CONVENTION ON THE ELIMINATION OF ALL FORMS OF RACIAL DISCRIMINATION (2016).

124. *See, e.g.*, WILLIAM SCHABAS, INTERNATIONAL COURTS AND TRIBUNALS (William Schabas ed. 2014); A.A. CANÇADO TRINDADE, THE ACCESS OF INDIVIDUALS TO INTERNATIONAL JUSTICE (2012).

Committee to consider communications from individuals who claim to be victims of violations of the CERD and ICCPR, respectively. Russia has also accepted the jurisdiction of the European Court of Human Rights to consider claims by individuals who allege Russian violations of the ECHR.[125] Despite this, several jurisdictional issues and admissibility requirements must be addressed before an individual may pursue claims against Russia in these treaty bodies.[126]

A. Substantive Claims

Russia is bound by the substantive obligations of the CERD, ICCPR, and ECHR. These treaties recognize that individuals have a basic set of human rights. These include the right to be free from discrimination and the right to freedom of thought, conscience, and religion. They also include the right to vote as well as the right to hold opinions without interference.[127] In addition, these treaties acknowledge states have an obligation to protect these human rights. To be clear, these human rights norms apply to protect individuals, and they are distinct from international norms that protect states.[128]

For example, the right to be free from discrimination based on race, color, and descent, as well as national and ethnic origin, is recognized in the CERD, ICCPR, and ECHR.[129] Discrimination is defined by CERD to include:

> any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose

125. In contrast, Russia would not be subject to the jurisdiction of other human rights bodies such as the Inter-American Commission on Human Rights or the African Commission on Human and Peoples' Rights because it has not accepted the jurisdiction of these bodies. While the United States has ratified CERD and the ICCPR, it is not a party to the ECHR. But, in fact, US ratification has no impact on the possibility of US citizens commencing proceedings against Russia in these three treaty bodies.

126. *See generally* EUROPEAN COURT OF HUMAN RIGHTS, PRACTICAL GUIDE ON ADMISSIBILITY GUIDE (4th ed. 2017) [hereinafter ECHR PRACTICAL GUIDE]; U.N. OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, INDIVIDUAL COMPLAINT PROCEDURES UNDER THE UNITED NATIONS HUMAN RIGHTS TREATIES (2013) [hereinafter OHCHR INDIVIDUAL COMPLAINT PROCEDURES].

127. Other human rights norms are also implicated, including the right to privacy. *See* Lisl Brunner, *Digital Communications and the Evolving Right to Privacy*, in NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE 217 (2018)**;** Eliza Watt, *The Right to Privacy and the Future of Mass Surveillance*, 21 INT'L J. HUM. RTS. 773 (2017).

128. There is a distinction between the violation of human rights norms and sovereignty norms. *See* Ohlin, *supra* note 20, at 1587-95.

129. For a detailed analysis, see William J. Aceves, *Virtual Hatred: How Russia Tried to Start a Race War in the United States*, 24 U. MICH. J. RACE & L. 177, 209-25 (2019).

> or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life.[130]

The ICCPR and the ECHR also prohibit discrimination on the basis of race, color, and national origin.[131]

Project Lakhta targeted minorities on the basis of race, color, and national origin.[132] Many Facebook, Instagram, and Twitter posts distinguished individuals based on these characteristics. These posts challenged the right of these individuals to the recognition, enjoyment, and exercise of basic human rights. Some posts rejected their right to basic government services.[133] Other posts promoted hatred and incitement to hatred by disparaging individuals based on race, color, or national origin.[134] Some posts even called for violence against these groups.[135]

Project Lakhta targeted religious minorities for similar treatment, thereby implicating both the prohibition against discrimination as well as the freedom of religion. While CERD does not specifically reference religion as a protected category, the CERD Committee has interpreted its protections against discrimination to cover religious discrimination.[136] Both the ICCPR and the European Convention specifically prohibit religious discrimination.[137] They also affirm the right of everyone to freedom of thought, conscience, and religion.[138] These protections apply to state action that coerces or punishes adherents of a particular religion.

International law recognizes the right of individuals to vote and participate in the political process.[139] Project Lakhta violated these

---

130. CERD, *supra* note 121, at art. 1(1).

131. ICCPR, *supra* note 121, at arts. 2(1), 26; ECHR, *supra* note 121, art. 14.

132. Aceves, *supra* note 129, at 1.

133. Complaint at 31, United States of America v. Elena Alekseevna Khusyaynova, No. 1:18-MJ-464 (E.D. Va. Sept. 27, 2018).

134. *Id*. at 29.

135. Curt Devine, *"Kill Them All"—Russian-Linked Facebook Accounts Called for Violence*, CNN MONEY (Oct. 31, 2017), https://money.cnn.com/2017/10/31/media/russia-facebook-violence/index.html [https://perma.cc/35VR-93MT].

136. THORNBERRY, *supra* note 123, at 303-05, 351-56.

137. ICCPR, *supra* note 121, arts. 2(1), 26; ECHR, *supra* note 121, art. 14.

138. ICCPR, *supra* note 121, art. 18; ECHR, *supra* note 121, art. 9.

139. *See generally* Niels Petersen, *Elections, Right to Participate in, International Protection*, MAX PLANCK ENCY. PUB. INT'L L. (2012), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e785

basic norms.[140] The right to vote was clearly subverted when US voters were targeted by systematic disinformation campaigns about specific candidates and issues. In addition, voter suppression efforts targeted specific groups with misinformation about voting procedures and even encouraged these groups to abstain from voting.[141]

The right to vote is explicitly recognized in the ICCPR as well as Protocol 1 of the ECHR, which Russia has also ratified.[142] The ICCPR indicates that citizens shall have the right to vote in elections that guarantee "the free expression of the will of the electors" and that are not affected by discrimination.[143] The Human Rights Committee has indicated that "[v]oters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind."[144] Protocol 1 of the ECHR indicates that elections must "ensure the free expression of the opinion

---

[https://perma.cc/PUT8-PB3R]; DEMOCRATIC GOVERNANCE AND INTERNATIONAL LAW (Gregory H. Fox & Brad R. Roth eds., 2000); Thomas M. Franck, *The Emerging Right to Democratic Governance*, 86 AM. J. INT'L L. 46 (1994); Gregory H. Fox, *The Right to Political Participation in International Law*, 17 YALE J. INT'L L. 539 (1992); *but see* Ludvig Beckman, *The Right to Democracy and the Human Rights to Vote: The Instrumental Argument Rejected*, 13 J. HUM. RTS. 381 (2013). *Cf.* Jacob Rush, *Hacking the Right to Vote*, 105 VA. L. REV. ONLINE 67 (2018).

140. HAROLD HONGJU KOH, THE TRUMP ADMINISTRATION AND INTERNATIONAL LAW 83-84 (2019). *See* TALLINN MANUAL 2.0, *supra* note 99, at 45 ("Illegal coercive interference could include manipulation of elections or of public opinion on the eve of elections, as when online news services are altered in favor of a particular party, false news is spread, or the online services of one party are shut off.").

141. *See* Joe Davidson, *Russia and Republicans Attempt to Suppress Black Vote, But Russians are Slicker*, WASH. POST (Dec. 19, 2018), https://www.washingtonpost.com/politics/2018/12/19/russia-republicans-attempt-suppress-black-vote-russians-are-slicker/?utm_term=.5e8b03f48591 [https://perma.cc/6DFW-CDH8]; Zak Cheney-Rice, *What Russia Learned About Black Voters From America*, N.Y. MAG., (Dec. 17, 2018), http://nymag.com/intelligencer/2018/12/russia-voter-suppression.html [https://perma.cc/PKN9-632F]; Young Mie Kim, Brennan Ctr. J., *Voter Suppression Has Gone Digital*, BRENNAN CENTER FOR JUSTICE (Nov. 20, 2019), https://www.brennancenter.org/blog/voter-suppression-has-gone-digital [https://perma.cc/AF2H-NPZL].

142. Russia ratified the Optional Protocol (Protocol I) to the ECHR in 1998. *See* Council of Europe, Chart of Signatures and Ratifications of Treaty 009, (last visited Oct. 10, 2019), https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND [https://perma.cc/6JBA-DGRJ].

143. ICCPR, *supra* note 121, art. 25; KOH, *supra* note 140, at 83 ("An external attempt to distort the information that voters possess when they go to the polls also violates the human rights of the electors under the International Covenant on Civil and Political Rights.").

144. U.N. Hum. Rts. Comm., CCPR General Comment No. 25: Article 25 (Participation in Public Affairs and the Right to Vote), ¶ 19, U.N. Doc. CCPR/C/21/Rev.1/Add.7 (July 12, 1996).

of the people in the choice of the legislature."[145] The European Court of Human Rights has indicated that the ECHR sets forth the same rights regarding the right to vote as the ICCPR.[146] CERD requires member states to protect the right of all individuals to vote without discrimination.[147]

In sum, Project Lakhta violated numerous international human rights norms. These norms are set forth in the CERD, ICCPR, and ECHR, and they apply to Russia because it ratified these treaties.

B. Extraterritoriality

By their terms, most treaties appear to limit the scope of member state obligations to their own territory.[148] While the Internet Research Agency was located in Russia, it operated in cyberspace and its victims were in the United States. Accordingly, Russia could argue that its human rights obligations do not extend to protect individuals outside its territory, including in cyberspace. There is, however, growing recognition that human rights obligations extend beyond a state's territory.[149] Such obligations also apply when a state's actions affect individuals outside its territory. In fact, such a functionalist approach now appears to be the norm.[150]

---

145. Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms art. 3 Mar. 20, 1952, E.T.S. No. 9.

146. Hirst v. United Kingdom, App. No. 74025/01, Eur. Ct. H.R. (2005).

147. CERD, *supra* note 121, art. 5(c).

148. *See generally* MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011); Oona A. Hathaway et al., *Human Rights Abroad: When Do Human Rights Treaty Obligations Apply Extraterritorially?*, 43 ARIZ. ST. L.J. 389 (2011).

149. *See generally* Monika Heupel, *How Do States Perceive Extraterritorial Human Rights Obligations? Insights from the Universal Periodic Review*, 40 HUM. RTS. Q. 521 (2018); Hugh King, *The Extraterritorial Human Rights Obligations of States*, 9 HUM. RTS. L. REV. 521 (2009); Mark Gibney et al., *Transnational State Responsibility for Violations of Human Rights*, 12 HARV. HUM. RTS. J. 267 (1999); Theodor Meron, *Extraterritoriality of Human Rights Treaties*, 89 AM. J. INT'L L. 78, 82 (1995).

150. *But see* Ohlin, *supra* note 20, at 1585. There is some debate as to whether the extraterritorial application of human rights norms applies to all such norms. *See, e.g.*, Martin Scheinin, *Letter to the Editor from Former Member of the Human Rights Committee, Martin Scheinin*, JUST SECURITY (Mar. 10, 2014), https://www.justsecurity.org/8049/letter-editor-martin-scheinin/; Jennifer Daskal, *Extraterritorial Surveillance Under the ICCPR . . . The Treaty Allows It!*, JUST SECURITY (Mar. 7, 2014), https://www.justsecurity.org/7966/extraterritorial-surveillance-iccpr-its-allowed/ [https://perma.cc/9HC6-53EG]; Ashley Deeks, *Extraterritorial Right to Privacy: A Response to Luca Urech*, LAWFARE (Nov. 15, 2013), https://www.lawfareblog.com/extraterritorial-right-privacy-response-luca-urech [https://perma.cc/89ZH-JVD6].

In *Georgia v. The Russian Federation*, the International Court of Justice ("ICJ") considered whether Russia's obligations under CERD were limited to Russian territory or extended beyond its borders to include Russian actions in Georgia.[151] In its Provisional Measures Order, the ICJ concluded that Russia's CERD obligations applied extraterritorially.

> [T]here is no restriction of a general nature in CERD relating to its territorial application . . . neither Article 2 nor Article 5, alleged violations of which were invoked by Georgia, contain a specific territorial limitation . . . . [T]he Court consequently finds that these provisions of CERD generally appear to apply, like other provisions of instruments of that nature, to the actions of a State party when it acts beyond its territory.[152]

Significantly, the ICJ's language implies that other human rights treaties would also have extraterritorial reach.[153] And, in fact, similar determinations have been issued by the Human Rights Committee and the European Court of Human Rights.[154] The reasons for such an approach are evident—the object and purpose of human rights treaties "would be severely undermined if States could evade responsibility by relocating their abuse of individuals."[155]

The Tallinn Manual 2.0 offers conflicting views on the extraterritorial application of human rights norms.[156] In the absence of physical control over affected individuals, the International Group of Experts that drafted the Tallinn Manual 2.0 could not agree on whether activities conducted through cyberspace give rise to state liability under

---

151. Application of the International Convention on the Elimination of all Forms of Racial Discrimination, (Georgia v. Russian Federation), Provisional Measures Order, I.C.J. REP. 353 (Oct. 15, 2008).

152. *Id*. at 109.

153. The ICJ has made similar findings in several cases. *See e.g*., Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda), Judgment, I.C.J. REP. 168 (Dec. 19, 2005); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ REP. 136 (July 9, 2004).

154. JOSEPH & CASTAN, *supra* note 123, at 96-100; SCHABAS, *supra* note 123, at 100-102; THORNBERRY, *supra* note 123, at 171-78. *See also* Daniel Mogster, *Toward Universality: Activities Impacting the Enjoyment of the Right to Life and the Extraterritorial Application of the ICCPR*, EJIL: TALK! (Nov. 27, 2018), https://www.ejiltalk.org/towards-universality-activities-impacting-the-enjoyment-of-the-right-to-life-and-the-extraterritorial-application-of-the-iccpr/ [https://perma.cc/G7A6-E8VW].

155. NOAM UBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 205 (2010).

156. TALLINN MANUAL 2.0, *supra* note 99, at 182-86 (Rule 34 – Applicability).

customary international law.[157] There was agreement, however, that the extraterritorial application of human rights treaties was governed by the provisions of those treaties.[158] The understanding of the institutional bodies responsible for interpreting and applying these human rights treaties is, therefore, dispositive because these bodies would be adjudicating any such claims.

State responsibility for harms that occur outside their territory can also be established through the principle of due diligence and the obligation to prevent transboundary harm. This principle of customary international law focuses on where the harmful conduct arose rather than on where the damage occurred.[159] Essentially, this obligation is domestic rather than extraterritorial: states have "a duty to protect other states against injurious acts by individuals from within their jurisdiction."[160] Thus, this obligation would extend to harms that occur anywhere, including cyberspace.[161] Even the Tallinn Manual 2.0 recognizes the due diligence principle.[162]

C. Victim Status

In order to bring a claim before any of these human rights bodies, an applicant must be considered a victim. This requirement exists for CERD, the ICCPR, and the European Court.[163] At a minimum, this means the applicant must be personally affected by a state's acts or omissions. Human rights bodies generally do not accept a claim perceived as an *actio popularis*.[164] This simply means an applicant

157. *Id*. at 185.

158. *Id*. at 186.

159. JOANNA KULESZA, DUE DILIGENCE IN INTERNATIONAL LAW 9 (2016).

160. Trail Smelter Case (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (Perm. Ct. Arb. 1941).

161. *See generally* Akiko Takano, *Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications*, 7 LAWS 36 (2018); Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68 (2015).

162. TALLINN MANUAL 2.0, *supra* note 99, at 30 (Rule 6 – Due Diligence (General Principle)).

163. U.N. Hum. Rts. Comm., Rules of Procedure of the Human Rights Committee, ¶ r. 96(b), U.N. Doc. CCPR/C/3/Rev. 10 (Jan. 11, 2012) [hereinafter HRC Rules of Procedure]; Comm. on the Elimination of Racial Discrimination, Rules of Procedure of the Committee on the Elimination of Racial Discrimination, ¶ r. 91(b), U.N. Doc. CERD/C/35/Rev.3 (1986) [hereinafter CERD Rules of Procedure]; ECHR, *supra* note 121, art. 34; *see also* JOSEPH & CASTAN, *supra* note 123, at 71-75; SCHABAS, *supra* note 123, at 736-45; THORNBERRY, *supra* note 123, at 56.

164. JOSEPH & CASTAN, *supra* note 123, at 75; SCHABAS, *supra* note 123, at 738-39; THORNBERRY, *supra* note 123, at 60. *See generally* FARID AHMADOV, THE RIGHTS OF *ACTIO POPULARIS* BEFORE INTERNATIONAL COURTS AND TRIBUNALS (2018); William J. Aceves,

must have been personally affected and cannot claim victim status through the suffering of other individuals.

While an applicant must be personally affected, this does not require the applicant to be specifically targeted. Human rights bodies have recognized victim status in cases involving hate speech directed at particular groups and not at specific individuals.[165] In *Rabbae, A.B.S. & N.A. v. Netherlands*, for example, the Human Rights Committee accepted the victim status of the applicants and rejected claims they were pursuing an *actio popularis*.[166] This case involved a Dutch politician who made numerous online and print media statements demeaning the Muslim community and non-Western immigrants.

> In the present case, the Committee notes that the authors do not bring abstract claims as members of the general population of the State party. The authors are Muslims and Moroccan nationals, and allege that Mr. Wilders' statements specifically target Muslims, Moroccans, non-Western immigrants and Islam. The authors are therefore members of the category of persons who were the specific focus of Mr. Wilders' statements. They also allege that they feel personally and directly affected by Mr. Wilders' hate speech and suffer the effects of it in their daily lives, including through attacks on the Internet, and that they have been adversely affected by the signal given to the public, through the acquittal, that Mr. Wilders' conduct is not criminal.[167]

Another consideration in assessing victim status is whether the applicant is a human being, a group of individuals, an organization, or a business entity. Of the three treaty institutions, the Human Rights Committee appears to have the most restrictive view on victim status and generally limits claims to human beings.[168] The European Court has the most liberal view on victim status due to the broad mandate offered by the ECHR. It allows persons as well as non-governmental

---

Actio Popularis? The Class Action in International Law, 2003 U. CHI. LEGAL FORUM 353 (2003).

165. *See generally* Whittney Barth, *Taking "Great Care": Defining Victims of Hate Speech Targeting Religious Minorities*, 19 CHI. J. INT'L L. 68 (2018).

166. Rabbae, A.B.S. & N.A. v. Netherlands, Views adopted by the Committee under article 5 (4) of the Optional Protocol, Comm. No. 2124/2011, at ¶¶ 5.2, 9.5-9.6, U.N. Doc. CCPR/C/117/D/2124/2011 (2017).

167. *Id.* ¶ 9.6; *see also* Toonen v. Australia, Views of the Human Rights Committee under article 5, paragraph 4, of the Optional Protocol to the International Covenant on Civil and Political Rights, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994).

168. ICCPR Optional Protocol, *supra* note 121, art. 1; HRC Rules of Procedure, *supra* note 163, ¶ r. 96(b); *see also* JOSEPH & CASTAN, *supra* note 123, at 71-79.

organizations and groups of individuals to bring claims.[169] The CERD Committee is authorized by the treaty to consider communications submitted from "individuals or groups of individuals."[170] In *TBB-Turkish Union in Berlin/Brandenburg v. Germany*, therefore, the CERD Committee allowed an organization to bring a claim in a case involving discriminatory statements made against Muslims and other citizens of Turkish heritage.[171]

The European Convention adds an additional consideration related to victim status—a case is inadmissible if the applicant "has not suffered a significant disadvantage . . . ."[172] The purpose of this requirement is to ensure that only meaningful harms are subject to legal proceedings. In other words, a violation must "attain a minimum level of severity to warrant consideration by an international court."[173]

D. Exhaustion of Domestic Remedies

Human rights treaties typically require applicants to exhaust domestic remedies before initiating proceedings.[174] This means an applicant must first seek to address alleged harms domestically through judicial or administrative proceedings.[175] There is, however, a significant caveat to this requirement. Applicants are not required to exhaust domestic remedies that are considered futile.[176] For example, applicants need not exhaust domestic remedies when they would have "no prospect of success before the domestic courts."[177] Similarly, the

169. ECHR, *supra* note 121, art. 34; *see also* SCHABAS, *supra* note 123, at 737-45.

170. CERD, *supra* note 121, art. 14(1); *see also* THORNBERRY, *supra* note 123, at 56-57.

171. TBB-Turkish Union in Berlin/Brandenburg v. Germany, Opinion adopted by the Committee at its eighty-second session, 11 February to 8 March 2013, Comm. No. 48/2010, at ¶ 11.3, U.N. Doc. CERD/C/82/D/48/2010 (2013).

172. ECHR, *supra* note 121, art. 35(3)(b).

173. ECHR PRACTICAL GUIDE, *supra* note 126, at 66-67.

174. HRC Rules of Procedure, *supra* note 163, ¶ r. 96(f); CERD Rules of Procedure, *supra* note 163, ¶ r. 91(f); ECHR, *supra* note 121, art. 35(1); *see also* JOSEPH & CASTAN, *supra* note 123, at 121-49; SCHABAS, *supra* note 123, at 764-769; THORNBERRY, *supra* note 123, at 56.

175. *See generally* Matthew H. Adler, *The Exhaustion of the Local Remedies Rule after the International Court of Justice's Decision in ELSI*, 39 INT'L & COMP. L.Q. 641 (1990); A.A. CANÇADO TRINDADE, THE APPLICATION OF THE RULE OF EXHAUSTION OF LOCAL REMEDIES IN INTERNATIONAL LAW: ITS RATIONALE IN THE INTERNATIONAL PROTECTION OF INDIVIDUAL RIGHTS (1983).

176. JOSEPH & CASTAN, *supra* note 123, at 130; SCHABAS, *supra* note 123, at 765; THORNBERRY, *supra* note 123, at 59.

177. Carson and Others v. United Kingdom, App. No. 42184/05, Eur. Ct. H.R., at ¶ 58 (2010).

exhaustion requirement does not apply if domestic proceedings are of unreasonable duration.[178]

E. Statute of Limitations

Some human rights bodies place limits on when an applicant may bring a claim. This temporal requirement generally functions in tandem with the exhaustion of domestic remedies requirement. Both the CERD Committee and the European Court require that a claim be brought within six months from the date on which a final decision was taken regarding domestic remedies.[179] When the exhaustion of domestic remedies is considered futile, the six month period will run from the date that the alleged acts occurred or the date the applicant became aware of the act.[180] The Human Rights Committee offers a more generous time period in which individuals may bring claims.[181] A claim may be considered an abuse of the right of submission if it is not brought within five years from the exhaustion of domestic remedies.[182]

F. Consideration of Other International Procedures

An applicant is generally not allowed to bring concurrent actions involving the same issue before multiple human rights bodies.[183] While human rights treaties create unique substantive obligations and corresponding institutional bodies, there is a recognition that concurrent proceedings are inefficient and waste the limited resources available to victims of human rights abuses. The Human Rights Committee and the European Court each impose this admissibility requirement on applicants.[184] The CERD Committee asks applicants to

178. *See, e.g.*, Fillastre & Bizouarn v. Bolivia, Views of the Human Rights Committee under article 5, paragraph 4, of the Optional Protocol to the International Covenant on Civil and Political Rights, Comm. No. 336/1988, ¶ 5.2, U.N. Doc. CCPR/C/43/D/336/1988, at 96 (1991).

179. CERD Rules of Procedure, *supra* note 163, ¶ r. art. 35(1); *see also* SCHABAS, *supra* note 123, at 770-73; THORNBERRY, *supra* note 123, at 56. Protocol No. 15 to the European Convention will reduce the six-month time period to four months when it enters into force. Protocol No. 15 Amending the Convention on the Protection of Human Rights and Fundamental Freedoms art. 4, June 24, 2013, C.E.T.S. No. 213.

180. SCHABAS, *supra* note 123, at 772.

181. HRC Rules of Procedure, *supra* note 163, ¶ 96(c).

182. OHCHR INDIVIDUAL COMPLAINT PROCEDURES, *supra* note 126, at 13.

183. OLIVIER DE SCHUTTER, INTERNATIONAL HUMAN RIGHTS LAW: CASES, MATERIALS, COMMENTARY 903 (2d ed. 2014).

184. HRC Rules of Procedure, *supra* note 163, ¶ 96(e); ECHR, *supra* note 121, art. 35(2)(b); *see also* JOSEPH & CASTAN, *supra* note 123, at 113-20; SCHABAS, *supra* note 123, at 776–78.

indicate whether "the same matter is being examined under another procedure of international investigation or settlement."[185] However, this is not designated as an admissibility requirement.[186] Of course, there is no preclusion for cases brought by different individuals in each of the human rights bodies.

Of the three human rights bodies, the decisions of the European Court are unique because they are considered legally binding on member states and there is an obligation to comply. Article 46 of the ECHR provides that member states "undertake to abide by the final judgment of the Court in any case to which they are parties."[187] And, significantly, the Committee of Ministers is authorized to supervise the execution of these judgments.[188] While the decisions of the CERD Committee and the Human Rights Committee are considered authoritative interpretations of the respective treaties and should be implemented in good faith, they are not considered legally binding.[189]

V. CONCLUSION

Through Project Lakhta, Russia targeted the United States; but its actual targets and the real victims were the American people. The CERD Committee, Human Rights Committee, and the European Court of Human Rights offer US citizens an opportunity to hold Russia accountable for Project Lakhta and the work of the Internet Research Agency. There are, of course, some challenges with respect to jurisdiction and admissibility. Notwithstanding, there are several reasons why these claims should be brought.[190]

Most significantly, there are no other viable forums to hear claims against Russia. A federal district court acknowledged the ultimate goal of Project Lakhta and the Internet Research Agency was "to sow discord among U.S. voters through divisive social media posts and political rallies. That goal, by itself, was not illegal."[191] While two criminal proceedings were filed in relation to Project Lakhta, neither

185. CERD Rules of Procedure, *supra* note 163, ¶ 84(g).

186. THORNBERRY, *supra* note 123, at 57.

187. ECHR, *supra* note 121, art. 46(1).

188. *Id*. art. 46(2); *see also* SCHABAS, *supra* note 123, at 871–72.

189. OHCHR INDIVIDUAL COMPLAINT PROCEDURES, *supra* note 126, at 11. *See also* Keller & Ulfstein, *supra* note 122, at 4.

190. *See generally* HELEN DUFFY, STRATEGIC HUMAN RIGHTS LITIGATION: UNDERSTANDING AND MAXIMIZING (2018).

191. United States v. Concord Mgmt. & Consulting LLC, No. 18-cr-32-2, 2019 WL 2247792, at *1 (D.D.C. May 24, 2019).

case involves the Russian government as a defendant. No civil cases have been filed against Russia in US or Russian courts.

The commencement of proceedings against Russia will generate publicity and force it to respond in a public forum.[192] Multiple filings will heighten their impact even if some cases are eventually consolidated. By highlighting these issues to the CERD Committee and the Human Rights Committee, these bodies may choose to address them in their future assessments of Russia's compliance with their respective treaty obligations even if the cases do not move forward. These bodies may also address these issues in their General Comments regarding treaty norms. While the European Court does not have comparable authority to act outside the litigation process, the Council of Europe may choose to respond to Russia's actions.

Heightened publicity may result in these issues being addressed by other UN human rights mechanisms. Several UN thematic procedures could address these issues, including the UN Working Group of Experts on People of African Descent, the UN Special Rapporteur on Minority Issues, and the UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance.[193] The use of social media by states to violate human rights could be addressed by the UN Special Rapporteur on the Promotion of the Right to Freedom of Opinion and Expression.[194] Finally, these issues could be addressed through the Universal Periodic Review process at the United Nations, which is designed to review Russia's overall compliance with its human rights obligations.[195]

Proceedings before human rights bodies offer a unique opportunity. This is a victim-centered process, which seems particularly important because human beings were Project Lakhta's targets. Accordingly, victims should be able to file their own claims against Russia without the need for US government authorization or

192. *But see* Jack Goldsmith, *The Strange WannaCry Attribution*, LAWFARE (Dec. 21, 2018), https://www.lawfareblog.com/strange-wannacry-attribution [https://perma.cc/T2RC-9HAP].

193. *See generally* THE UNITED NATIONS SPECIAL PROCEDURES SYSTEM (Aoife Nolan et al. eds., 2017); TED PICCONE, CATALYSTS FOR CHANGE: HOW THE U.N.'S INDEPENDENT EXPERTS PROMOTE HUMAN RIGHTS (2012).

194. *See* U.N. Human Rights Council, Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, ¶¶ 2 U.N. Doc. A/HRC/38/35 (Apr. 6, 2018).

195. *See* HUMAN RIGHTS AND THE UNIVERSAL PERIODIC REVIEW: RITUALS AND RITUALISM 1-22 (Hilary Charlesworth & Emma Larking eds., 2015).

support. This victim-centered approach is appropriate for other reasons. Social media users must take responsibility for monitoring and protecting their rights in cyberspace.[196] Citizens also have an obligation to defend the democratic process, which is under attack.[197] By relying solely on governments and social media companies to address these issues, citizens and social media users abdicate their own responsibilities. In fact, it is striking that many studies on the Russian disinformation campaign simply disregard the role of individuals in protecting their own rights.[198]

Finally, Russia's use of inauthentic social media accounts is ongoing.[199] Efforts were made to influence the 2018 US midterm elections. Reports indicate similar efforts will be made to affect the 2020 US presidential elections.[200] In addition, Project Lakhta targeted

196. *See, e.g.*, Chandelis R. Duster, *NAACP Launches #LogOutFacebook After Reports on Black Voter Suppression*, NBC NEWS (Dec. 18, 2018), https://www.nbcnews.com/news/nbcblk/naacp-launches-logoutfacebook-after-reports-black-voter-suppression-n949156 [https://perma.cc/ZL48-FGB2].

197. *See* David M. Howard, *Can Democracy Withstand the Cyber Age?: 1984 in the 21st Century,* 69 HASTINGS L.J. 1355, 1373-74 (2018).

198. *See, e.g.*, Michael Carpenter, *Countering Russia's Malign Influence Operations*, JUST SECURITY (May 29, 2019), https://www.justsecurity.org/64327/countering-russias-malign-influence-operations/ [https://perma.cc/8USF-H3GR]; Renee DiResta & Mike Godwin, *The Seven Step Program for Fighting Disinformation*, JUST SECURITY (Feb. 28, 2019), https://www.justsecurity.org/62718/step-program-fighting-disinformation/ [https://perma.cc/89FA-N8YB]; BARRETT, *supra* note 1, at 23-29; SAMANTHA BRADSHAW ET AL., NATO STRATCOM COE, GOVERNMENT RESPONSES TO MALICIOUS USE OF SOCIAL MEDIA 4 (2018). *But see* Nina Jankowicz, *How the U.S. Can Fight Russian Disinformation for Real*, ATLANTIC COUNCIL (July 11, 2019), https://www.atlanticcouncil.org/blogs/ukrainealert/how-the-us-can-fight-russian-disinformation-for-real [https://perma.cc/9TJM-5FRL]. In fact, one organization, IREX, has worked to create educational programs that help social media users detect inauthentic communications. *See* IREX, *Learn to Discern (L2D) – Media Literacy Training*, https://www.irex.org/project/learn-discern-l2d-media-literacy-training [https://perma.cc/5SDW-MSUH].

199. *See* Nathaniel Gleicher, Facebook, *Removing More Coordinated Inauthentic Behavior from Russia*, FACEBOOK (May 6, 2019), https://newsroom.fb.com/news/2019/05/more-cib-from-russia/ [https://perma.cc/XU57-N35H].

200. *See, e.g.*, Maggie Miller, *U.S. Officials Tracking Influence Operations on Social Media from Russia, Iran*, THE HILL (June 24, 2019), https://thehill.com/policy/cybersecurity/450077-us-officials-tracking-influence-operations-on-social-media-from-russia [https://perma.cc/LEX9-6X3A]; Ali Breland, *Want to See How Disinformation Could Play Out in 2020? Just Look Overseas*, MOTHER JONES (June 20, 2019), https://www.motherjones.com/politics/2019/06/want-to-see-how-disinformation-could-play-out-in-2020-just-look-overseas/ [https://perma.cc/8TMW-UGKD].

several countries.[201] And, Russia is not alone in developing such online propaganda campaigns.[202]

This Article is not meant to be purely descriptive or solely academic in nature. It has a prescriptive agenda that supports the initiation of legal proceedings against Russia.[203] Individuals interested in bringing claims against Russia should examine the complaint requirements for each treaty body, review the model complaint forms, and file their claims.

---

201. *See* Digital Forensic Research Lab, The Atlantic Council, *Top Takes: Suspected Russian Intelligence Operation*, MEDIUM (June 22, 2019), https://medium.com/dfrlab/top-takes-suspected-russian-intelligence-operation-39212367d2f0 [https://perma.cc/977G-6C4R]; ERIK BRATTBERG & TIM MAURER, CARNEGIE ENDOWMENT FOR INT'L PEACE, RUSSIAN ELECTION INTERFERENCE: EUROPE'S COUNTER TO FAKE NEWS AND CYBER ATTACKS (2018); TODD C. HELMUS ET AL., RAND CORP., RUSSIAN SOCIAL MEDIA INFLUENCE: UNDERSTANDING RUSSIAN PROPAGANDA IN EASTERN EUROPE (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf [https://perma.cc/B9F2-KYQ9].

202. *See, e.g.*, Diego A. Martin & Jacob N. Shapiro, *Trends in Online Foreign Influence Efforts*, ESOC Publications (July 1, 2019); Samuel Woodhams, *To Battle Russian Disinformation, Ukraine Mimics . . .Russia*, JUST SECURITY (Apr. 17, 2019), https://www.justsecurity.org/63682/to-battle-russian-disinformation-ukraine-mimics-russia/ [https://perma.cc/989F-W43T]; Ayesha Tanzeem, *Facebook Removes Accounts Linked to Indian Political Parties, Pakistan's Military*, VOA (Apr. 1, 2019), https://www.voanews.com/south-central-asia/facebook-removes-accounts-linked-indian-political-parties-pakistans-military [https://perma.cc/PGM4-9VDZ]; Natalia Drozdiak, *Facebook Removes Hundreds of Fake Accounts Linked to Iran*, BLOOMBERG (Mar. 26, 2019), https://www.bloomberg.com/news/articles/2019-03-26/facebook-removes-hundreds-of-fake-accounts-linked-to-iran [https://perma.cc/FQ9F-XALV].

203. There are some risks in engaging with Russian "trolls." *See* Johan Sigholm, *I Wrote About Russian Election Interference. Then I Was Trolled Online*, LAWFARE (Sept. 4, 2018), https://www.lawfareblog.com/i-wrote-about-russian-election-interference-then-i-was-trolled-online [https://perma.cc/YEJ8-X7NG]; Paul R. Gregory, Hoover Inst., *My War with Russian Trolls*, DEFINING IDEAS (Mar. 21, 2018), https://www.hoover.org/research/my-war-russian-trolls [https://perma.cc/3MTN-EJUT].

Committee on the Elimination of Racial Discrimination[204]
and Human Rights Committee[205]
Petitions and Inquiries Section
Office of the High Commissioner for Human Rights
United Nations Office at Geneva
1211 Geneva 10, Switzerland
petitions@ohchr.org

European Court of Human Rights[206]
The Registrar
European Court of Human Rights
Council of Europe
F-6705 Strasbourg cedex
France

204. For information on filing a complaint with the CERD Committee, *see* U.N. OHCHR, *CERD*, https://www.ohchr.org/en/hrbodies/cerd/pages/cerdindex.aspx [https://perma.cc/2LZ8-D4TU].

205. For information on filing a complaint with the Human Rights Committee, *see* U.N. OHCHR, *Human Rights Committee*, https://www.ohchr.org/en/hrbodies/ccpr/pages/ccprindex.aspx [https://perma.cc/EK38-TPC6].

206. For information on filing a complaint with the European Court of Human Rights, *see* ECHR, *Apply to the Court*, https://www.echr.coe.int/Pages/home.aspx?p=applicants&c=#n1365511805813_pointer [https://perma.cc/F7VS-HHYW].