Indiana Law Journal

Volume 95 | Issue 3 Article 4

Summer 2020

The Changing Face of Terrorism and the Designation of Foreign Terrorist Organizations

Patrick J. Keenan
University of Illinois College of Law, pjkeenan@illinois.edu

The Changing Face of Terrorism and the Designation of Foreign Terrorist Organizations

PATRICK J. KEENAN*

CONTENTS

INTRODUCTION 789
I. THE PROBLEM: NEW ATTACKS AND NEW ATTACKERS.....796
A. Attacks on U.S. Elections 796
B. Attacks on Critical Infrastructure 799
II. FTO DESIGNATION AND ITS IMPLICATIONS FOR LAW ENFORCEMENT 800
A. FTO Designation in U.S. Policy 801
B. The Law of FTO Designation 805
1. Designation Process..... 805
2. Legal Consequences of Designation..... 807
III. APPLYING FTO DESIGNATION TO THE NEW ATTACKS 808
A. The Nature of an Organization Under the Statute 810
B. Threat to U.S. National Security..... 814
C. Defining Terrorism 817
CONCLUSION.....819

INTRODUCTION

There is a new kind of conflict taking place that targets physical, social, and political infrastructure. The most prominent example, but far from the only one, is well known to most Americans. In 2016, Russian operatives and others attempted to interfere with the elections in the United States.[1] This led to the appointment of Robert S. Mueller as Special Counsel for the U.S. Department of Justice to investigate the

---

* I am grateful to Andy Leipold and Verity Winship for their helpful comments and conversations.

1. *See, e.g.*, RENEE DIRESTA, KRIS SHAFFER, BECKY RUPPEL, DAVID SULLIVAN, ROBERT MATNEY, RYAN FOX, JONATHAN ALBRIGHT & BEN JOHNSON, NEW KNOWLEDGE, THE TACTICS AND TROPES OF THE INTERNET RESEARCH AGENCY 4 (2018) (describing, based on analysis of the social media data disclosed to the Senate Select Committee on Intelligence, the ways that Russia and its operatives interfered in the 2016 U.S. elections); OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS 1 (2017) (finding that "Putin and the Russian Government aspired to help [candidate] Trump's election chances when possible by discrediting [candidate] Clinton"); SENATE SELECT COMM. ON INTELLIGENCE, 115TH CONG., RUSSIAN TARGETING OF ELECTION INFRASTRUCTURE DURING THE 2016 ELECTION: SUMMARY OF INITIAL FINDINGS AND RECOMMENDATIONS (2018), https://www.intelligence.senate.gov/publications/russia-inquiry [https://perma.cc/7TA3-UVFR] (describing attempts to hack or otherwise penetrate U.S. election infrastructure); Scott Shane & Mark Mazzetti, *The Plot to Subvert an Election: Unraveling the Russia Story So Far*, 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/S86D-5QW6] (finding, based on comprehensive reporting, that "Russians carried out a landmark intervention" in the U.S. elections).

alleged interference,[2] and provoked thousands of news reports.[3] The flood of stories about Russian interference in the 2016 U.S. elections threatens to obscure other attacks that are perhaps even more serious, and for which the United States is equally poorly prepared.[4] In March 2018, the U.S. Department of Homeland Security and the F.B.I. issued a technical alert about a large, "multi-stage intrusion campaign" launched by the Russian government against targets in the U.S. energy sector, including nuclear, commercial, and aviation facilities.[5] If the full threat of the attack materializes, Russia and its operatives could wreak havoc on large swaths of the U.S. power grid, including hospitals, sensitive aviation facilities, and dams. Russia launched similar attacks in Ukraine in 2015 and disabled that country's electric grid.[6] Russia also tested attacks against commercial actors in Ukraine whose operations were essential to the functioning of that country's economy and governance.[7] As significant as it was, Russia's interference with the 2016 election was not nearly as deadly as these other potential attacks could become.[8] All of these attacks and threats

---

2. OFFICE OF THE DEPUTY ATTORNEY GEN., DEP'T OF JUSTICE, APPOINTMENT OF SPECIAL COUNSEL TO INVESTIGATE RUSSIAN INTERFERENCE WITH THE 2016 PRESIDENTIAL ELECTION AND RELATED MATTERS, ORDER NO. 3915-2017 (2017), https://www.justice.gov/opa/press-release/file/967231/download [https://perma.cc/FL9U-BW3R].

3. For a comprehensive guide to the various stories, see Mount Holyoke College, *Trump Presidency: Election, Transition, and Administration*, MOUNT HOLYOKE LIBR. RES. GUIDES, http://guides.mtholyoke.edu/trump [https://perma.cc/X3F3-E9Y8]. The research guide brings together the relevant documents, news feeds, and other sources.

4. *See, e.g.*, Rebecca Smith, *U.S. Officials Push New Penalties for Hackers of Electrical Grid*, WALL ST. J. (Aug. 5, 2018), https://www.wsj.com/articles/u-s-officials-push-new-penalties-for-hackers-of-electrical-grid-1533492714 [https://perma.cc/RZD6-VQCE]. (describing attempts by U.S. law enforcement agencies to increase protections of critical infrastructure against cyberattacks); Arthur H. House, Opinion, *We'd Be Crippled by a Cyberattack on Our Utilities*, WASH. POST. (Oct. 14, 2018), https://www.washingtonpost.com/opinions/wed-be-crippled-by-a-cyberattack-on-our-utilities/2018/10/14/206b0dc6-cca8-11e8-a360-85875bac0b1f_story.html [https://perma.cc/T3TS-LVGM].

5. *See* NATI'L CYBERSECURITY AND COMMC'NS INTEGRATION CTR., U.S. DEP'T OF HOMELAND SEC., RUSSIAN GOVERNMENT CYBER ACTIVITY TARGETING ENERGY AND OTHER CRITICAL INFRASTRUCTURE SECTORS (2018), https://www.us-cert.gov/ncas/alerts/TA18-074A [https://perma.cc/WJJ7-55FM] (describing "a multi-stage intrusion campaign by Russian government cyber actors" against U.S. infrastructure).

6. Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [https://perma.cc/637V-8NE2] (describing coordinated attack on power grid that disabled power to approximately 225,000 people).

7. *See, e.g.*, Andrew E. Kramer, *Ukraine Cyberattack Was Meant to Paralyze, not Profit, Evidence Shows*, N.Y. TIMES (June 28, 2017), https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html [https://perma.cc/ZG5Z-Y3XS] (describing Russian-directed cyberattack on Ukrainian computer systems and critical infrastructure).

8. *See, e.g.*, Rob Knake, *The Next Cyber Battleground: Defending the U.S. Power Grid from Russian Hackers*, FOREIGN AFF. (July 19, 2018), https://www.foreignaffairs.com/articles/north-america/2018-07-19/next-cyber-battleground [https://perma.cc/AHH7-C7N5] (describing potential impacts of cyberattack on U.S. power grid).

represent variations of a new and potentially devastating type of conflict for which U.S. law is unprepared.

These attacks are new for two principal reasons: the kind of attack is different from what has come before; and the attacker is a combination of participants, including state and nonstate actors, witting and unwitting contributors, and civilian and military personnel. These differences are particularly important because the legal tools available to law enforcement personnel have not caught up with the changes on the ground. Many of the attacks rely principally on cyber tools and have as their aim not to kill their enemies quickly but to sow political, social, or economic uncertainty and discord. The objective is destabilization and the means include both potentially violent and nonviolent means. And the attacks are different for a second reason: the kind of attacker is new. The apparent wrongdoers are not states, political parties with a military wing, or quasi-states.[9] Instead, they are a collection of like-minded individuals with some connections to each other and to a state, but not wholly a part of it. And they rely in large part on their ability to mobilize at least some unwitting civilian participants to inflict harms. As terrorism evolves, the time is right for a reexamination of available law enforcement tools to determine how to best address these attacks.

For prosecutors putting together cases against suspected terrorists, one of the most important tools of counterterrorism has been the designation of terrorist groups as foreign terrorist organizations.[10] Doing this requires the Secretary of State to assemble a dossier of information about the organization to determine that it is a foreign organization that engages in terrorist activity that threatens the national security of the United States.[11] One of the consequences of such a designation is that prosecutors can easily target for prosecution supporters of designated organizations. There are two statutes that make it a crime to provide material support to terrorist organizations. One targets those who provide support for crimes that a terrorist commits or may be planning to commit.[12] The other targets those who provide support for designated terrorist organizations. This second material support statute allows prosecutors to obtain a conviction or use the threat of prosecution to secure cooperation, even if the defendant is unaware of any specific attack or plan or the

---

9. To be clear, I do not argue that the new terrorist threat is completely unprecedented. Instead, I argue that it represents a departure from the presumed type of organization against which U.S. legal tools have been mobilized. For a brief history of terrorism and terrorist groups, see generally WALTER ENDERS & TODD SANDLER, THE POLITICAL ECONOMY OF TERRORISM 14–20 (2006) (describing varieties of terrorist groups from 19th century through contemporary groups).

10. For a thorough analysis of the designation of foreign terrorist organizations and the implications of designation for organizations and individuals associated with them, see generally Wadie E. Said, *The Material Support Prosecution and Foreign Policy*, 86 IND. L.J. 543, 558–76 (2011).

11. *See* Antiterrorism and Effective Death Penalty Act (AEDPA), 8 U.S.C. § 1189(a)(1)(A)–(C) (2012).

12. AEDPA, 18 U.S.C. § 2339A (2012) (criminalizing the provision of support knowing that it will be "used in preparation for, or in carrying out" a terrorist act). For a description of the operation of the statute, see CHARLES DOYLE, CONG. RESEARCH SERV., R41333, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C. 2339 § A AND 2339 § B 2–12 (2016).

organization is not at that time planning a specific attack.[13] This allows law enforcement and counterterrorism personnel to act sooner than might otherwise be possible and leverage early-level cooperation to obtain information about other participants. For example, prosecutors are able to obtain a conviction before a terrorist act is carried out or even planned.[14]

In this Article, I take up one slice of what should be a broad re-examination of U.S. law and policy. I argue that the new attacks have been undertaken by entities that can and should be designated as foreign terrorist organizations. Doing this would permit prosecutors to target those who support these entities with tools that are not currently available. This Article is both a doctrinal argument that directly addresses the many legal hurdles that make designating groups, such as foreign hackers and troll farms, terrorist organizations a complicated endeavor, and a policy argument about how U.S. law and policy should respond to new modes of terrorism.

To make this case, I make two principal claims. First, on the doctrinal front, I argue that my proposed reconsideration of the kinds of entities that may be designated as terrorist organizations is consistent with existing law and with the purposes of 8 U.S.C. § 1189, the statute permitting designation. Making this case requires consideration of what it means for an entity to be an "organization," what activities constitute terrorism, and how this activity is similar to activity that is currently considered terrorism. Although the context is different, new organizations have similar structures and characteristics as organizations that have been designated already.[15] With respect to what constitutes terrorism, I argue that a harms-based approach is appropriate. The magnitude and type of harm done by the new organizations are similar to harm done by existing organizations.[16] Second, on the policy side, I argue that the problem of the entities that are threatening U.S. economic, governmental, and social infrastructure can be more effectively addressed if they are designated as terrorist organizations. Despite the attention paid to counterterrorism law and policy in the past two decades, the area of law is far from fully developed and has struggled to keep up with changes in the world. Designating these entities as foreign terrorist organizations would amount to an updating of law and policy to better combat an evolving threat.

Before moving on, a brief detour is in order to explain how the law can accommodate itself to novel or evolving issues. The law always struggles to catch up to current events. Legal institutions are conservative, relying on precedent to reach predictable results.[17] But events move quickly and sometimes the law must quickly evolve. International criminal law and its close relative international humanitarian

---

13. AEDPA, 18 U.S.C. § 2339B; *see also* DOYLE, *supra* note 12 (describing differences between two material support statutes).

14. *See, e.g.*, United States v. Mehanna, 735 F.3d 32, 47–49 (2013) (denying defendant's argument on appeal that a material support conviction could not rest on his translation of potentially incendiary materials and posting the translations online).

15. *See infra* Section III.A.

16. *See infra* Section III.A.

17. For a full theory of legal change, see generally Oona A. Hathaway, *Path Dependence in the Law: The Course and Pattern of Legal Change in a Common Law System*, 86 IOWA L. REV. 601 (2001). Hathaway argues that legal evolution is inevitably, and powerfully, connected to past decisions, which can slow the process of change and determine its course.

law have developed in response to events, many of which were unanticipated and seemingly beyond the reach of the law to address.[18] To be clear, I do not argue that it is possible, or even desirable, to identify convenient principles of international criminal law and import them wholesale into the application of U.S. domestic counterterrorism law. There are significant differences between the two areas of law that militate against that approach.[19] Instead, I argue that international criminal law has confronted this problem—a poor fit between new problems and old principles of law—and developed the interpretive means by which to address them.

The horrors of the Holocaust were a principal catalyst for the development of the crime of genocide, and the Nuremberg prosecutions for these crimes were the first formal application of the prohibition of crimes against humanity.[20] More recently, when armed groups in Sierra Leone began the practice of forcing young women into conjugal relationships with fighters, including labeling the young women as their "wives," international criminal law had the doctrinal space to include this behavior as a separate crime against humanity.[21] The evolution of international criminal law and international humanitarian law takes place within well-known constraints, however. Chief among them is the legality principle, also known as *nullum crimen sine lege*, which permits prosecution only if the allegedly criminal activity was defined as a crime and those who engaged in the substantive conduct were subject to individual criminal prosecution at the time the conduct occurred.[22]

In addition to this formal limitation, the law has evolved principles for reasoning by analogy that could be usefully applied to any decision to designate a new terrorist entity as a foreign terrorist organization. One example to look for is the rough equivalence of harms or rights. For example, when determining if some conduct can

---

18. One prominent example is the ways that international criminal law has addressed crimes of sexual violence. For a comprehensive treatment of the changing ways that rape under international law, see generally Phillip Weiner, *The Evolving Jurisprudence of the Crime of Rape in International Criminal Law*, 54 B.C. L. REV. 1207 (2013).

19. *See generally* Hari M. Osofsky, Note, *Domesticating International Criminal Law: Bringing Human Rights Violators to Justice*, 107 YALE L.J. 191 (1997) (analyzing areas of difference and convergence between international criminal law and domestic legal systems).

20. *See generally* Egon Schwelb, *Crimes Against Humanity*, 23 BRIT. Y.B. INT'L L. 178 (1946) (describing the doctrinal history of crimes against humanity and the crime of genocide).

21. Prosecutor v. Brima, Case No. SCSL-2004-16-A, Judgment, ¶¶ 187–96 (Feb. 22, 2008). The Appeals Chamber held that even if "forced marriage shares certain elements with sexual slavery . . . there are also distinguishing factors," which included a consideration of the different harms associated with each offense. *Id*. ¶ 195. Importantly, the Appeals Chamber concluded that the harms associated with each offense were both distinct from each other—meaning that each crime was capturing some aspect of harm not captured by the other—and of similar magnitude. *Id*. ¶¶ 199–201.

22. STEVEN R. RATNER, JASON S. ABRAMS & JAMES L. BISCHOFF, ACCOUNTABILITY FOR HUMAN RIGHTS ATROCITIES IN INTERNATIONAL LAW 23–24 (3rd ed., 2009) (describing contours of the legality principle). For a comprehensive argument regarding the role the legality principle plays in the development of international criminal law, see generally Mohamed Shahabuddeen, *Does the Principle of Legality Stand in the Way of Progressive Development of Law?*, 2 J. INT'L CRIM. JUST. 1007 (2004). Shahabuddeen argues that, if the elements of new crimes are constructed in a way that comports with established crimes, the legality principle need not block the evolution of the law. *Id.* at 1014.

be prosecuted as an international crime, courts often attempt to determine if the harms caused by the underlying conduct are roughly equivalent to the harms caused by existing, accepted crimes.[23] Further, courts sometimes attempt to determine if the nature of the right violated by the underlying conduct, such as the right to life or the right to be free from arbitrary arrest, is roughly equivalent to the rights protected by existing, accepted crimes.[24]

To illustrate this approach, consider the prosecution of several leaders of one of the armed factions in Sierra Leone. They were charged with the crime of forced marriage, among other things.[25] In the prolonged violence in Sierra Leone, fighters from all sides abused women in myriad ways.[26] During and after the conflict there was ample evidence of rape and other sexual violence, sexual slavery, kidnapping, and forced labor.[27] The Statute of the Special Court for Sierra Leone (SCSL) permitted the tribunal to try defendants for the crimes against humanity of rape, sexual slavery, forced prostitution, forced pregnancy, sexual violence, and torture.[28] All of the actions described above amounted to crimes that would fit squarely into existing categories of crimes against humanity.

This is not the approach that prosecutors pursued. They charged Brima and other defendants from the leadership of the Armed Forces Revolutionary Council (AFRC)[29] with the crime against humanity of "forced marriage."[30] Prosecutors alleged that forced marriage was a means by which the defendants committed "other

---

23. *See, e.g.*, Micaela Frulli, *Advancing International Criminal Law: The Special Court for Sierra Leone Recognizes Forced Marriage as a 'New' Crime Against Humanity*, 6 J. INT'L CRIM. JUST. 1033, 1037–40 (2008) (arguing that harms must be both distinct from each other and comparable in magnitude to support the creation of a new crime in a way that is consistent with the legality principle).

24. *See, e.g.*, Neha Jain, *Forced Marriage as a Crime Against Humanity*, 6 J. INT'L CRIM. JUST. 1013, 1030–31 (2008) (arguing that the harms associated with each crime must violate rights of similar magnitude).

25. Prosecutor v. Brima, Kamara & Kanu, Case No. SCSL-2004-16-PT, Further Amended Consolidated Indictment, ¶¶ 51–57 (Feb. 18, 2005) (indicting defendants for the crime against humanity of "other inhumane acts," including "forced marriage").

26. *See generally* LOUISE TAYLOR, HUMAN RIGHTS WATCH, WE'LL KILL YOU IF YOU CRY: SEXUAL VIOLENCE IN THE SIERRA LEONE CONFLICT (2003) (describing, based on interviews with survivors and witnesses, sexual violence against women and girls in Sierra Leone during the conflict).

27. *See generally* Michelle Staggs Kelsall & Shanee Stepakoff, *"When We Wanted to Talk About Rape": Silencing Sexual Violence at the Special Court for Sierra Leone*, 1 INT'L J. TRANSITIONAL JUST. 355 (2007) (describing extent of sexual violence in conflict in Sierra Leone and experiences of survivors who were prepared to testify about it).

28. Statute of the Special Court for Sierra Leone arts. 2–4, Jan. 16, 2002, 2178 U.N.T.S. 145, (detailing the powers of the SCSL, including the ability to prosecute crimes against humanity, war crimes, and other serious violations respectively).

29. The AFRC was one of several organized armed groups fighting in Sierra Leone. *See generally* Prosecutor v. Brima, Kamara & Kanu, Case No. SCSL-2004-16-PT, Further Amended Consolidated Indictment, ¶¶ 7–17 (describing combatant parties in conflict in Sierra Leone).

30. Prosecutor v. Brima, Kamara & Kanu, Case No. SCSL-2004-16-A, Judgment, ¶ 175 (Feb. 22, 2008).

inhumane acts," a crime in the statute.[31] And prosecutors sought convictions even when they were prosecuting the defendants for most of the same underlying violent conduct against the same victims.[32] Prosecutors took the approach they did not because there was insufficient evidence of those other crimes—rape, kidnaping, and so forth—but because those crimes did not precisely capture the unique nature of the harms done to women who were forced into "marriages" with their captors and abusers.[33]

In *Brima*, prosecutors maintained that this was appropriate because one of the purposes of the tribunal was to address as many of the most substantial harms as possible.[34] I argue that this move was significant for another reason, the legal strategy the prosecutors chose when justifying their charging decision.[35] When they were charging and justifying the crime of forced marriage, they started by using existing doctrinal space. They showed that the new crime addressed harms that were of equivalent weight to the harms addressed by other crimes in the same category but that the harms covered by the new crime were not otherwise addressed.[36] There was no crime that addressed the harms that flowed from forced conjugal association, for example.[37] Finally, they showed that the elements of the new crime were not themselves novel.[38] Put differently, prosecutors argued, and the tribunal concluded, that even if the finished dish was new, the ingredients were familiar and had been used before.

A second important means of permitting the law to evolve in a principled way is to look closely at the object and purpose of the law or provision at issue to determine if it was created to address that particular kind of behavior. To do this, courts typically rely on Article 31 of the Vienna Convention on the Law of Treaties, which provides that treaties should be interpreted in light of their "object and purpose."[39] In

---

31. *See* Statute of the Special Court for Sierra Leone art. 2.i, Jan. 16, 2002, 2178 U.N.T.S. 145, (permitting the prosecution of the crime against humanity of "[o]ther inhumane acts"); Prosecutor v. Brima, Kamara & Kanu, Case No. SCSL-2004-16-A, Judgment, ¶¶ 175–76 (describing prosecution's decision to charge "forced marriage" as the crime against humanity of other inhumane acts).

32. Prosecutor v. Brima, Kamara & Kanu, Case No. SCSL-2004-16-A, Judgment, ¶¶ 187–96 (describing similarities between forced marriage and other crimes of sexual violence).

33. *See id.* ¶¶ 177–78 (describing prosecution arguments that the harms associated with forced marriage were different from those associated with other crimes of sexual violence).

34. *See* Statute of the Special Court for Sierra Leone art. 1, ¶ 1, Jan. 16, 2002, 2178 U.N.T.S. 145 (stating that the purpose of the SCSL was to "prosecute persons who bear the greatest responsibility for serious violations of international humanitarian law and Sierra Leonean law").

35. *See* Prosecutor v. Brima, Kamara & Kanu, Case No. SCSL-2004-16-PT, Indictment, ¶¶ 51–57, (May 13, 2004) (indicting defendants for the crime against humanity of "other inhumane acts," including "forced marriage").

36. *See* Prosecutor v. Brima, Kamara & Kanu, Case No. SCSL-2004-16-PT, Appeals Judgement, ¶¶ 177–78 (Feb. 22, 2008) (describing prosecution arguments that the harms associated with forced marriage were different from those associated with other crimes of sexual violence).

37. *See id.* ¶¶ 187–96.

38. *Id.* at ¶¶ 197–98 (finding that the crime did not violate the legality principle).

39. *See* Vienna Convention on the Law of Treaties art. 31, Jan. 27, 1980, 1155 U.N.T.S.

practice, this approach has come to mean that courts look for one or two primary purposes, which are typically the protection of civilians or an end to impunity for wrongdoing, when interpreting international criminal law or applying existing law to new situations.[40]

I. THE PROBLEM: NEW ATTACKS AND NEW ATTACKERS

In this Part, I describe the attacks on the 2016 U.S. elections and attempts to attack critical infrastructure in Europe and elsewhere. The purpose of this Part is twofold. First, by describing the attacks in some detail, I aim to demonstrate that the harms they inflicted are similar in magnitude and type to those inflicted in other terrorist attacks by groups that have been designed as foreign terrorist organizations. Second, this Part helps to show that the available law enforcement tools are inadequate. Taken together, this helps to make the case that U.S. policy is confronting a threat that is significant and for which the United States is unprepared.

A. Attacks on U.S. Elections

The attacks on the 2016 U.S. elections comprised multiple fronts and included a number of attackers. In this Section, I describe the broad outlines of what happened to show the importance of the attacks and some of their social effects. It is important to note that there have been, and continue to be, several overlapping investigations into the many ways that Russian entities interfered in U.S. elections. Both chambers of the U.S. Congress have undertaken investigations.[41] The Attorney General appointed Robert Mueller to investigate certain aspects of these activities.[42] And journalists have doggedly pursued the many tendrils of the story.[43] There is, as yet,

---

331 (providing that a "treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose").

40. *See* Darryl Robinson, *The Identity Crisis of International Criminal Law*, 21 LEIDEN J. INT'L L. 925, 935–36 (2008) (describing the purposes that courts identify when interpreting international criminal law statutes).

41. *See, e.g.*, David E. Sanger & Catie Edmondson, *Russia Targeted Election Systems in All 50 States, Report Finds*, N.Y. TIMES (July 24, 2019), https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html [https://perma.cc/WEB4-LT7P] (reporting results of Senate investigation into Russian interference in U.S. elections); Charlie Savage & Matthew Rosenberg, *Five Takeaways from the House Report on Russian Election Meddling*, N.Y. TIMES (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/us/politics/takeaways-house-intelligence-committee-russian-election-interference.html [https://perma.cc/Y355-TZ3S] (describing results of the investigation undertaken by the House of Representatives into Russian interference in U.S. elections).

42. OFFICE OF THE DEPUTY ATTORNEY GEN., *supra* note 2.

43. Reporting on Russia's role in the 2016 elections has been extensive. For just one example, see generally MICHAEL ISIKOFF & DAVID CORN, RUSSIAN ROULETTE: THE INSIDE STORY OF PUTIN'S WAR ON AMERICA AND THE ELECTION OF DONALD TRUMP (2018) (describing aspects of Russia's interference in the 2016 U.S. elections).

no complete, authoritative history of the problem.[44] Nonetheless, it is important to describe what is known at this point.

There were three basic prongs of the attacks on the U.S. electoral processes: a social influence campaign, an attack on the Democratic National Committee's database, and a series of attempts to gain access to state electoral system databases.[45] In the assessment of the U.S. intelligence community, the social influence campaign was ordered by Russian President Vladimir Putin[46] and carried out by individuals and organizations affiliated with Russia's Internet Research Agency.[47] The goal was to push voters toward candidate Donald Trump and away from candidate Hillary Clinton.[48] The consequences of this effort were to exacerbate existing social tensions and reduce voter turnout based on false claims.[49] The social influence campaign had several facets, all based on the goal of bolstering candidate Trump and harming the prospects of candidate Clinton.[50] Indeed, the U.S. intelligence community concluded that "Putin, his advisers, and the Russian Government developed a clear preference for . . . Trump over . . . Clinton."[51] One component of Russia's interference was a concerted attempt to suppress the number of African-American voters through social media messages suggesting that voting was futile or that neither candidate would address issues important to many African Americans.[52] Another part of the campaign

---

44. The report issued by Robert S. Mueller is likely the most comprehensive treatment of the subject. *See generally* 1–2 ROBERT S. MUELLER III, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION (2019), https://www.justice.gov/storage/report.pdf [https://perma.cc/T2H8-8ZJJ].

45. DIRESTA ET AL., *supra* note 1. In this Part, I rely heavily on the report from New Knowledge, an analytics firm contracted by the Senate Select Committee on Intelligence (SSCI), analyzing all of the social media turned over to the SSCI in its investigation into Russian interference in the U.S. elections and other attempts to attack U.S. electoral processes. *Id.* at 3. The report is based on tens of millions of posts, tweets, videos, and other electronic engagements (collectively engaged with approximately 337 million times) turned over to the SSCI by Facebook, Google, Instagram, YouTube, and other companies. *Id*. at 7. The report's findings do not represent official U.S. government findings, *id*. at 3, but they are based on the most comprehensive dataset publicly available.

46. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 1 (noting that the intelligence community "assess[ed] with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election").

47. *See generally* Indictment at ¶¶ 1–24, United States v. Internet Research Agency LLC (D.D.C. filed Feb. 16, 2018) (No. 1:18-cr-0032-DLF) (describing web of organizations and individuals who allegedly worked together to interfere in U.S. elections).

48. DIRESTA ET AL., *supra* note 1.

49. See PHILIP N. HOWARD, BHARATH GANESH, DIMITRA LIOTSIOU, JOHN KELLY & CAMILLE FRANÇOIS, THE IRA, SOCIAL MEDIA AND POLITICAL POLARIZATION IN THE UNITED STATES, 2012-2018 at 17–20 (2018) (describing Russia's attempts to polarize the U.S. public through misinformation during the 2016 elections).

50. DIRESTA ET AL., *supra* note 1, at 9 (describing Russia's attempts to benefit candidate Trump and harm candidate Clinton).

51. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 1.

52. *See, e.g*., Scott Shane & Sheera Frenkel, *Russian 2016 Influence Operation Targeted African-Americans on Social Media*, N.Y. TIMES (Dec. 17, 2018), https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html [https://perma.cc/KFU8-TK7N] (describing campaign by Internet Research Agency to suppress the turnout of African-

attempted to bolster the case for candidate Trump by, among other things, spreading false but inflammatory stories designed to appeal to right-wing voters and by encouraging those on the extreme right to become more engaged.[53] Data from U.S. social media companies showed that those involved in the campaign worked their way into online chatrooms to connect with Americans who already held extreme views to steer them either toward candidate Trump or away from voting at all.[54]

The second prong was the coordinated attack on the Democratic National Committee's database and the subsequent release of data related to the Hillary Clinton campaign.[55] Using an identity that was falsely identified as an independent Romanian hacker, the Russian-led effort obtained personal email information from U.S. political operatives.[56] The hackers sent emails to members of the Clinton campaign to obtain their confidential login information.[57] They used this information to gain access to the entire network of the Democratic National Committee, obtaining information about election strategy and other matters. The hackers then shared this information with intermediaries who ensured that it would be posted on WikiLeaks and other websites, thus making it public.[58] The release of the information was also timed to do as much damage as possible to candidate Clinton over as long a time period as possible.[59]

The third prong involved attempts to gain access to state electoral system databases, including voter registration data.[60] Elements of the same organization that

---

American voters); *see also* PHILIP N. HOWARD ET AL., *supra* note 40, at 3 (finding, based on data provided to the SSCI, that "Russia's IRA activities were designed to . . . interfere in elections by . . . campaigning for African American voters to boycott elections or follow wrong voting procedures").

53. PHILIP N. HOWARD ET AL., *supra* note 49, at 3.

54. *See id*. at 39 (finding that the Russian social influence campaign "used a variety of fake accounts to infiltrate political discussion communities on the right and left . . . in order to exacerbate social divisions and influence the agenda").

55. DIRESTA ET AL., *supra* note 1; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 1, at 1–2. The United States indicted twelve individuals, charging them with participating in the hacking operation. Indictment at ¶¶ 22–31, United States v. Netyksho (D.D.C. filed July 13, 2018) (No. 1:18-cr-00215-ABJ) (describing means by which the defendants allegedly gained illegal access to databases belonging to the Democratic National Committee).

56. Ellen Nakashima & Shane Harris, *How the Russians Hacked the DNC and Passed Its Emails to WikiLeaks*, WASH. POST (July 13, 2018), https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html [https://perma.cc/Y9NA-7J6M].

57. *See* Indictment at ¶¶ 21–23, 26–31, United States v. Netyksho (D.D.C. filed July 13, 2018) (No. 1:18-cr-00215-ABJ) (describing means by which the defendants allegedly obtained damaging information from databases of the Democratic National Committee).

58. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 1, at 12–13 (finding that elements of Russia's intelligence directorate "used the Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks to release US victim data obtained in cyber operations publicly and in exclusives to media outlets").

59. Nakashima & Harris, *supra* note 56 (reporting that hacked emails were "released on WikiLeaks in a steady stream" through 2016, "ensuring that material embarrassing to Clinton's campaign would continue on a daily basis to deflect from her message in the weeks leading up to the election").

60. U.S. SENATE SELECT COMM. ON INTELLIGENCE, *supra* note 1.

engineered the other attacks have consistently attempted to gain access to the databases of state election officials.[61] These attacks took different forms. Based on information provided to the Senate Select Committee on Intelligence, a number of states observed that their election systems, including voter registration databases, were scanned for weaknesses.[62] In other states, the attacks went further. The attackers were able to penetrate the election infrastructure so deeply that they were in a position to "alter or delete voter registration data."[63] In addition, after the 2016 elections, the hackers appear to have attacked vendors who provide the election technology in some states.[64]

B. Attacks on Critical Infrastructure

An increasing focus of Russian-affiliated terrorists is critical infrastructure in the United States and Europe.[65] The most audacious of these attacks took place in December 2015 and targeted the power grid in Ukraine.[66] Beginning in the afternoon of December 23 and continuing for several hours, seven power substations were disconnected and unable to provide power. The outages affected approximately 225,000 people.[67] The attackers even disabled the backup power in two of the substations, which meant that officials working to respond to the attack were cut off and had no access to power themselves.[68] Officials were eventually able to use antiquated, manual workarounds to restore power.[69] The attackers had laid the

---

61. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 1, at 13 (finding that "Russian intelligence accessed elements of state or local electoral boards").

62. U.S. SENATE SELECT COMM. ON INTELLIGENCE, *supra* note 1, at 1 (reporting that at least "18 states had election systems targeted by Russian-affiliated cyber actors" and that this behavior included "vulnerability scanning directed at their Secretary of State websites or voter registration infrastructure").

63. *Id.* at 1–2 (reporting that "in a small number of states, these cyber actors were in a position to, at a minimum, alter or delete voter registration data" but "they did not appear to be in a position to manipulate individual votes or aggregate vote totals").

64. Nicole Perlroth, Michael Wines & Matthew Rosenberg, *Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny*, N.Y. TIMES (Sept. 1, 2017), https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html [https://perma.cc/P39Y-26M3] (reporting that hackers infiltrated the systems of VR Systems, a company providing election technology to states, and other similar companies).

65. *See, e.g.*, Nicole Perlroth & David E. Sanger, *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says*, N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html [https://perma.cc/U9JP-MBAH] (reporting on Russian attempts to attack power and water facilities in the United States and Europe).

66. *See* Zetter, *supra* note 6 (reporting steps in the attack on the power grid).

67. *See* ELEC. INFO. SHARING AND ANALYSIS CTR., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID iv (2016) (finding, based on extensive technical analysis of the attack, that 225,000 customers were affected for several hours).

68. Zetter, *supra* note 6 (reporting that the attacks "disabled backup power supplies to two of the three distribution centers, leaving operators themselves stumbling in the dark").

69. Kim Zetter, *Everything We Know About Ukraine's Power Plant Hack*, WIRED (Jan. 20, 2016), https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ [https://perma.cc/DLT2-8U9A] (reporting that because Ukraine's relatively old

groundwork for their eventual effort to seize control of the grid through a months-long phishing campaign in which they obtained the necessary personal credentials to gain access to the grid operators' network.[70]

The attack on Ukraine's power grid was not an isolated incident. In 2017, Russia-affiliated hackers had perpetrated a cyberattack against a petrochemical plant in Saudi Arabia.[71] In 2016, hackers affiliated with the Russian government hacked into the laptop of an official with an electricity company in Vermont and installed malicious code.[72] It was not clear to investigators whether the goal was to take over the grid or merely to assess its vulnerability for a future operation,[73] as had been done in the Ukraine case. Indeed, according to U.S. security officials, it appears that hackers are increasingly targeting critical infrastructure and focusing less on election systems.[74]

II. FTO DESIGNATION AND ITS IMPLICATIONS FOR LAW ENFORCEMENT

One of the cornerstones of U.S. counterterrorism policy has been to deny terrorists the resources they need to plan and carry out attacks.[75] In this Part, I show how this policy has been implemented through a range of mechanisms. The goal is to situate the Foreign Terrorist Organization (FTO) designation process in the larger counterterrorism strategy. I then describe the law of FTO designation. Taken together, this sets the stage for Part IV, in which I argue that designation of new

---

system still contained manual overrides, it was easier for officials to bring the grid back online that would have been possible in a more modern system lacking manual overrides).

70. For a thorough technical analysis of all known steps in the attack, see generally ELEC. INFO. ANALYSIS CTR., *supra* note 67, which describes plan that took several months and combined a range of hacking techniques to accomplish the goal.

71. Dustin Volz, *Researches Link Cyberattack on Saudi Petrochemical Plant to Russia*, WALL ST. J. (Oct. 23, 2018), https://www.wsj.com/articles/u-s-researchers-link-cyberattack-on-saudi-petrochemical-plant-to-russia-1540322439 [https://perma.cc/ZPH5-ZFHV] (reporting that malicious code was used by hackers to gain control over a critical safety system in the plant).

72. Juliet Eilperin & Adam Entous, *Russian Operation Hacked a Vermont Utility, Showing Risk to U.S. Electrical Grid Security, Officials Say*, WASH. POST (Dec. 31, 2016), https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html [https://perma.cc/ZKJ3-4YKC] (describing hack of Burlington Electric by hackers associated with Russia).

73. *Id.* (reporting that "[t]he incursion may have been designed to disrupt the utility's operations or as a test to see whether they could penetrate a portion of the grid").

74. *Id.*; David E. Sanger, *Russian Hackers Appear to Shift Focus to U.S. Power Grid*, N.Y. TIMES (July 27, 2018), https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html?login=email&auth=login-email [https://perma.cc/4RSJ-TDFK] (reporting that the Department of Homeland Security found that "Russia's military intelligence agency had infiltrated the control rooms of power plants across the United States," which, in theory, would have given the attackers the power to "take control of parts of the grid by remote control").

75. *See* DOYLE, *supra* note 12, at 1 ("The two federal material support statutes have been at the heart of the Justice Department's terrorist prosecution efforts").

terrorist groups would be consistent with U.S. policy and that the doctrinal hurdles are not insurmountable.

A. FTO Designation in U.S. Policy

A recent hallmark of U.S. policy has been to attempt to prevent terrorist attacks rather than prosecuting terrorists after the fact. To do this, law enforcement personnel must have tools to acquire evidence before an attack is imminent so they can intercede and prevent the attack. This has meant a greater focus on the prosecution of individuals associated with terror plots or terrorist organizations, even if they play ancillary roles in these plots or organizations.[76] Prosecutors target individuals who do things such as talk about their support for ISIS, undertake weapons training, or indicate a desire to travel to Syria.[77]

U.S. policy has also focused on cutting off financial support for terrorists, which the U.S. government has attempted to do by imposing strict disclosure requirements on U.S. financial institutions, requiring foreign financial institutions that do business in the U.S. to comply with stricter regulations, and promoting greater sharing of financial information.[78] This strategy is designed to make it possible for financial institutions and law enforcement agencies to identify where funding comes from, where it goes, and whom it ultimately benefits, while not unduly restricting the flow of legitimate finance.

Another hallmark of U.S. policy has been to turn individuals vulnerable to prosecution into confidential informants as a way to identify other potential wrongdoers.[79] As with the prevention strategy, this practice is neither unprecedented nor novel. Prosecutors identify individuals who may be subject to prosecution and convince them to work as informants to help the prosecution build cases against other individuals.[80]

---

76. For a comprehensive analysis of this shift in policy, see Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. LEGIS. 1, 26–36 (2005). Chesney argues that the shift in policy came after then-Attorney General John Ashcroft concluded that prevention of terrorist attacks should take a higher priority than ensuring that any evidence gathered would be admissible in court. *Id.* at 27. This shift led to several strategy changes, including arresting individuals for lower-level crimes such as immigration violations or detaining them as material witnesses. *Id.* at 30–36.

77. *See, e.g.*, Press Release, U.S. Dep't. of Justice, Three Florida Men Sentenced for Conspiring to Provide Material Support to ISIS (May 16, 2018), at https://www.justice.gov /opa/pr/three-florida-men-sentenced-conspiring-provide-material-support-isis [https://perma.cc/6J2W-D9XU].

78. *See, e.g.*, U.S. DEP'T. OF THE TREASURY, TERRORIST FINANCE TRACKING PROGRAM: FACT SHEET (Aug. 2, 2010), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/TFTP%20Fact%20Sheet%20revised%20-%20(8-8-11).pdf [https://perma.cc/432Z-XQCR] (describing new regulations to monitor financial systems as part of counterterrorism strategy).

79. *See, e.g.*, Jesse J. Norris & Hanna Grol-Prokopczyk, *Estimating the Prevalence of Entrapment in Post-9/11 Terrorism Cases*, 105 J. CRIM. L. & CRIMINOLOGY 609, 617–19 (2016) (describing FBI's strategy of using confidential informants in terrorism cases).

80. For an analysis of the abuses that can occur in such cases, see generally COLUMBIA LAW SCHOOL HUMAN RIGHTS INSTITUTE, ILLUSION OF JUSTICE: HUMAN RIGHTS ABUSES IN US

All of these strategies depend, at least in part, on the ability of prosecutors to target individuals for providing material support to a designated terrorist organization before there is an extant terrorist plot. Counterterrorism and law enforcement officials count this as one of the most important tools in the fight against terrorism and have increasingly relied on it to build cases.

That tool is unavailable in the fight against the new terrorism that Russian hackers and others have directed against the United States and others in the West over the past several years. In this Article, I argue that this tool should be available to prosecutors; there is doctrinal space for it in existing law. Making this tool available does not require a radical reimagining of existing law. Instead, it requires attention to the principles that have formed the foundation for existing rules and a willingness to adapt those rules to changed conditions.

Part of the reason that the law has yet to catch up fully with the new forms of terrorism is simply a lack of imagination. Put differently, just as ordinary forms of work have evolved, so have terrorist entities. And the law has not yet adjusted. The U.S. government has been in the business of designating entities as FTOs since 1997.[81] As of mid-2019, there are sixty-nine entities that have been designated as FTOs by the U.S. State Department.[82] So far, those entities have all been organized, hierarchical entities with clear leadership; some semblance of command structure; and some degree of organization, coherence, and integrity. The current law enforcement model is built on the assumption that terrorist organizations are such standing entities with some kind of core organizational structure. To be sure, these organizations are neither rigid nor unchanging, and their structures may not mimic that of the U.S. military, for example. But roughly speaking, existing law is based on the assumption that terrorist organizations are like traditional corporations: well organized, ideologically coherent, with identifiable boundaries. They may have suppliers or financiers, but all involved know whom they are working for and with. The designation of an entity as an FTO is done according to standards that appear to be based in a classical theory of the firm, but the world is changing.

For many years, there have been good reasons to challenge that assumption, particularly with organizations such as al-Qaeda or the Islamic State. Even conventional organizations are constantly evolving, splintering, combining with other groups, and adding and shedding members.[83] Policymakers and prosecutors have responded in two principal ways. First, policymakers have identified these new

---

TERRORISM PROSECUTIONS (2014), https://web.law.columbia.edu/sites/default/files/microsites/human-rights-institute/files/report_final_draft.pdf [https://perma.cc/Z7BN-RMFT] (cataloging the ways that material support charges have been used to manipulate vulnerable defendants).

81. Designation occurs pursuant to 8 U.S.C. § 1189 (2012). The first designations under the statute occurred in 1997, when twenty organizations were designated. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-629, COMBATING TERRORISM: FOREIGN TERRORIST DESIGNATION PROCESS AND U.S. AGENCY ENFORCEMENT ACTIONS 5 (2015) (noting that the first twenty designations occurred in 1997) [hereinafter GAO, COMBATING TERRORISM].

82. JOHN W. ROLLINS, CONGRESSIONAL RESEARCH SERVICE, 7–5700, IN FOCUS: FOREIGN TERRORIST ORGANIZATION (FTO) 2 (2019).

83. *See* Chesney, *supra* note 76, at 72–75 (cataloging evidence of shifts in terrorist organization structure and arguing that existing law is based on outdated assumptions).

splinter groups as independent entities and designated them as FTOs. For example, in 2004, the State Department designated the Islamic State of Iraq and the Levant (or ISIL) as an FTO.[84] Since then, various branches of ISIL have been separately designated as FTOs, including ISIL-Sinai Peninsula, ISIL-Khorasan, ISIL in Libya, and ISIS branches in Bangladesh, the Philippines, and West Africa.[85] This strategy recognizes the shifts taking place on the ground but has progressed slowly.

Second, prosecutors have responded to changes in the nature of terrorist groups by stretching the definition of "material support" to cover activity that is further and further from the core of the organization. A person can be guilty of material support for activities that are increasingly disconnected from actual terror operations. For example, translating controversial material and posting it on a website or listserv that is frequently used by people who are connected to a designated terrorist organization may be sufficient for a material support charge.[86] The advent of looser terrorist structures, like that of al-Qaeda or similar groups, is a variation on the traditional theme, not a different approach altogether. The core organization is present and known to all, but the various cells may not know each other or closely coordinate.

The new terrorist entities are different. They have more in common with new forms of project-based work arrangements than they do with traditional terrorist organizations. The entity may have come into existence only for a specific task, such as hacking the power grid in the Ukraine or influencing the elections in the United States. The entity likely has leadership and direction, but not a hierarchy or traditional organization structure. The various participants may not know each other or may know each other only through online aliases. The participants operate as a kind of team of freelancers, rather than as soldiers in the forces of a quasi-state or as the armed wing of a political party. Based on the available information, it is this kind of entity that appears to have conducted the attacks on the U.S. presidential election and other attacks in Europe since 2015.[87]

Current U.S. policy appears to be based on the structure of the entity rather than on its activities, capacity to inflict harm, or purpose, but this result is not dictated by the law. Existing law could be used to designate entities such as those which interfered in the U.S. elections as FTOs, thereby enabling prosecutors to use a tool that has proven invaluable in other cases. To make this shift, there are two principal doctrinal issues that must be resolved. First, the statute, 8 U.S.C. § 1189, requires that the entity be an "organization" but does not define or provide any guidance as to what this term means.[88] To fill this gap, I draw on interdisciplinary literature relating to work arrangements to show that the entities that appear to have committed

---

84. *See* CONG. RESEARCH SERV., *supra* note 82.

85. *Id.*

86. *See, e.g.*, United States v. Mehanna, 735 F.3d 32, 47–49 (2013) (denying defendant's argument on appeal that a material support conviction could not rest on his translation of potentially incendiary materials and posting the translations online).

87. *See* Oren Dorell, *Alleged Russian Political Meddling Documented in 27 Countries Since 2004*, USA TODAY (Sept. 7, 2017, 9:06 AM), https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/ [https://perma.cc/KQ35-MUHQ] (reporting that Russia had interfered in at least twenty-seven elections in Europe and North America since 2004).

88. 8 U.S.C. § 1189(a)(1)(A) (2012).

the attacks on the United States and Western Europe have all the hallmarks of an organization and can meet the statutory definition contained in 8 U.S.C. § 1189. Second, the activities must constitute either "politically motivated violence" or a "violent attack."[89] To address this issue, I draw on the history of the law of terrorism to show that the activities undertaken by the entities that are the subject of my argument are the kind of attacks that the law has attempted to address. They may not have been violent in the same way as an improvised explosive device or a car bomb, but their effects threatened human life and disruption on a scale and of a kind similar to attacks that are commonly understood as violent attacks.

Overcoming these doctrinal hurdles will not eliminate all possible complications or challenges. One obvious and important issue is timing. The process of designating a terrorist organization has both legal and political elements. The State Department is required to assemble evidence about the entity and determine if it meets the necessary criteria.[90] The current process involves seeking and assessing information from sixteen federal agencies or departments across the government.[91] For the tool to be most useful to prosecutors, the assessment process must be faster and more focused on the entity's activities and purpose rather than on its structure.

The United States, and many other states, maintain a number of terrorism-related watch lists. These lists, broadly conceived, create a process by which some part of the government makes factual findings about an individual or organization, puts that individual or organization on a list, and imposes legal restrictions on that individual or organization as a consequence.[92] The FTO designation originated in the 1996 Antiterrorism and Effective Death Penalty Act, which amended the Immigration and Nationality Act.[93] At the time, proponents argued that the purpose of the statute was to give the government an additional tool to cut off support for terrorist organizations.[94] Terrorist funding was one main target. The U.S. government has long argued that cutting off terrorists' funding was an essential component of the

---

89. The requirement of "politically motivated violence" comes from 22 U.S.C. § 2656f(d)(2) (2012). The "violent attack" language comes from 8 U.S.C. § 1182(a)(3)(B)(iii) (2012). To be sure, the statute does not require a violent attack in all cases. Other possible forms of "terrorist activity" under the statute involve actions like hijacking aircrafts or ships, detaining persons and threatening to kill them, or assassination. *See id.* Those issues are obviously not implicated in my argument.

90. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 81, at 5–8 (describing the process used by the State Department to assemble evidence used to designate terrorist organizations).

91. *See id.* at 21.

92. The U.S. State Department maintains a comprehensive list of designated organizations. There are currently sixty-nine designated organizations. *See* U.S. DEP'T OF STATE, *Foreign Terrorist Organizations*, STATE.GOV, https://www.state.gov/foreign-terrorist-organizations/ [https://perma.cc/32VW-FMZ3]. The European Union maintains multiple lists of people and organizations for similar purposes. *See* COUNCIL OF THE EUR. UNION, *EU Terrorist List*, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list/ [https://perma.cc/46EJ-JXDA].

93. CONG. RESEARCH SERV., *supra* note 82, at 1.

94. *See generally* Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law*, 94 AM. J. INT'L L. 102, 117–24 (2000) (reporting the objectives of the U.S. government when enacting statute).

government's counterterrorism strategy.[95] Another principal objective was to make it easier to prosecute individuals who helped terrorist groups.[96] The FTO designation list was a way to help with both of these objectives. If a group was designated as an FTO, then its funding and its funders could be targeted without showing that the funding was connected to any particular terrorist plot.[97] Similarly, individuals who assisted the designated organization could be prosecuted even in the absence of evidence of a specific terrorist plot.

B. The Law of FTO Designation

In the Parts that follow, I first describe the details of the designation process. The process takes place within the executive branch without substantial judicial oversight. I then explain the legal consequences of designation and show why it is such an important tool for law enforcement.

1. Designation Process

The designation of an organization as an FTO is done entirely within the executive branch. Under the statute, the Secretary of State may designate an organization based on three findings. The Secretary must determine that the organization is (a) a foreign organization that (b) engages in terrorism or has the ability and intent to do so, and (c) that the terrorist activity threatens the security of the United States or U.S. nationals.[98] The State Department is charged with monitoring, and reporting on, terrorist activity around the world.[99] Its annual reports provide an overview of

---

95. *See generally* MARTIN A. WEISS, CONGRESSIONAL RESEARCH SERVICE, RS21902, TERRORIST FINANCING: THE 9/11 COMMISSION RECOMMENDATION (2005) (describing efforts to target terrorist financing).

96. Robert Chesney, *Anticipatory Prosecution in Terrorism-Related Cases*, *in* THE CHANGING ROLE OF THE AMERICAN PROSECUTOR 157, 162–69 (John L. Worrall & M. Elaine Nugent-Borakove eds., 2008) (describing strategy to reduce impediments to terrorism prosecutions).

97. 18 U.S.C. § 2339B(a)(1) (2012) (providing for prosecution of individuals who provide material support for designated FTOs).

98. Specifically, 8 U.S.C. § 1189(a)(1) provides as follows:

> The Secretary is authorized to designate an organization as a foreign terrorist organization in accordance with this subsection if the Secretary finds that--
>
> (A) the organization is a foreign organization;
>
> (B) the organization engages in terrorist activity (as defined in section 1182(a)(3)(B) of this title or terrorism (as defined in section 2656f(d)(2) of Title 22), or retains the capability and intent to engage in terrorist activity or terrorism); and
>
> (C) the terrorist activity or terrorism of the organization threatens the security of United States nationals or the national security of the United States.

8 U.S.C. § 1189(a)(1) (2012).

99. *See* 22 U.S.C. § 2656f(a) (2012) (requiring the Secretary of State to assess and report on terrorist activities in foreign countries).

terrorist organizations working around the world[100] and can help it identify groups to consider for designation.[101] The State Department has established a multistep process to make this determination.[102] After it has identified a potential designee, the Department initiates an "equity check" designed to ensure that the designation will not interfere with some other national security or law enforcement priority or operation.[103] The State Department consults with other members of the intelligence community for their input as well.[104]

After the equity check, the State Department begins to assemble the administrative dossier necessary to make the designation decision.[105] This is the evidentiary record that will support the eventual decision.[106] When the record is fully assembled, the State Department shares this record with the Justice and Treasury Departments for their agreement to go forward.[107] It is on this record that the Secretary of State makes his or her decision.[108] Under the statute, the State Department must notify Congress before the organization is designated[109] and then must publish the designation decision in the Federal Register.[110]

What is noteworthy about this process is that it is entirely within the executive branch and does not provide meaningful opportunities for target organizations to contest the evidence on which the decision is made.[111] The designated organization

---

100. *See* U.S. DEP'T OF STATE, COUNTRY REPORTS ON TERRORISM 2017 (2018) (reporting on terrorist activity and counterterrorism efforts in countries around the world).

101. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 81, at 5 (reporting that the Bureau of Counterterrorism within the State Department "monitors the activities of terrorist groups around the world to identify potential targets for designation").

102. *See id.* at 6 (describing six-step process by which the State Department makes the designation decision). It is important to note that some of the steps in the State Department's process are not mandated by statute. Instead, they appear to be internal checks designed to regularize the process.

103. *Id.* at 7 (stating that the goal of the equity check is to determine if "law enforcement, diplomatic, or intelligence concerns should prevent the designation of the target organization").

104. *Id.* at 9–10 (reporting that the officials from the Departments of Defense, Justice, and Treasury and the CIA, NSA, National Counterterrorism Center, and National Security Council provide information during the equity check).

105. *Id.* at 10 (describing process of creating administrative record to support designation decision).

106. *See* 8 U.S.C. § 1189(a)(3) (2012) (requiring the Secretary of State to "create an administrative record" and permitting the Secretary to "consider classified information" in the process).

107. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 81, at 10 (reporting that the State Department seeks the concurrence of Justice and Treasury before finalizing the administrative record).

108. *See* 8 U.S.C. § 1189(a)(1) (providing that that the Secretary of State makes the designation decision); U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 81, at 6 (describing steps in the designation process).

109. *Id.* § 1189(a)(2)(A)(i) (requiring the Secretary of State to notify select members of Congress seven days before making the designation decision).

110. *Id.* § 1189 (a)(2)(A)(ii) (requiring publication of the designation decision in the Federal Register seven days after providing notice to Congress).

111. For a more substantial analysis of the process, see generally Randolph N. Jonakait, *A*

may seek judicial review of the decision.[112] However, the designated organization has no right to present evidence on its own behalf,[113] and the government is permitted to rely on classified information that it does not disclose to the organization but is provided to the reviewing court ex parte and in camera.[114] Courts may set aside the designation decision only if there is no substantial basis in the record to support it or if the Secretary of State acted unconstitutionally, illegally, or arbitrarily.[115] Congress has the power to revoke or block a designation decision for any reason.[116]

2. Legal Consequences of Designation

The designation of an organization has three principal consequences. First, it makes it possible for the government to prosecute individuals who provide material support to the organization.[117] Prosecution for material support for terrorism has become one of the U.S. government's most powerful tools in its counterterrorism strategy.[118] Using the material support statute, prosecutors may charge an individual with providing support for terrorism for virtually any assistance to a designated organization. Individuals who translate documents, engage in social media campaigns, or otherwise help the organization are vulnerable to prosecution.[119] In

---

Double Due Process Denial: The Crime of Providing Material Support or Resources to Designated Foreign Terrorist Organizations, 48 N.Y.L. SCH. L. REV. 125 (2003) (arguing that the designation process and its consequences violate the U.S. Constitution).

112. 8 U.S.C. § 1189(c) (detailing review process).

113. *Id.* § 1189(c)(2) (providing that judicial review "shall be based solely on the administrative record").

114. *Id.* § 1189(c)(2) (permitting the government to present classified components of the judicial record "ex parte and in camera").

115. *Id.* § 1189(c)(3) (providing bases for setting aside a designation decision).

116. *Id.* § 1189(a)(5) (providing that "Congress, by an Act of Congress, may block or revoke" a designation decision).

117. *See* 18 U.S.C. § 2339B(a)(1) (2012). The statue provides as follows:

> Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life. To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization (as defined in subsection (g)(6)), that the organization has engaged or engages in terrorist activity (as defined in section 212(a)(3)(B) of the Immigration and Nationality Act), or that the organization has engaged or engages in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989).

Id.

118. *See* DOYLE, TERRORIST MATERIAL SUPPORT, *supra* note 12, at 1 (noting, based on Congressional testimony of counterterrorism experts, that the "two federal material support statutes have been at the heart of the Justice Department's terrorist prosecution efforts").

119. *See, e.g.*, United States. v. Mehanna, 735 F.3d 32, 47–49 (1st Cir. 2013) (describing defendant's role in translating materials and posting the translations online); Matt Zapotosky, *Northern Virginia Teen Sentenced to 11 Years for Aiding Islamic State*, WASH. POST (Aug. 30, 2015), https://www.washingtonpost.com/local/crime/a-sophisticated-terrorist-supporter-or-a-troubled-teen/2015/08/27/9138cb6e-4c1e-11e5-bfb9-9736d04fc8e4_story.html

addition, the threat of a material-support prosecution has become an important additional tool for prosecutors seeking to obtain information on terrorist organizations.[120] Prosecutors, armed with the credible threat of a material-support prosecution, have powerful leverage to encourage those involved with terrorist groups to become informants or cooperating witnesses.

The second consequence of designation is that the Secretary of the Treasury may freeze the designated organization's assets and block its financial transactions.[121] This essentially closes the U.S. financial system to the organization and makes it illegal for individuals to conduct transactions with the organization.[122] Finally, individuals associated with designated organizations face travel bans or other restrictions.[123] They are barred from entering the United States and non-citizens face removal if they are in the United States.[124]

III. APPLYING FTO DESIGNATION TO THE NEW ATTACKS

I argue that the U.S. government should designate as terrorist organizations the entities that interfered in the 2016 elections and attacked critical infrastructure. To do so, the government could rely on existing legal tools. In this Part, I argue that there are three principal doctrinal issues relating to designation of the new organizations: whether they constitute an "organization" under the statute, whether their behavior threatens national security, and whether they engage in "terrorism" as that term is defined in U.S. law. To preview my conclusions, I argue that these doctrinal hurdles can be surmounted without unduly stretching the law.

The FTO designation process has both political and legal dimensions. The State Department must apply specific, albeit poorly defined, statutory criteria when it

---

[https://perma.cc/J8R8-6CUG] (reporting on the sentencing of Ali Amin, convicted of material support for terrorism for running a pro-ISIS Twitter account).

120. *See, e.g.*, Emily Stabile, *Recruiting Terrorism Informants: The Problems with Immigration Incentives and the S-6 Visa*, 102 CAL. L. REV. 235, 236–38 (2014) (describing FBI's recruitment of informants using threats of prosecution for material support).

121. 8 U.S.C. § 1189 (a)(2)(C) (2012). The statute provides as follows:

> Upon notification under paragraph (2)(A)(i), the Secretary of the Treasury may require United States financial institutions possessing or controlling any assets of any foreign organization included in the notification to block all financial transactions involving those assets until further directive from either the Secretary of the Treasury, Act of Congress, or order of court.

Id.

122. *See* 31 C.F.R. § 597.201 (2018) (requiring all financial institutions to "block all financial transactions involving any assets" of a designated organization); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 81, at 11–12 (describing steps taken by the U.S. government to freeze assets and block financial transactions of designated organizations).

123. *See* 8 U.S.C. § 1182(a)(3)(B), (F) (blocking entry or making deportable individuals who engage in terrorist activities or who are members of designated organizations); *Id.* § 1227(a)(4)(B).

124. *See id.* § 1182(a)(3)(B), (F) (blocking entry or making deportable individuals who engage in terrorist activities or who are members of designated organizations); *id.* § 1227(a)(4)(B).

decides to designate an entity.[125] But the State Department is not required to designate organizations, leading to disagreement among policymakers about whether to designate politically sensitive organizations.[126] In this Part, I first address the doctrinal issues that would arise if the State Department attempted to designate an entity like the one responsible for the interference in the 2016 elections. I then argue that the designation process must adapt to fit the entities that are conducting some of the most damaging terrorist attacks today.

The doctrinal hurdles are substantial but can all be addressed within the law. Put differently, my approach does not hinge on the passage of a new statute or the radical reinterpretation of existing doctrine. I address three doctrinal issues. First, I argue that entities like the one that interfered in the 2016 elections are organizations under the statute. The statute does not define the term and previous contested designated cases have not turned on whether an entity constitutes an organization. With this dearth of precedent, I draw on similar concepts from elsewhere in the law, including the law of armed conflict in international law, domestic conspiracy law, and interdisciplinary scholarly research on organizations. A second statutory criterion is that the activity of the designated organization must threaten the "security of United States nationals or the national security of the United States."[127] I argue that threats to civilian infrastructure and the integrity of political processes are threats to national security. Finally, a designated organization must engage in terrorist activity.[128] The relevant statutory definitions of terrorism require either "politically motivated violence"[129] or a "violent attack."[130] Attacks on political processes or threats to civilian infrastructure meet these criteria even if they do not cause death or direct physical trauma to individuals.

---

125. *See id*. § 1189(a)(1).

126. *See, e.g*., Stephen Roy Jackson, *Terror in Mexico: Why Designating Mexican Cartels as Terrorist Organizations Eases Prosecution of Drug Traffickers Under the Narcoterrorism Statute*, 4 NAT'L SEC. L.J. 83 (2015) (arguing that Mexican drug cartels meet the criteria for designation and that their designation would be consistent with U.S. law enforcement policy); Robert Chesney, *The Haqqani Network Not (Yet) a Designated Foreign Terrorist Organization*, LAWFARE (Sept. 23, 2011, 7:11 PM), https://www.lawfareblog.com/haqqani-network-not-yet-designated-foreign-terrorist-organization-ridiculous-i-agree-how-much-does [https://perma.cc/JFJ7-GR5C] (arguing that the Haqqani Network, a terrorist organization operating in Afghanistan and Pakistan, fits the criteria for designation); Audrey Kurth Cronin, *Why the Haqqani Network is Not on the Foreign Terrorist Organizations List*, FOREIGN AFF. (Dec. 21, 2011), https://www.foreignaffairs.com/articles/2011-12-21/why-haqqani-network-not-foreign-terrorist-organizations-list [https://perma.cc/FT9Q-SMGS] (describing political arguments over whether the Haqqani Network should be designated).

127. 8 U.S.C. § 1189(a)(1)(C).

128. *Id.* § 1189(a)(1)(B) (requiring that "the organization engages in terrorist activity (as defined in section 1182(a)(3)(B) of this title or terrorism (as defined in section 2656f(d)(2) of Title 22), or retains the capability and intent to engage in terrorist activity or terrorism").

129. 22 U.S.C. § 2656f(d)(2) (2012).

130. *See* 8 U.S.C. § 1182(a)(3)(B)(iii).

A. The Nature of an Organization Under the Statute

The FTO statute does not define what constitutes an organization under the law. The statute has been litigated but none of the reported decisions have addressed this issue. Prosecutors have asserted without proof, and defendants have accepted without contesting, that the targeted entity fulfilled the organization requirement under the statute. Even without guidance from the statute governing the designation of foreign terrorist organizations discussed above, there are other areas of the law from which a definition might be borrowed or adapted.[131] First, the U.S. statute that allows prosecutors to target Racketeer Influenced and Corrupt Organizations (RICO) provides some helpful guidance.[132] The RICO statute was enacted to allow prosecutors to target those whose activities contributed to organized crime.[133] Second, the development of joint criminal enterprise (JCE) liability in international criminal tribunals has allowed international prosecutors to prosecute individuals who contributed to an entity that caused harmful criminal conduct, even if the defendant was not herself the physical perpetrator of the crimes.[134] This doctrine has necessarily included some consideration of what constitutes a criminal "enterprise."[135] Finally, the development of the law of conspiracy in the United States has also required consideration of what transforms a collection of individuals into a conspiracy under the law.[136]

To preview my conclusions, I argue that the term "organization," when used in the FTO statute, is a collection of people who knowingly associate with others to accomplish a shared purpose or goal. To be sure, this simple definition is not likely to fully address the nuances of every potential entity, especially informal terrorist organizations. But it is sufficient to serve two purposes. First, by adopting this definition, prosecutors could target organizations that are destructive and actively engaging in terrorist activities but which have not formalized their structure or openly declared their existence. As the law now stands, terrorist organizations that are sufficiently sophisticated to work together and hide their existence have access to more tools and resources than those that openly declare their existence. The second purpose this definition serves is to provide practical guidance to prosecutors or

---

131. *See generally* Catherine H. Gibson, *Testing the Legitimacy of the Joint Criminal Enterprise Doctrine in the ICTY: A Comparison of Individual Liability for Group Conduct in International and Domestic Law*, 18 DUKE J. COMP. & INT'L L. 521 (2008) (describing the evolution of joint criminal enterprise liability).

132. *See* 18 U.S.C. §§ 1961–68 (1970).

133. *See* CHARLES DOYLE, CONG. RESEARCH SERV., R7-5700, RICO: A BRIEF OVERVIEW 1 (2016) [hereinafter DOYLE, RICO] (describing origins and purpose of RICO statute).

134. *See generally* Allison Marston Danner & Jenny S. Martinez, *Guilty Associations: Joint Criminal Enterprise, Command Responsibility, and the Development of International Criminal Law*, 93 CALIF. L. REV. 75 (2005) (providing history of joint criminal enterprise liability to hold accountable those who are not physical perpetrators of crimes).

135. *See* DOYLE, RICO *supra* note 133, at 12–13 (describing analysis of what constitutes an "enterprise").

136. *See generally* CHARLES DOYLE, CONG. RESEARCH SERV., R41223, FEDERAL CONSPIRACY LAW: A BRIEF OVERVIEW (2016) (hereinafter, DOYLE, CONSPIRACY LAW) (describing conspiracy law in the United States).

policymakers who wish to target an informal terrorist organization. To prove that an entity is an organization under the statute, policymakers might start by showing the pattern of interactions among the participants. They could show, for example, that some in the organization had decided to target a state's electoral processes and that they had communicated with others to develop the technical tools to do this. Or they could show that there was a pattern of financial transactions that benefitted those undertaking terrorist actions. As to the requisite shared purpose, policymakers could assemble evidence regarding the targets of terrorist actions and use that evidence to support an inference of shared purpose.

Under the RICO statute, an individual may be prosecuted if she participates in an enterprise which engages in criminal activity.[137] As the statute has been put to use, the purpose of the law is not to prohibit substantive conduct which would not otherwise be criminal. Instead, the statute gives tools to prosecutors to target individuals whose criminal activity is associated with others. Put another way, the RICO statute allows the government to prosecute individuals who work with, or through, organizations to commit criminal acts. Originally conceived to prevent organized crime from infiltrating legitimate businesses, the statute has been broadly used against a wide range of organizations that engage in criminal activity.[138]

Most relevant for my purposes is the way the statute and subsequent cases have defined the term "enterprise." Under the statute, an enterprise includes traditional entities like corporations or partnerships.[139] Importantly, it also includes "any . . . group of individuals associated in fact although not a legal entity."[140] Such an enterprise can include governmental and nongovernmental actors and may be formed to undertake legitimate activities or illicit activities.[141] To constitute an enterprise, the U.S. Supreme Court has held that an association-in-fact must have three structural elements: "a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose."[142] Put simply, such an enterprise is a "group of persons associated together for a common purpose of engaging in a course of conduct."[143] Thus, what matters is that there is some relationship among those involved in the enterprise and that it exists to serve a larger goal or purpose. Importantly, it does not require that all of those involved be known to each other, be in direct communication, or work according to any particular hierarchy.

The theory of JCE, developed by the International Criminal Tribunal for the Former Yugoslavia (ICTY), is another useful source of guidance on what constitutes

---

137. *See* DOYLE, RICO, *supra* note 133, at 2–6 (analyzing elements of RICO statute).

138. *Id.*

139. *Id.* at 12–13.

140. Under 18 U.S.C. § 1961(4) (2012), an enterprise "includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity."

141. *See* DOYLE, RICO, *supra* note 133, at 12–14 (analyzing organization elements of RICO statute).

142. Boyle v. United States, 556 U.S. 938, 946 (2009).

143. United States v. Turkette, 452 U.S. 576, 583 (1981).

an organization.[144] JCE is a mode of criminal liability that permits prosecutors to charge individuals who are not the physical perpetrator of a crime for criminal acts done by others if they were part of the same enterprise.[145] In creating the doctrine, the ICTY was interpreting its statute, which provided that people could be held individually criminally responsible for crimes if they "planned, instigated, ordered, committed, or otherwise aided and abetted in the planning or execution" of the crime.[146] The ICTY Appeals Chamber, in *Tadic*, held that the statute permitted conviction of individuals if they were part of a "joint criminal enterprise," that is: "several persons having a common purpose embark on criminal activity that is then carried out either jointly or by some members of this plurality of persons."[147] To convict, prosecutors must show, among other things, that there was a "plurality of persons" and a "common plan, design or purpose."[148] Importantly, the appeals chamber held that the prosecution did not need to show that the plurality of persons was organized in any particular way or that every element of the common purpose was known to all members.[149] Although the doctrine of JCE has continued to evolve and become ever more complex, its definition of what constitutes an enterprise remains useful. As with the RICO statute, what matters is that there is a collective of persons whose actions contribute to a larger plan or purpose. The collective need not have any particular structure or hierarchy. In addition, the collective need not think of or see itself as an enterprise. Put differently, a JCE need not declare itself such or even see itself as such.

The final area of law that is relevant to defining "organization" is the law of criminal conspiracy. Broadly speaking, under U.S. law, a conspiracy requires an agreement between two or more persons and an intent to undertake a certain objective.[150] The agreement need not be explicit or proven through direct evidence. But the government must prove that those involved in the conspiracy had a shared purpose and acted accordingly.[151]

---

144. *See generally* Danner & Martinez, *supra* note 134 (describing history and contours of joint criminal enterprise).

145. *See* Prosecutor v. Tadic, Case No. IT-94-1-A, Opinion and Judgement, ¶¶ 195–204 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997) (describing the three categories of joint criminal enterprise liability). *See generally* Danner & Martinez, *supra* note 134 (providing history of the development of liability for those who are not physical perpetrators of crimes).

146. The statute of the International Criminal Tribunal for the Former Yugoslavia was adopted by the U.N. Security Council in 1993 pursuant to S.C. Res. 827 and has been amended several times since then. Updated Statute of the International Criminal Tribunal for the Former Yugoslavia (Sept. 2009), http://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_en.pdf [https://perma.cc/2M46-89XY]. Article 7(1) of the statute provides as follows: "A person who planned, instigated, ordered, committed or otherwise aided and abetted in the planning, preparation or execution of a crime referred to in articles 2 to 5 of the present Statute, shall be individually responsible for the crime." *Id.*

147. *Tadic*, Case No. IT-94-I-A, ¶ 190.

148. *Id.* ¶ 227.

149. *See id.* ¶ 190.

150. *See* 2 WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 12.2 (3d ed. 2018) (describing elements of conspiracy under U.S. law).

151. *See* DOYLE, CONSPIRACY LAW, *supra* note 136, at 4–7 (describing requirements

The legal analogues on which I draw share two principal characteristics that are prominent in the social science literature on organizations and organizational structure. The first is that an organization—as distinct from a random collection of individuals—has some identifiable network of social relations.[152] Put differently, a necessary component of an organization is some regular pattern of interaction among the individuals who constitute it. The second requirement is that those in the organization must be united by some shared belief or goals.[153] These two characteristics—regular interactions and shared goals or beliefs—are present in each of the legal concepts, albeit to different degrees.

Scholars who study terrorism have devoted considerable attention to defining terrorism and terrorist groups, but most of that attention goes to other issues.[154] Although this literature does not fully address the question of what constitutes an organization, it is nonetheless helpful. First, the scant scholarship on the issue is consistent with the ways that legal policymakers and advocates have approached the issue. Second, the theoretical literature helps to illuminate what should not be part of the definition.

Much of the literature is focused on determining what kind of activity a group must engage in to be considered a terrorist organization.[155] For example, is a liberation group that uses violence a terrorist organization in the same way as anarchists or those who use violence in organized crime? But what is important for my purposes is to determine what constitutes an organization. That is, are there particular characteristics that must be present to conclude that any given grouping of people is a terrorist organization and not simply a group of like-minded and violent people? On this issue the literature is thin, but it does provide some helpful ideas. Some scholars borrow from the political scientist James Q. Wilson, who argued that organizations were formal voluntary associations.[156] This loose definition does not address how formal or organized the entity must be to be considered an organization. Counterterrorism policy makers have long recognized that the precise structure of a terrorist entity is less important than whether it is able to inflict harm or otherwise spread its message.[157] An entity might have a rigid hierarchical structure like the

---

regarding agreements among the participants in a conspiracy under U.S. law).

152. *See* PETER M. BLAU & W. RICHARD SCOTT, FORMAL ORGANIZATIONS: A COMPARATIVE APPROACH 2 (1962) (arguing that social organizations have a "structure of social relations in a group or larger collectivity of people").

153. *See id*. (arguing that those in a social organization have "shared beliefs and orientations that unite the members . . . and guide their conduct").

154. *See generally* Brian J. Phillips, *What Is a Terrorist Group? Conceptual Issues and Empirical Implications*, 27 TERRORISM & POL. VIOLENCE 225 (2015) (analyzing research on defining terrorist groups).

155. *See, e.g.*, BRUCE HOFFMAN, INSIDE TERRORISM 1–34 (1998). (analyzing various definitions of terrorism and terrorist activity).

156. *See generally* JAMES Q. WILSON, POLITICAL ORGANIZATIONS 31 (Princeton Univ. Press 1995) (describing the characteristics of organizations). Wilson's influence has extended to those who study terrorist groups. *See, e.g*., Phillips, *supra* note 154, at 227 (using Wilson's framework to understand terrorist organizations).

157. *See generally* U.S. ARMY TRAINING & DOCTRINE COMMAND, A MILITARY GUIDE TO TERRORISM IN THE TWENTY-FIRST CENTURY (2007) (analyzing capacity of organizations to

army of a state, or it might have a loose networked structure in which each cell operates almost independently. A terrorist organization can operate effectively with either structure. Thus, internal structure does not determine whether an entity is an organization.

The areas of law that I have considered are useful because they can provide some help in interpreting a term that is not defined in the FTO statute and do so along the same dimensions that organizational theory suggests are necessary. Borrowing legal definitions from one context and applying them in another should be done with some caution and particular attention to the purposes of each context. In each of the cases—RICO, JCE, and conspiracy—the principal issue is how to determine the individual criminal liability of a person who was part of, or associated with, a collection of individuals that committed criminal acts. Broadly speaking, the contested question is whether the individual has a sufficient connection to the group to justify, under some standard of law or morality, holding him or her responsible for criminal acts perpetrated by another person. The FTO context raises different questions: what are the characteristics of an "organization," and does the collection of governments, individuals, and entities involved in new terrorist attacks possess those characteristics? The question of individual criminal responsibility is a separate question. The effect of finding that an individual participated in a criminal conspiracy is to convict him or her of a crime. The effect of the designation decision is to label the organization as off limits. It does not convict the organization, or any individuals, of anything.

B. Threat to U.S. National Security

The FTO designation statute requires the Secretary of State to find that the organization's activity "threatens the security" of the United States or of U.S. nationals.[158] A designated organization may challenge the Secretary of State's decision on a number of grounds, [159] but it may not challenge the Secretary's national security conclusion.[160] Thus, the Secretary of State's conclusion that the

---

inflict damage and arguing that such capacity is more important than the structure of the organization).

158. 8 U.S.C. § 1189(a)(1)(C) (2012).

159. With respect to judicial review, the statute provides as follows at 8 U.S.C. § 1189 (c)(3):

> The Court shall hold unlawful and set aside a designation, amended designation, or determination in response to a petition for revocation the court finds to be--
>
> (A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;
>
> (B) contrary to constitutional right, power, privilege, or immunity;
>
> (C) in excess of statutory jurisdiction, authority, or limitation, or short of statutory right;
>
> (D) lacking substantial support in the administrative record taken as a whole or in classified information submitted to the court under paragraph (2), or
>
> (E) not in accord with the procedures required by law.

Id. § 1189(c)(3).

160. *See* People's Mojahedin Org. v. U.S. Dep't of State, 182 F.3d 17, 23 (D.C. Cir. 1999)

organization's activities threaten national security is reviewed only to ensure that there was evidence to support it and that it was not reached capriciously.[161] The FTO designation statute does not define the term "national security," but the term is defined elsewhere in the same chapter of the U.S. Code as relating to "the national defense and foreign relations of the United States."[162] This scant guidance does little to change the fact that determining what is a threat to the national security of a sovereign state is an inherently political and problematic task. It is beyond the scope of this Article to provide a positive theory of national security, but it is nonetheless important to provide at least some more insight into the concept of national security and to consider how and why attacks such as those against critical infrastructure in Ukraine and elsewhere or those against the electoral process in the United States might constitute a threat to national security.

Scholars and advocates have devoted attention to the concept of national security.[163] The FTO designation process is one of a number of tools that enable the U.S. government to identify and respond to external threats to U.S. interests. In the context of counterterrorism policy and the FTO designation process, the concept of national security is focused on external threats to the United States or U.S. interests. These threats might be against U.S. territory or persons, or against critical systems like transportation, and can come from a variety of sources. Consider the definition of national security put forward by the political scientist Richard H. Ullman, who argued that threats to national security could come in two broad categories.[164] The first category is actions that threaten "drastically and over a relatively brief span of time to degrade the quality of life for the inhabitants of a state."[165] This category might include terrorist attacks such as those on September 11, 2001. Ullman describes this category as including those incidents after which "the well-being of a society had been drastically impaired" in a way that was obvious.[166] The second category comprises those threats that significantly "narrow the range of policy choices available to the government of a state or to private . . . entities . . . within the state."[167] This category might include slower-developing threats or those whose impacts cause a cascade of problems that eventually affect the state at issue.[168] Perhaps the most useful definition in the context of the FTO designations statute

---

(noting that the national security issue is "nonjusticiable" under the statute, and that the nonjusticiability of that issue did not render the state's review procedures infirm).

161. 8 U.S.C § 1189(c)(3).

162. See *id.* § 1531(3), which provides that "the term 'national security' has the same meaning as in section 1(b) of the Classified Information Procedures Act." That Act, 18 U.S.C. app. 3, §§ 1–16 (2012), states that "National security . . . means the national defense and foreign relations of the United States." 18 U.S.C. app. 3, §1(b).

163. For an early treatment of the issue, see generally Arnold Wolfers, *"National Security" as an Ambiguous Symbol*, 4 POL. SCI. Q. 481 (1952). Wolfers argues that security connotes, among other things, the absence of external threats to national wealth or power. *Id*. at 484–85.

164. *See* Richard H. Ullman, *Redefining Security*, 8 INT'L SECURITY 129, 133–34 (1981) (arguing that threats to national security could be assigned to groups based on their characteristics).

165. *Id*. at 133.

166. *Id.*

167. *Id.*

168. *Id.* at 133–34.

might be one that comes from an environmental law scholar, who argues that a "threat to national security is a situation in which some of the nation's most important values are drastically degraded by external action."[169] This definition has the appropriate focus on external threats and is therefore consistent with the statute's reference to "foreign relations."

Perhaps more important than scholarship on the issue is the fact that this definition is consistent with the way that government officials have discussed potential attacks on critical infrastructure or attempts to undermine electoral processes.[170]

Policymakers from across the political spectrum have described the attempts to undermine the 2016 elections in the strongest possible terms, describing them as grave threats to U.S. national interests and ongoing threats to national security.[171] There have been, and continue to be, extensive investigations into the exact nature of the interference, and the investigations are premised on the argument that the interference represented a serious threat to national security. State and local election officials have begun to devote substantial resources to protecting the integrity of electoral systems, again premised on the argument that attempts to undermine elections would amount to a grave threat to national security.[172]

Similarly, security professionals in the U.S. government have argued that the protection of civilian infrastructure is vital. For example, in the 1990s, President Clinton appointed a commission to study the security of U.S. infrastructure.[173] That commission's report began by noting that "national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society."[174] That report detailed the ways that attacks—physical or cyber—on elements of civilian infrastructure would significantly erode quality of life, disrupt civilian activities, and undermine security.[175] More recently, President Obama issued

---

169. Marc A. Levy, *Is the Environment a National Security Issue?*, 20 INT'L SECURITY 35, 40 (1995).

170. *See, e.g.*, BRIAN E. HUMPHREYS, CONG. RESEARCH SERV., R45809, CRITICAL INFRASTRUCTURE: EMERGING TRENDS AND POLICY CONSIDERATIONS FOR CONG. 1–3 (2019) (describing history of concern for attacks on critical infrastructure); Thomas P. Bossert, *It's Official: North Korea is Behind WannaCry*, WALL ST. J. (Dec. 18, 2017), https://wsj.com /articles/its-official-north-korea-is-behind-wannacry-1513642537 [https://perma.cc/SS3Q-QHW5] (commentary by the homeland security advisor describing grave consequences of cyber-attacks on infrastructure).

171. *See, e.g.*, Jennifer Steinhauer, *Senate and House Leaders Call for Inquiry of Russian Hacking in Election*, N.Y. TIMES (Dec. 12, 2016), https://www.nytimes.com/2016/12/12/us /politics/mcconnell-supports-inquiry-of-russian-hacking-during-election.html [https://perma.cc/F6FW-99KA] (reporting that Republicans and Democrats strongly condemned interference in the election and had called for an investigation into the issue).

172. *See* SENATE SELECT COMM. ON INTELLIGENCE, 116TH CONG., REPORT ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 ELECTION: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE 49–52, REP. 116-XX, (describing the role of the states in addressing electoral interference).

173. *See* CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES, REPORT OF THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (1997).

174. *Id.* at IX.

175. *Id.* at 3–5.

a Presidential Policy Directive on the threats to civilian infrastructure.[176] As with the earlier report, that directive connected "the Nation's safety, prosperity, and well-being" to the maintenance of "secure, functioning, and resilient critical infrastructure."[177]

C. Defining Terrorism

Under the FTO state, the Secretary of State must find that the organization engages in terrorist activity,[178] which means it engages in "politically motivated violence"[179] or that it has conducted a violent attack.[180] Although much of U.S. law enforcement and foreign policy is devoted to countering terrorism and terrorist activity, there exists surprisingly little consensus around the concept and definition of terrorism.[181] U.S. statutes contain several different definitions of terrorism, which only adds to the conceptual confusion, much of which is beyond the scope of this Article. What most definitions share, however, is the requirement that the targeted behavior involve violence.[182] This requirement is the most significant doctrinal hurdle for my approach. In this Part, I argue that the U.S. should move beyond a formalist approach to defining terrorism to a more functional approach, which would accommodate terrorist activity that is not violent in any conventional sense, and that existing law would allow for such a shift in approach.

The FTO statute refers to two other statutes to define terrorism and both refer to violence.[183] This is consistent with most scholarly definitions of terrorism, which

---

176. Directive on Critical Infrastructure Security and Resilience, 2013 PUB. PAPERS 106 (Feb. 12, 2013).

177. *Id.* at 106.

178. The relevant portion of the statute, 8 U.S.C. § 1189(a)(1)(B) (2012), provides that the Secretary of State must find that "the organization engages in terrorist activity (as defined in section 1182(a)(3)(B) of this title or terrorism (as defined in section 2656f(d)(2) of Title 22) or retains the capability and intent to engage in terrorist activity or terrorism)."

179. 22 U.S.C. § 2656f(d)(2) (2012).

180. *See* 8 U.S.C. § 1182(a)(3)(B)(iii) (defining terrorism to include, among other activities, a "violent attack upon an internationally protected person . . . or upon the liberty of such a person").

181. This is not a new problem. For a survey of some of the attempts to define terrorism by policymakers, see generally Michael P. Scharf, *Defining Terrorism as the Peacetime Equivalent of War Crimes: Problems and Prospects*, 36 CASE W. RES. J. INT'L L. 359, 359 (2004) (arguing that the "problem of defining 'terrorism' has vexed the international community for decades"). There is perhaps even less scholarly consensus about how to define terrorism. *See* George P. Fletcher, *The Indefinable Concept of Terrorism*, 4 J. INT'L CRIM. JUST. 894 (2006). Fletcher argues that because the concept of terrorism is used so frequently and to describe so much behavior, it is impossible to arrive at a consensus definition. *Id.* at 895–900. Instead he argues that terrorism should be defined by resort to a collection of factors, some of which must be present for a given action to be described as terrorism but none of which must be present in every case. *Id*. at 910–11.

182. *See generally* Nicholas J. Perry, *The Numerous Federal Legal Definitions of Terrorism: The Problem of Too Many Grails*, 30 J. LEGIS. 249 (2004) (describing the various definitions of the term "terrorism" in U.S. law).

183. In 8 U.S.C. § 1189(a)(1)(B), the FTO statute refers to two other provisions of the

also typically include some mention of violence.[184] For example, Bruce Hoffman, a leading scholar of terrorism, argues that terrorism involves "the deliberate creation and exploitation of fear through violence or the threat of violence."[185] Walter Enders and Todd Sandler, other leading scholars of terrorism, define it as "the premeditated use or threat to use violence . . . in order to obtain a political or social objective."[186] But in these definitions, violence is serving as a kind of proxy for something more important. Violence is part of the definition of terrorism because some scholars assumed that without "violence or its threat, terrorists cannot make a political decision maker respond to their demands."[187] Violence is that which "inspire[s] terror in its victims and those indirectly affected."[188] It is the ingredient that serves to intimidate civilians.[189] Thus "the essence of terrorism lies in the intent behind the act of violence," which is to frighten civilians and disrupt important aspects of their lives.[190]

The attempts to disrupt the U.S. elections and the attacks on critical infrastructure in Europe highlight the need to move from a formalist definition of what constitutes a terrorist act to a functional one, and the FTO designation process is the appropriate venue to do so for several reasons. It is an inevitably political process. The Secretary of State must follow the statutory mandate but exercises great discretion throughout the process.[191] This is different from a criminal prosecution, where precision and specificity are necessarily more prominent.

Even more important than the appropriateness of the venue is the need to recognize that violence is simply not the only means by which these new terrorists can attempt to exert coercive force over political leaders or disrupt the lives of civilians. Consider the effects and potential effects of the interference with the U.S. elections. Competently managing the electoral process is among the most important civilian functions that a government undertakes. There are scores of examples of the grave consequences that can flow from electoral processes that are seen as tainted or unduly influenced by illegitimate considerations like foreign financing or interference. The harms caused by electoral interference are similar in kind and magnitude to those associated with events—like bombings or attacks by gunmen—that have long fitted comfortably within the definition of terrorism. Electoral

---

law—8 U.S.C. § 1182(a)(3)(B) and 22 U.S.C. § 2656f(d)(2)—for the definition of terrorism.

184. For a survey of legal definitions, including the identification of common elements, see generally Antonio Cassese, *The Multifaceted Criminal Notion of Terrorism in International Law*, 4 J. INT'L CRIM. JUST. 933 (2006). For a useful analysis of various legal definitions, see generally Susan Tiefenbrun, *A Semiotic Approach to a Legal Definition of Terrorism,* 9 ILSA J. OF INT'L & COMP. L. 357 (2003).

185. HOFFMAN, *supra* note 155, at 43.

186. ENDERS & SANDLER, *supra* note 9, at 3.

187. *Id*.

188. Tiefenbrun, *supra* note 184, at 362.

189. *See* Fletcher, *supra* note 181, at 901–02 (arguing that violence must have as its purpose to intimidate or coerce civilians in order to be considered terrorism).

190. Anthony Richards, *Conceptualizing Terrorism*, 37 STUD. CONFLICT & TERRORISM 213, 223 (2014).

191. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 81 (describing the FTO designation process and the role of the Secretary of State).

interference causes civilians to doubt the legitimacy of their government and its ability to manage important aspects of governance. It can force the government to spend time, political capital, and money to investigate how the attack happened and how to prevent such an attack from happening again. Note that all of these things are true about conventional terrorist attacks. Whether it is terrorists who wish to blow up an airplane or individuals who attack civilians, the government response is similar.

CONCLUSION

Determining that what I have called new terrorism—such as Russian interference in U.S. elections and attacks on critical infrastructure in Europe—constitutes terrorism under the FTO statute would represent a moderate middle ground between two poles. On one end are those who argue that this activity is different in kind from the kinds of activity that designated organizations typically engage in. Following from this is the conclusion that the appropriate response is a criminal law response that attempts to identify specific wrongful acts and target discrete actors. On the other pole are those who argue that such activity amounts to an act of war, suggesting a much broader—and potentially more lethal—set of responses.

The approach I suggest represents a pragmatic middle ground. By designating the organizations that engage in such activity, the Secretary of State would be giving prosecutors an enhanced set of tools to target the organization for what it has done and address what it is likely to do in the future if not stopped. Contrast this to the criminal law response, which is almost entirely reactive and backward-looking. To be sure, law enforcement is always aiming to prevent crimes. But designating an organization is designed to augment the ordinary prevention tools by making it possible for the government to target those who assist the organization in any way. Designation has the effect of depriving the organization of labor and money, its most important assets, before there is a direct link to a specific future terrorist act.

Treating election interference and social manipulation as a full-fledged attack, as many have suggested, is unnecessary and would likely be counterproductive. The harms associated with such activity, as serious as they are, are not sufficient to justify an armed response. And cyber responses, like hacking back or employing similar means, are inherently problematic. They almost always occur secretly and become known to the public only much later, if at all. This reduces the possible deterrent effect. Such responses also run the risk of harming civilians. It is almost impossible to mount a cyber response without targeting civilian or dual-use infrastructure or institutions. Not only would this violate bedrock principles of the law of armed conflict and U.S. policy, it is also likely to be counterproductive by apparently justifying the original wrongdoer's actions.