2016

Will Cyber-Terrorism Make § 2339B a Constitutional Suicide Vest?

Jay Lonick

Will Cyber-Terrorism Make § 2339B a Constitutional Suicide Vest?

by

Jay Lonick

Submitted in partial fulfillment of of requirements of the
King Scholar Program
Michigan State University College of Law
under the direction of Professor Glen Staszewski
Spring 2016

INTRODUCTION

"Fear of serious injury alone cannot justify oppression of free speech and assembly."[1]

A grave national security risk that the United States faces is the growing threat of cyber attacks.[2] Almost weekly, cyber attackers target private U.S. companies, the government, and the military.[3] These attacks range from direct attacks, such as installing malicious code capable of hijacking critical infrastructures—like nuclear power plants, bridges, or emergency response systems—to passive collection of confidential communications.[4] Some believe these cyber-attacks, many of which originate in Russia and China, could be viewed as traditional acts of warfare.[5] But one area that demands more serious attention in legal scholarship is the next potential chapter in the War on Terror:[6] cyber-terrorism. In fact, many cyber-security experts predict that by 2018 a cyber-terrorist organization will carry out a "cataclysmic" attack on the United States.[7] Responding to this threat will be difficult, however, if the government uses its most vital counter-terrorism tool, § 2339B of the Anti-Terrorism and Effective Death Penalty Act. The Act is powerful because it treats support for

---

[1] Louis D. Brandeis, Whitney v. California, 274 U.S. 357, 376 (1927).
[2] Benjamin Runkle, *Obama's Underwhelming Cyber Offensive Against the Islamic State*, FP (Mar. 25, 2016, 1:07 PM), http://foreignpolicy.com/2016/03/25/obamas-underwhelming-cyber-offensive-against-the-islamic-state/ (describing the Obama administration's hesitant approach to fighting ISIS has been "especially puzzling" in the realm of cyber operations); *FBI: Cyber Attacks Will Pose Biggest Threat in Next Decade*, TRIPWIRE (Nov. 15, 2013), http://www.tripwire.com/state-of-security/latest-security-news/fbi-cyber-attacks-will-pose-biggest-threats-next-decade/.
[3] Gary D. Solis, *Cyber Warfare*, 219 MILITARY L. REV. 1, 3-4 (2014) (describing the Internet as a "battlefield" often involving state-actors, like China and Russia, as major players).
[4] *Id.* at 10 (using examples offered by scholars and experts on the different types of attacks).
[5] *Id.* at 18 ("Cyber attacks may accordingly initiate either international or non-international armed conflicts.").
[6] Eric Schmitt & Thom Shanker, *U.S. Officials Retool Slogan for Terror War*, N.Y. TIMES (July 26, 2005), http://www.nytimes.com/2005/07/26/politics/us-officials-retool-slogan-for-terror-war.html.
[7] Tara Seals, *Cyber-Execs: Expect a Cataclysmic Cyber-Terror Event Within 2 Years*, INFO SECURITY (Apr. 12, 2016), http://www.infosecurity-magazine.com/news/cyberexecs-expect-a-cataclysmic/.

terrorists as an inchoate act of terrorism itself, but it is weak because it was not passed with the Internet in mind.[8]

Also known as the "material support" statute, the government has used § 2339B to—among many other things—successfully prevent individuals from providing money,[9] weapons,[10] car rides,[11] computer access,[12] translated pro-jihad materials,[13] and even shipments of paintballs for terrorist training camps.[14] Most importantly, § 2339B can also prohibit certain activities that appear to conflict with the First Amendment right of speech and association. Specifically, in *Humanitarian Law Project v. Holder*, the Supreme Court held that § 2339B could criminalize the provision of humanitarian aid, legal training, and even political advocacy to foreign terrorists.[15] The Court deferred to the judgment of Congress and the Executive, agreeing that § 2339B is "a vital weapon in this nation's continuing struggle against international terrorism,"[16] and that even certain speech and association could eventually be used to further terroristic goals. Given the preventative purpose of § 2339B, the question is whether it can be used to prevent support from flowing to potential cyber-terrorist organizations wishing to harm the United States.

The plain language of § 2339B's ban on "knowingly" providing material support to a "foreign" organization known to engage in "terrorist activity" or "terrorism" does not fit the realities of cyber-terrorism. First, a cyber-terrorist organization is arguably not "foreign."

---

[8] Andrew Peterson, Addressing Tomorrow's Terrorists, 2 J. Nat'l Security L. & Pol'y 297, 345 (2008) ("The FTO approach cannot deal effectively with dynamic networks accelerated by cyber-jihad.").
[9] United States v. Hammoud, 483 F. App'x 865, 865 n.1 (2012).
[10] United States v. al-Kassar, 660 F.3d 108 (2011) (involving a conspiracy to acquire and provide anti-aircraft missiles to a foreign terrorist organization).
[11] United States v. Chandia, 514 F.3d 365, 370 (2008).
[12] *Id.*
[13] United States v. Mehanna, 735 F.3d 32 (2013).
[14] *Chandia*, 514 F.3d at 370.
[15] *Id.*
[16] Oral Argument at 31:24-25, 32:1, Holder v. Humanitarian Law Project, 561 U.S. 1 (2010) (No. 08-1498).

Second, to prove that an individual knew an organization engages or engaged in "terrorism" or "terrorist activity," the government must rely on examples of traditional, violent acts that are distinguishable from how cyber-attacks occur.[17] Aside from the statutory language, applying § 2339B to Internet communications and online association would include speech and association purportedly protected by the First Amendment.[18] Though *Humanitarian Law Project* allows this in theory, the holding is far less forceful in distinguishing when protected online activity would become criminal. Moreover, unlike with joining Al-Qaeda, a person is less likely to know who exactly he or she is communicating with online and, therefore, may be more likely to inadvertently provide material support.

Congress must amend § 2339B by, first, clearly indicating that § 2339B should apply to cyber-terrorism and cyber-terrorist organizations. Second, Congress should require rulemaking by Department of Justice to clarify what a cyber-terrorist operation is and what acts would be criminal. To the latter point, the new rule should seek to clarify the different *mens rea* needed to "knowingly" provide material support to a cyber-terrorist organization. This would provide clear prosecutorial direction and also protect individuals from inadvertently violating § 2339B by giving aid to an anonymous Internet user who turns out to be a cyber-terrorist.

Rulemaking is necessary because an amendment alone would fail to address a phenomenon in the judiciary that occurred after in the post-9/11 era, where courts struggled to balance fundamental rights and national security.[19] Therefore, Congress should require notice-and-comment rulemaking by the Department of Justice (DOJ) because it would enable

[17] *See infra* Section III.B.
[18] *See infra* Section III.B-C.
[19] *See infra* Section II.C.

judicial review at the rule-making stage, which would avoid balancing First Amendment rights of individuals and national security in the courtroom. Without the pressures of an emergency, courts can "insist that the executive comply with the rules."[20] Ultimately, this Article seeks to rectify this judicial-deference phenomenon by using rulemaking and judicial review at the front end[21] to preemptively "mend" these holes.[22] The result is a sharpened tool for the Executive and a Judiciary re-aligned with its Article III duty to ensure § 2339B is applied constitutionally in cyber-space.

Part I summarizes the purpose of the Anti-Terrorism and Effective Death Penalty Act, the preventative vision behind the Act, and the elements of § 2339B. Part II explains the challenges that § 2339B raises under the First Amendment. Part II also addresses how the Supreme Court upheld the constitutionality of § 2339B as-applied to speech and association in *Holder v. Humanitarian Law Project.* Part III describes the new threat of cyber-terrorism, the contours of defining exactly what "cyber-terrorism" means, and the demands it could place on the Executive branch to continue preventing attacks on American citizens. Part IV applies the current law, § 2339B, to a CTO, highlights the limitations of the Act, and demonstrates why the proposals in Part V create a regime that more precisely addresses the new cyber-terror concerns and better aligns the branches of government around their constitutional duties than § 2339B does, as currently written.[23]

---

[20] Eric A. Posner, *Deference to the Executive in the United States after 9/11: Congress, the Courts, and the Office of Legal Counsel*, http://ssrn.com/abstract=1932393.

[21] By front end, I mean before charges are brought against defendants. In these situations, the court is forced to make a value judgment when the realities of terrorism are already tangible, and the fears of releasing the accused are greater.

[22] *See generally* Evan J. Criddle, *Mending Holes in the Rule of (Administrative) Law*, 104 NW. UNIV. L. REV. COLLOQUY 309 (2010).

[23] *See* Norman C. Bay, *Executive Power and the War on Terror*, 83 DENV. U. L. REV. 335 (describing the greater use of military power to address terrorism in place of the criminal justice system and the coinciding rise of the "centralization of foreign and domestic intelligence").

I. The Anti-Terrorism and Effective Death Penalty Act

Most people can easily put into words what terrorism means. Horrifying scenes from Boston,[24] Paris,[25] San Bernadino,[26] Brussels,[27] and thousands of others[28] are implanted into the lives of citizens around the United States and the world. These attacks demonstrate how no two attacks are the same, and the evolution of terrorism requires law enforcement to approach national security aggressively and proactively. In the United States, counterterrorism law is comprised of an array of broad statutes that either punish offenders after-the-fact, or prevent efforts to legitimize and support terrorism before a terrorist attack ever occurs.[29]

In the United States Code, "the federal crime of terrorism" is any offense that "is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct" and involves one or more of the forty-one predicate offenses listed.[30] Many of these offenses punish terrorist acts that have already been attempted or completed.[31] However, two statutes aim to prevent terrorist acts before they occur, by criminalizing the provision of "material support" before it might be used to recruit new terrorists or carry out new attacks.

---

[24] Michael Cooper, Michael S. Schmidt, & Eric Schmitt, *Boston Suspects are Seen as Self-Taught and Fueled by Web*, N.Y. TIMES (Apr. 23, 2013), http://www.nytimes.com/2013/04/24/us/boston-marathon-bombing-developments.html?pagewanted=all&_r=1&.

[25] Mariano Castillo, *Paris Suicide Bomber Identified; ISIS Claims Responsibility for 129 Dead*, CNN (Nov. 16, 2015, 12:30 PM), http://www.cnn.com/2015/11/14/world/paris-attacks/.

[26] Michael S. Schmidt & Richard Perez-Pena, *F.B.I. Treating San Bernadino Attack as Terror Case*, N.Y. TIMES (Dec. 4, 2015), http://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

[27] *Factbox: Suspects Linked to the Paris, Brussels Attacks*, REUTERS (Mar. 16, 2016, 5:42 PM), http://www.reuters.com/article/us-belgium-blast-people-factbox-idUSKCN0WS0LX.

[28] Since September 11, 2001, there have been 28,052 attacks from Islamic terrorist groups worldwide. *See What Makes Islam so Different?*, THE RELIGION OF PEACE, http://www.thereligionofpeace.com/attacks/attacks.aspx?Yr=2015 (last visited Mar. 30, 2016).

[29] CHARLES DOYLE, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C. 2339A AND 2339B 12, CONG. RES. SVS. (July 19, 2010).

[30] 18 U.S.C. § 2332(g)(5).

[31] *Id.*

The Department of Justice, through the U.S. Attorney Office (USAO), has plenary authority over federal criminal prosecutions, including "material support" cases.[32] Since the mid-1990s, and especially since 9/11, the USAO has largely succeeded in preventing major terrorist attacks in the U.S. by aggressively coordinating a strong national enforcement strategy.[33] Much of this success can be attributed to the United States' primary tool for preventing terrorism, the Anti-Terrorism and Effective Death Penalty Act (AEDPA).[34] Most vital to counter-terrorism are the "material support" statutes, specifically § 2339B, a far-reaching statute that carries a fifteen year prison sentence for those who attempt, conspire, or actually provide support to foreign terrorists.[35]

A. The Anti-Terrorism and Effective Death Penalty Act (AEDPA)

Two months after the first World Trade Center attack in 1993, then-Senator Joe Biden said in a Senate Hearing that "terrorism is no longer an abstract concept" as he urged for new laws to prevent terroristic acts before they occurred.[36] Three years later, the U.S. suffered another devastating attack in the Oklahoma City bombing, and Congress passed the AEDPA.[37] At first, there was only one material support statute, § 2339A, which states: Whoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, *knowing or intending that they are to be used* in preparation for, or in carrying out" one or more of forty predicate offenses."[38] It

---

[32] U.S. ATTORNEY'S MANUAL, TIT. 9: CRIMINAL, OFF. U.S. ATT'YS, U.S. DEP'T JUST., https://www.justice.gov/usam/usam-9-2000-authority-us-attorney-criminal-division-mattersprior-approvals, (last visited Apr. 3, 2016).
[33] *Id.*
[34] Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110. Stat. 1214 (1996).
[35] *See* 18 U.S.C. § 2339B.
[36] *Terrorism and America: A Comprehensive Review of the Threat, Policy, and Law Before the S. Comm. on the Judiciary*, 103d Cong. 1 (1993) (statement of Del. Joseph R. Biden, Jr., Chairman of the Committee).
[37] Pub. L. No. 104-132, 110. Stat. 1214 (1996).
[38] 18 U.S.C. § 2339A(a) (emphasis added).

applies to individuals who provide or attempt to provide material support to both foreign and domestic terrorists, and it requires proof of specific intent that one's support will be used for a specific terrorist act.[39] Further, "material support" is defined to broadly encompass anything that might be of value to a terrorist organization. It includes:

> [A]ny property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials;[40]

Congress later added § 2339B—a much more flexible provision—which does not require a showing that an individual intended to further a specific act of terrorism.[41] It states:

> 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 . . . that the organization has engaged or engages in terrorist activity . . . or that the organization has engaged or engages in terrorism . . . .[42]

In large part, Congress added § 2339B after finding that terrorist organizations could seek support "under the cloak of humanitarian or charitable exercise;" therefore, individuals could easily escape liability under § 2339A.[43] According to the House committee report, § 2339B addressed "the fungibility of financial resources and other types of material support."[44] In other words, Congress sought a strict ban on all funds, supplies, or other services because any

---

[39] *Id.*
[40] 18 U.S.C. § 2339A(b)(1). "Training" is further defined as "instruction or teaching designed to impart a specific skill, as opposed to general knowledge. *Id.* § 2339A(b)(2). Additionally, "[e]xpert assistance" means "advice or assistance derived from scientific, technical, or other specialized knowledge." *Id.* § 2339A(b)(3).
[41] DOYLE, supra 29, at 17.
[42] 18 U.S.C § 2339B(a)(1).
[43] H.R. Rep. No. 104-383, at 43 (1995) ("Many of these organizations operate under the cloak of a humanitarian or charitable exercise, or are wrapped in the blanket of religion. They use the mantle of religion to protect themselves from scrutiny, and thus operate largely without fear of recrimination.").
[44] *Id.* at 81.

support would "defray the costs" of running the organization, and "[t]his in turn frees an equal sum that can then be spent on terrorist activities."[45]

Section 2339B borrows the definitions of "material support" from § 2339A, but applies only where there is a "foreign terrorist organization."[46] Mainly, Congress recognized it could easily regulate foreign affairs based on having previously regulated citizens' interactions with Cuba without violating the First Amendment in *Regan v. Wald* and *Zemel v. Rusk*.[47] The legislative history of § 2339B shows a careful consideration of the danger of infringing on one's right to associate with individuals engaged in illegal activity,[48] content-based regulations of speech, and the fear of chilling independent advocacy.[49] However, members noted that the First Amendment is not absolute, and that in regulating for public safety, § 2339B was "absolutely necessary to achieve the government's compelling interest in protecting the nation's safety from the very real and growing terrorist threat."[50]

Nevertheless, groups challenged § 2339B on Fifth Amendment vagueness and First Amendment grounds.[51] In response, Congress clarified several definitions of "material support" in the USA PATRIOT Act and the Intelligence Reform and Terrorism Protection Act (IRTPA).[52] In these amendments, Congress clarified the terms "training" and "expert

---

[45] *Id.*
[46] *See* §§ 2339A, 2339B(a)(1).
[47] H.R. Rep. No. 104-383, at 43.
[48] *Id.*
[49] *Id.*
[50] *Id.* at 46
[51] *See* DOYLE, *supra* note 29, at 5. The primary case at issue was Humanitarian Law Project v. Reno, 9 F.Supp.2d 1176 (C.D. Cal. 1998). *Id.* As Congress amended § 2339B, the groups again sought new claims based on the new definitions in *Humanitarian Law Project v. Ashcroft*, 209 F.Supp.2d 1185 (C.D. Cal. 2004). *Id.* In both cases, the court held that "personnel," "training," and "expert advice and assistance" could include pure speech and advocacy protected by the First Amendment. *Id.*
[52] *Id.* After these amendments, the Ninth Circuit vacated its decisions in the past cases and remanded to the district court for further analysis after the amendments. *See* Humanitarian Law Project v. United States Dept. of Justice, 393 F.3d 902 (9th Cir. 2004).

advice or assistance"[53] and added a more specific definition of the word "personnel" provided in § 2339B(h):

> No person may be prosecuted under this section in connection with the term 'personnel' unless that person has knowingly provided, attempted to provide, or conspired to provide a terrorist organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct the operation of that organization.[54]

The litigation continued to the Supreme Court[55] and became part of a consolidated opinion, *Holder v. Humanitarian Law Project*, which is discussed in Part II.[56] The most important takeaway from the early challenges is they targeted the definitions that naturally include speech-related aspects, like "training," "expert assistance," "service," and "personnel." The reason is because, they argued, it was unclear when protected speech or association crosses the line into criminal activity;[57] in cyberspace, that line is much less clear.

B. Elements: Providing Material Support to a Foreign Terrorist Organization under § 2339B

Under § 2339B it is unlawful to: (1) Attempt to provide, conspire to provide, or actually provide (2) material support or resources (3) to a foreign terrorist organization (4) knowing that the organization is an FTO.[58] Without the specific-intent requirement to further an act of terrorism from § 2339A, Congress needed to prevent criminalizing inadvertent material

---

[53] *See* P.L. 107-56, § 805(a)(2), 115 Stat. 377 (2001).
[54] 18 U.S.C. 2339B(h) (emphasis added).
[55] On remand, the district court held that the definitions of "personnel" were constitutional, but that "expert advice and assistance" and "training" still raised problems. Humanitarian Law Project v. Mukasey, 552 F.2d 916 (9th Cir. 2009), *cert. granted sub nom.*, Humanitarian Law Project v. Holder, 130 S.Ct. 48 (2009)
[56] *See infra* Section II.B.
[57] *See* DOYLE, *supra* note 29 (explaining that one district court found these terms "could be construed to include unequivocally pure speech and advocacy protected by the First Amendment").
[58] 18 U.S.C. § 2339B.

support under § 2339B.[59] For example, Congress did intend for a person to be charged for giving a cab ride if that person did not know the rider was a member of a foreign terrorist organization.[60] Therefore, the law has three methods by which the government can prove someone "knowingly" provided material support to an FTO.

1. *Knowledge of Designation as an FTO by the U.S. Secretary of State*

The first method requires proof that a person knew the group had been designated as a "foreign terrorist organization" by the Secretary of State.[61] The Secretary of State has authority to designate an entity as "foreign terrorist organization" under the Immigration and Nationality Act.[62] The Secretary must find that the organization is "foreign," and that it engages in "terrorist activity" or "terrorism."[63] Further, the Secretary must find that the entity's activity "threatens the security of United States nationals" or national security generally.[64] Once designated, the FTO can seek an appeal in the U.S. Court of Appeals for the District of Columbia, but a defendant charged with providing material support cannot challenge the FTO's designation.[65]

The best example of this method comes from *Humanitarian Law Project v. Holder*, where the plaintiffs had been assisting two foreign groups subsequently designated as FTOs.[66] When the plaintiffs discovered this news, they feared that their continued efforts

---

[59] *See* Michael G. Freedman, Note, *Prosecuting Terrorism: The Material Support Statute and Muslim Charities*, 38 HASTINGS CONST. L.Q. 1113 (2011) (proposing that § 2339B's ban interferes with the Muslim belief in "zakat," a form of charitable giving, and should be amended to require specific intent to avoid accidental material support).
[60] *Cf.* United States v. Chandia, 514 F.3d 365, 370 (2008) (punishing a defendant for knowingly providing car rides to a person that he knew was a terrorist).
[61] § 2339B(a)(1).
[62] *Id.*
[63] § 1189(a)(1)(B).
[64] *Id.*
[65] *See id.* at § 1189(a); DOYLE, *supra* note 29, at 9.
[66] 561 U.S. 1 (2010).

would be considered "material support" under § 2339B.[67] In response, they brought a pre-enforcement challenge in district court, arguing that as-applied § 2339B would violate their First Amendment rights to speak and associate in the form of giving humanitarian aid, legal training, and political advocacy.[68]

2. *Knowledge of "terrorist activity"*

Second, knowledge may be proven if an individual knew that the entity "has engaged or engages in terrorist activity."[69] Of the two methods that do not rely on knowledge of an FTO's designation, Charles Doyle calls this route the more "multi-faceted" of the two.[70] Here, "terrorist activity" is defined by the Immigration and Nationality Act as any act that is illegal in the United States and includes any of the following: (1) hijacking; (2) holding an individual for ransom; (3) a violent attack on an "internationally protected person;" (4) assassinations; (5) the use of any "biological agent, chemical agent, or nuclear weapon or device" or "explosive, firearm, or other weapon or dangerous device . . . with the intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property; or (6) "[a] threat, attempt, or conspiracy to do any of the foregoing."[71]

3. *Knowledge of "terrorism"*

The third method requires proof that an individual knew an organization engaged or engages in "terrorism" as defined in the Foreign Relations Authorization Act.[72] This

[67] Id. at 10.
[68] *Id.*; *see also infra* Section II.B.
[69] *See* 8 U.S.C.A § 1182(B)(iii) (2013).
[70] *See* DOYLE, *supra* note 29, at 9.
[71] *See id.* § 1182(B)(iii).
[72] *See* § 2339B; 22 U.S.C. § 2656(f) (2004).

definition is the least specific, defining "terrorism" as "premeditated, politically motivated violence."[73] Like with "terrorist activity," violence is central to the definition.

In sum, the first method can be distinguished from the latter two; it applies when the Secretary of State has designated a "foreign terrorist organization[s]," and it only triggers when the accused also knew of that designation.[74] If an individual did not know a group was a designated FTO, the government must prove that the individual knew the entity engaged in "terrorist activity" or "terrorism."[75] But designating an FTO requires the Secretary of State to find that the entity has engaged in "terrorist activity" or "terrorism"[76]—so ultimately, knowledge centers on the latter two definitions. Oftentimes, convictions involve support for radical jihadist groups known to engage in violent attacks on civilians.[77] Therefore, meeting the knowledge requirement is typically a non-issue for the government, and defendants instead focus on arguing that § 2339B is unconstitutional as-applied. With cyber-terrorism, however, the problem is twofold: Not only are the same constitutional questions applicable, but "terrorist activity" and "terrorism" appear to plainly exclude support for non-violent terrorist groups.

C. The Difficult Migration from Traditional to Online "Material Support"

An archetypal example of § 2339B's application is *United States v. Chandia*, where the defendant was convicted after he attended an overseas militant training camp, provided rides and computer access to militant officials, and assisted in shipping paintballs for future

[73] 22 U.S.C. § 2656(f) (2004).
[74] § 2339B(a)(1).
[75] *Id.*
[76] *See* § 1189.
[77] *See, e.g.*, United States v. Warsame, 537 F.Supp.2d 1005, 1018 (D. Minn. 2008) (defendant assisted with al Qaeda training camp by providing "personnel"); United States v. Shah, 474 F.Supp.2d 492, 497 n.5 (S.D.N.Y. 2007) (providing assistance as a doctor treating wounded al Qaeda jihadists).

training camps in Pakistan.[78] There, the provision of tangible materials and services illustrate common-sense applications of "service," "personnel," "property," and "transportation." Another clear case is *United States v. Farhane*, where the defendant, a surgeon trained at Columbia University, agreed to be a battlefield surgeon for wounded jihadists and swore his allegiance to al Qaeda in a ritual swearing-in called a "bayat."[79] Accordingly, he was convicted for attempting to provide "expert training," "personnel," and "training."[80]

But prosecutions under § 2339B are not always clear. They may not pinpoint exactly which definition of "material support" applies to the purportedly illegal act. For example, in *United States v. Mehanna*, the defendant traveled to Yemen, hoping to find an al-Qaeda training camp.[81] After searching unsuccessfully, he returned to his home in Boston, translated a publication called "39 Ways to Serve and Participate in Jihad" into English, and published it on a website dedicated to al-Qaeda sympathizers.[82] For these actions, Mehanna was indicted for conspiring to provide "property, services, currency and monetary instruments, training, expert advice and assistance, facilities and personnel, to a foreign terrorist organization, namely al Qaeda."[83] Despite his failure to find the camp, Mehanna's attempt to join al Qaeda, along with proof of his intent to wage jihad, satisfied an attempt to provide "personnel."[84] While this act clearly fits the definition, the application of § 2339B to Mehanna's online translation is unclear.

---

[78] United States v. Chandia, 675 F.3d 329, 332 (4th Cir. 2012).
[79] 634 F.3d 127, 133 (2d. Cir. 2011).
[80] *Id.* at 134.
[81] United States v. Mehanna, 735 F.3d 32, 41-42 (1st Cir. 2013).
[82] United States v. Mehanna, 669 F.Supp.2d 160, 163 (D. Mass. 2009). Among other statements, the defendant expressed that he wished to be the "media wing" for al Qaeda. *Id.*
[83] Second Superseding Indictment, United States v. Mehanna, No. 09-CR-10017-GAO (D. Mass. June 17, 2010).
[84] *Mehanna*, 735 F.3d at 41-42.

This definition difficulty in *Mehanna* was not fatal to the case, but it begins to show why some believe § 2339B may be "inadequate for prosecuting these types of Internet activities."[85] In fact, in *United States v. Al-Hussayen* the government charged a University of Idaho student whose alleged "material support" took place completely online, and the government could not obtain a conviction.[86] Sami Al-Hussayen, a student at the University of Idaho, was accused of providing material support violations because he maintained websites for several Islamic charities,[87] moderated email groups to facilitate fundraising and recruiting for violent jihad, and published numerous speeches, articles, and lectures promoting jihad online.[88] However, the "evidence of Internet activity was not the 'hard evidence' the jurors expected,"[89] and Al-Hussayen was acquitted.[90] Moreover, there has only been one successful conviction for operating terrorist websites, but that case also involved an attempt to create a jihadist training camp in in the United States, giving it a "non-cyber hook" that grounded it in more "traditional" terrorism.[91]

Professor Alan Williams proposes a new material support statute in response to terrorists using the Internet.[92] He argues that the material support statutes were written broadly to cut off funding and services, but were "not fashioned with the Internet in mind."[93] Specifically, "the advent of the unique capabilities of the Internet" presents challenges for

---

[85] Alan F. Williams, *Prosecuting Website Development Under the Material Support to Terrorism Statutes: Time to Fix What's Broken*, 11 N.Y.U. J. LEGIS. & PUB POL'Y 365, 383 (2007-2008).
[86] United States v. Al-Hussayen, 2004 U.S. Dist. LEXIS 29793 (D. Idaho Apr. 6, 2004).
[87] Williams, *supra* note 85, at 367-371 (2007-2008) (referencing the investigation, warrant, and indictment).
[88] *Id.*
[89] *Id.* at 369.
[90] Bob Fick, *Saudi is Acquitted in Boise*, ASSOCIATED PRESS (June 11, 2004) http://www.deseretnews.com/article/595069604/Saudi-is-acquitted-in-Boise.html?pg=all ("'There was a lack of hard evidence,' said juror John Steger.").
[91] *See* United States v. Kassir, No. 04 Cr. 356 (JFK), 2009 U.S. Dist. LEXIS 83075, ay *1 (S.D.N.Y. Sept. 11, 2009).
[92] Williams, *supra* note 85, at 397.
[93] *Id.* at 380.

understanding the contours of terrorist organizations that now operate through a "loosely structured network of cells . . . without having to congregate in a physical location."[94] Consequently, despite the fall of Al-Qaeda in Afghanistan, the group used the Internet to spread information about how to make explosives, incite terrorism, recruit new members, and raise money.[95] Williams's proposal would be titled "Use of Internet Websites with Specific Intent to Facilitate Terrorism," which borrows the broad applicability of § 2339B, by not requiring intent to further specific terrorist acts, but replaces the "knowing" requirement with specific intent to "recruit persons" or "encourage violent attacks" through online postings.[96]

In sum, when the government prosecutes an individual for providing material support, case law shows that it is difficult when the support is non-traditional—especially when it entwines with speech online. The more "cyber" the interactions—and the alleged support—are, the less clear it may be to a jury that the person "knowingly" sought to provide material support to a terrorist.[97] Some cases have successfully prosecuted material support that took place online, but they also involved a combination of traditional and cyber support. For example, in *Mehanna*—the defendant translated pro-jihad materials online, but also attempted to provide "personnel" when he tried to participate in militant camps.[98] The reason that this distinction matters first requires an understanding of the protections one has—even in speaking or associating with terrorists—under the First Amendment.

II. THE FIRST AMENDMENT & *HOLDER V. HUMANITARIAN LAW PROJECT*

[94] *Id.*
[95] *Id.* at 397.
[96] *Id.* at 383-84.
[97] *See supra* note 89 and accompanying text.
[98] *See supra* notes 81-84 and accompanying text.

The protections guaranteed by the First Amendment and the Internet's value to terrorist organizations are in conflict. As terrorists have begun advocating and recruiting online, Newt Gingrich, for example, argued that the First Amendment should not be a "suicide pact."[99] Then in 2010, the Supreme Court decided *Humanitarian Law Project*. The Court held that § 2339B was narrowly tailored toward preventing terrorist acts, but limited its opinion solely to the facts of the case.[100] Nevertheless, scholars criticized this decision, and several others in the post-9/11 era, arguing that the judiciary has been overly deferential toward the government in counter-terrorism cases involving questions about constitutional rights.[101] In sum, Congress should amend § 2339B to clearly authorize charges to prevent cyber-terrorism, but also incorporate ways to protect the First Amendment, because otherwise lightened judicial review will continue.

A. Online Identity, Association, and First Amendment Rights

In First Amendment jurisprudence, "speech, assembly, association, and petition, 'though not identical, are inseparable.'"[102] The Court, in *Brandenburg v. Ohio*, held that states may not ban speech unless it "is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[103] This type of speaker's-intent requirement is premised on the need for "breathing space" to avoid chilling protected

[99] Newt Gingrich, *The 1st Amendment is not a Suicide Pact: Blocking the Speech that Calls for our Death*, HUMAN EVENTS (Dec. 4, 2006, 2:30 PM), http://humanevents.com/2006/12/04/the-1st-amendment-is-not-a-suicide-pact-blocking-the-speech-that-calls-for-our-death/.
[100] *Humanitarian Law Project*, 561 U.S. at 39.
[101] *See infra* Section II.C.
[102] NAACP v. Claiborne Hardware Co., 458 U.S. 886, 911(1982) (quoting Thomas v. Collins, 323 U.S. 516, 530 (1945)); *see also* Citizens United v. FEC, 130 S. Ct. 876, 904 (2010).
[103] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

speech.[104] Additionally, the Supreme Court's holding in *Scales v. United States* is important for the right to associate: "[A] blanket prohibition on association with a group having both legal and illegal aims" would be a "real danger" to legitimate expression and association guaranteed by the First Amendment.[105] Further, in *NAACP v. Claiborne Hardware Co.*, the Court held that intent to further illegal aims—which can be banned—must be "judged 'according to the strictest law.'"[106] Otherwise, individuals who sympathize with a group's lawful goals may be punished for "purposes which he does not necessarily share."[107]

The Supreme Court has also adhered to a principle that "whatever the challenges of applying the Constitution to ever-advancing technology," the basic guarantees of the First Amendment do not vary.[108] In the past two decades, courts have expanded First Amendment protection to video games,[109] computer code,[110] search-engine results,[111] and impliedly to broadcasted videos of criminal acts—like animal "crush" videos.[112] In contrast, the courts have excepted protection for hate speech, true threats, child pornography, and spam.[113] Important for the material-support debate, and particularly cyber-terrorism, is that the First

---

[104] *See generally* Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 WM. & MARY L. REV. 1633 (2013) (arguing that the "chilling effect" caused by regulating speech is an inadequate justification because in part these effects cannot be measured).
[105] Scales v. United States, 367 U.S. 203, 229-30 (1961); *see also* NAACP v. Claiborne Hardware Co., 458 U.S. 886, 918-19 (1982).
[106] 367 U.S. 886, 919 (1982) (quoting United States v. Noto, 367 U.S. 290, 299-300 (1961)).
[107] *Id.*
[108] *See* Brown v. Ent. Merchants Ass'n, 564 U.S. 786 (2010).
[109] *Id.*
[110] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445-46 (2001).
[111] Jian Zhiang v. Baidu.com Inc., 10 F.Supp.3d 433 (S.D.N.Y. Mar. 28, 2014)
[112] United States v. Stevens, 559 U.S. 460 (2010). Here the Court reserved its holding by reasoning that the statute targeted "animal cruelty" broadly, which could include hunting, and that a statute aimed only at "crush videos or other depictions of extreme animal cruelty" may be constitutional. *Id.* at 482.
[113] Catherine Pelker, Anthony J. Palmer, Brittany Raia & Jamin Agosti, *Computer Crimes*, 52 AM. CRIM. L. REV. 793, 803 (2015) (discussing the cases that reached these holdings); *see also See e.g.*, Alexander Tsesis, *The Categorical Free Speech Doctrine and Contextualization*, 65 EMORY L.J. 495 (2015) (discussing the Supreme Court's hesitation in using "ad hoc balancing" to find certain categories of speech outside of First Amendment protection) (quoting *Stevens*, 559 U.S. at 461).

Amendment protects anonymous speech.[114] Moreover, it is well-settled that individuals do not become criminals for merely speaking to or associating with terrorists.[115] Both anonymity and free association would create new constitutional obstacles if § 2339B were applied to potential online material support.

Where defendants have raised First Amendment challenges to § 2339B, courts often justify the statute's constitutionality as a ban on conduct—not speech.[116] Framed this way, § 2339B is not content-based because it does not aim to suppress the content of a communication; instead, it bans the conduct of offering valuable information or resources of any kind.[117] Defendants often raise doubts about the quantum of activity that is permitted without offering "material support."[118] Courts have been able to distinguish the conduct of providing support from the incidental speech that it may entail, but that line will be difficult to draw online, and several scholars have argued for changes to § 2339B.[119]

Current scholarship addressing the nexus between online activity, terrorism, and § 2339B is varied. Some argue that § 2339B chills speech and association,[120] and the low percentage of convictions proves the law's ineffectiveness.[121] To date, there has only been

---

[114] *See* Reno v. ACLU, 521 U.S. 844, 870(1997)

[115] *See* Humanitarian Law Project v. Holder, 561 U.S. 1, 39 (2010) (agreeing with the Ninth Circuit's framing that § 2339B "does not prohibit being a member of one of the designated groups"); *Scales*, 367 U.S. at 229-30.

[116] *See, e.g.*, United States v. Chandia, 514 F.3d 365, 371 (4th Cir. 2008); United States v. Assi, 414 F.Supp.2d 707, 713 (E.D. Mich. 2006) ("What AEDPA prohibits is the act of giving material support, and there is no constitutional right to facilitate terrorism by giving terrorists the weapons and explosives with which to carry out their grisly missions."); United States v. Sattar, 227 F.Supp.2d 348, 368 ("The statute does not interfere with Stewart's First Amendment rights because the material support restriction 'is not aimed at interfering with the expressive component of [Stewart's] conduct but at stopping aid to terrorist groups.'") (quoting Humanitarian Law Project v. Reno, 205 F.3d 1130, 1135 (9th Cir. 2000).

[117] *Id.*

[118] Andrew Peterson, *Addressing Tomorrow's Terrorists*, 2 J. NAT'L SECURITY L. POL'Y 297, 304 (2008).

[119] *See Humanitarian Law Project*, 561 U.S. at 4.

[120] *See, e.g.*, Brent Tunis, Note, *Material-Support-to-Terrorism Prosecutions: Fighting Terrorism by Eroding Judicial Review*, 49 AM. CRIM. L. REV. 269, 290 ("[I]f an individual can be a member of an FTO, but is prohibited from speaking or doing anything that can be construed as 'coordinated activity' with the organization, then what real value does his membership retain.").

[121] Elizabeth M. Renieris, *Combating Incitement to Terrorism on the Internet: Comparative Approaches in the*

one conviction under § 2339B for developing and maintaining terrorist Web sites, but that case also involved an attempt to set up a terrorist training camp in the United States.[122] Others argue that the law should be improved because the Internet can be used to "insulate[] the speaker from his or her audience, thus complicating the establishment of the criminal *mens rea* requirement, but in no way reducing the threat."[123] Yet none of these solutions address non-violent terrorist groups; they instead focus on applying § 2339B to the speech-related support offered to violent groups via the Internet. Emma Sutherland's argument relates tangentially to the one that I propose, as she argues that § 2339B cannot survive scrutiny as-applied to support for "quasi-domestic" organizations, which have domestic and foreign ties.[124]

Therefore, the First Amendment rights guaranteed to American citizens can be difficult to separate from the material support banned by § 2339. Even as the law was in development, several groups sued preemptively to ensure that they would not face criminal prosecutions.[125] Then in 2010, those cases became part of of a consolidated opinion in *Holder v. Humanitarian Law Project*, which addressed the speech-related aspects of material support directly, by deciding whether the statute was an unconstitutional ban on protected speech and association.[126] This case shows the current state of the law and why cyber-terrorism, under the law and in practice, is different. Cyber organizations are not "foreign," and "expert

---

United States and United Kingdom and the Need for International Solutions, 11 VAND. J. ENT. & TECH. L. 673, 690 (2009) (stating that of the almost 400 terrorist suspects since September 11th, only thirty-nine were convicted of terrorism or national security crimes)

[122] *See* Megan Anne Healy, *How the Legal Regimes of the European Union and the United States Approach Islamic Terrorist Websites: A Comparative Analysis*, 84 TUL. L. REV. 165 (2009)

[123] Daniel Hoffman, *Online Terrorism Advocacy: How AEDPA and Inchoate Crime Statutes can Simultaneously Protect America's Safety and Free Speech*, 2 NAT'L SEC. L.J. 200, 216 (2014).

[124] Emma Sutherland, *The Material Support Statute: Strangling Free Speech Domestically*, 23 GEO. MASON U. CIV. RTS. L.J. 229, 229 (2013).

[125] *See supra* notes 51-55 and accompanying text.

[126] 561 U.S. 1 (2010).

assistance," "training," and "personnel" are naturally entwined with speech online, making the conduct–speech distinction difficult to distinguish. Ultimately, the precedential value of *Humanitarian Law Project* will be limited for future challenges to § 2339B in cyber-terrorism cases.

B. Holder v. Humanitarian Law Project

In 1997, several humanitarian aid groups had been working with the Kurdistan Workers' Party (PKK) in Turkey and the Liberation Tigers of Tamil Eelam (LTTE) in Sri Lanka.[127] Both groups were actively pursuing statehood for Kurds in Turkey and Tamils in Sri Lanka,[128] but had also committed violent terrorist attacks—some of which targeted U.S. citizens.[129] Fearing a criminal prosecution, the plaintiffs challenged the constitutionality of § 2339B in a pre-enforcement action.[130] The plaintiffs argued, among other claims, that they had a First Amendment right to provide support for peaceable means, but that the statute would criminalize such actions as material support in the form of "training, "expert advice or assistance," "service," and "personnel."[131]

The First Amendment question in *Humanitarian Law Project* was whether the assistance that the humanitarian groups offered was protected speech or association, and if it was, whether § 2339B could prohibit it.[132] The plaintiffs urged the Court to apply strict scrutiny because, they argued, § 2339b would apply based on the value and content of their message.[133] The government urged the Court to apply the *O'Brien* test, because § 2339B was

---

[127] *Id.*
[128] *Id.*
[129] *Id.* at 10.
[130] In such a challenge, the Court is confined to only the facts in the present case. *See* Scales v. United States, 367 U.S. 203, 223 (1961). "[T]heoretical doubts" about a statute's application are irrelevant. *Id.*
[131] *Humanitarian Law Project*, 561 U.S. at 14.
[132] *Id.* at 28.
[133] *Id.*

"unrelated" to the message that the plaintiffs sought to convey in their training and created no greater a burden than necessary to further the important governmental interest in combatting terrorism.[134] The Court disagreed with both framings; the statute would have neither prohibited "pure political speech"—leaving the plaintiffs free to advocate independently about the LTTE and PKK[135]—nor would it have applied to mere conduct, as the speech-related aspects of training and advocacy were inseparable from the application of § 2339B.[136]

The majority never used the phrase "strict scrutiny" in the opinion, but still began much like it would have under such analysis, stating that "combating terrorism is an urgent objective of the highest order."[137] In upholding the constitutionality of the Act, the Court rejected the plaintiffs' view that banning humanitarian, peaceful support did nothing to further the objective of combating terrorism,[138] deferring instead to the "considered judgment of Congress and the Executive that providing material support to a designated foreign terrorist group—even seemingly benign support—bolsters terrorist activities of that organization."[139]

The majority credited Congress with considering the Constitution when it amended the Act in response to previous litigants. Congress carved out a safe harbor for independent advocacy and also clarified that "personnel" must be "coordinated with or under the direction or control" of a terrorist.[140] As for the right to freely associate, even with terrorists, the Court held that § 2339B avoided constitutional problems because it does not prohibit promoting or

---

[134] *Id.*
[135] *Id.* at 25-26.
[136] *Id.* at 28 (explaining why *O'Brien* was inapplicable because § 2339B was related to communicative conduct in this case).
[137] *Id.*
[138] *Id.* at 28-29.
[139] *Id.* at 37.
[140] *Id.*

supporting a terrorist organization's goals, but rather, the conduct of providing material support *to* that group.[141]

Presently, if the Executive Branch were to target online-only terrorist organizations, the holding in *Humanitarian Law Project* raises doubts as to § 2339B's continued application. To be sure, the Court afforded "significant weight" to conclusions by Congress and the Executive, such as that "designated foreign terrorist organizations 'are so tainted by their criminal conduct that any contribution to such an organization facilitates that conduct.'"[142] Yet the Court limited its holding to the precise facts of the case, and explicitly refused to "extend the same prohibition on material support at issue here to domestic organizations."[143] The dissent worried that there would be "no natural stopping place" in applying the Act, since all support is arguably fungible.[144] Despite the statute's plain language, and whether *Humanitarian Law Project* would theoretically present a challenge to using § 2339B for online material support, there is a much larger judicial phenomenon that colors the reason for more explicit statutory text; it began on September 11th, 2001 and continues today.

C. The "9/11 Effect" on the Courts: Judicial Passivity and Constitutional Erosion

In the decade between September 11th and *Humanitarian Law Project*, many scholars noticed a phenomenon of judicial passivity had emerged in the courts.[145] This, they argue, eroded constitutional rights in terrorism cases.[146] At risk now is the possibility that

---

[141] *Id.*
[142] *Id.* at 38.
[143] *Id.* at 39.
[144] *Id.* at 31.
[145] Trevor Sutton, *Foreword* to OWEN FISS, A WAR LIKE NO OTHER (Owen Fiss & Trevor Sutton eds., The New Press) (2015) (arguing that both the 2008 and 2012 presidential elections turned much more on domestic matters rather than disputes about national security).
[146] *Id.*

government will use § 2339B—despite its poor application—to dutifully protect national security again cyber-terrorism,[147] and further passivity might allow it to happen.[148]

1. *Executive "Stretching:" Defining the War on Terror*

In 1919 the Supreme Court decided *Schenck v. United States*,[149] and Justice Wendell Oliver Holmes wrote that "[w]hen a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight."[150] These words do not apply easily to the war on terror.[151] For one, Congress has not formally declared war since World War II, much less on terrorist organizations like al Qaeda and ISIS.[152] The Obama administration instead stretches congressional authorization from 2001—authorizing force against al Qaeda—as an implied authorization to target new "associated forces," like ISIL.[153] Presumably, the same executive "stretching" would occur in response to cyber-terrorism and using § 2339B to prevent it.[154]

---

[147] *See generally* Adrian Vermeule, *Our Schmittian Administrative Law*, 122 HARV. L. REV. 1095, 1096 (2009) (defining "black holes" as zones where agencies can act freely in response to emergencies without clearly binding rules and "grey holes" as the heightened deference offered to agencies by the judiciary in responding to such emergencies).

[148] *Id.*

[149] 249 U.S. 47, (1919) (describing the "clear and present danger" test).

[150] *Id.*

[151] Robert O'Neill, HATE PROPAGANDA AND NATIONAL SECURITY *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR 171, 171 (Carolina Academic Press 2010).

[152] *Official Declarations of War by Congress*, U.S. SENATE (last visited Apr. 24, 2016), http://www.senate.gov/pagelayout/history/h_multi_sections_and_teasers/WarDeclarationsbyCongress.htm.

[153] Siobhan Hughes, *War Powers: Avoiding a Congressional Use-of-Force Vote, for Now*, WALL ST. J. (Sept. 12, 2014, 2:43 PM), http://blogs.wsj.com/law/2014/09/12/war-powers-avoiding-a-congressional-use-of-force-vote-for-now/.

[154] O'Neill, *supra* note 151, at 171-72. This trend has been ongoing. For example, in 2007 the U.S. Commission on International Religious Freedom cautioned that the State Department should consider closing a Saudi-backed private school in Virginia unless the school proved it was not advancing religious intolerance toward the United States. *Id.* Also in 2007, the House of Representatives approved the Violent Radicalization and Homegrown Terrorism Prevention Act, which addressed concerns that sponsor of the bill, Rep. Jane Harman, made about how the Internet offers "access to broad and constant streams of terrorist-related propaganda," and "violent radicalization." *Id.* Some literature suggests that restricting hateful material through online is worthwhile. *See* Spencer W. Davis, Note, *Incitement to Terrorism in Media Coverage: Solutions to Al-Jazeera After the Rwandan Media Trial*, 38 GEO. WASH. L. REV. 749, 778 (2006); *See generally* Jane Bailey, *Private Regulation and Public Policy: Toward Effective Restriction of Internet Hate Propaganda*, 49 MCGILL L.J. 59 (2004).

2. *Judicial Deference: The "9/11 Effect" on Constitutional Rights*

Professor Adrian Vermeule suggests that "in times of national emergency, the intensity of judicial review of legal questions has been dialed down."[155] Vermeule's theory of legal "grey holes" appear in the touchstone cases from the 9/11 era, like *Hamdi v. Rumsfeld* and *Boumediene v. Bush*, where the difficulty of balancing aggressive counterterrorism law with individual rights often resulted in pro-national security results.[156] This phenomenon is a primary reason that counterterrorism law appears to have proven "unusually enduring" to constitutional challenges, since the courts appear to have acquiesced by trusting Congress and the Executive to keep American lives safe.[157]

First under President George W. Bush, and more recently under President Obama, the Executive branch imprisoned individuals without trial,[158] conducted warrantless wiretapping,[159] and conducted targeted killings of alleged terrorists. In each of the corresponding lawsuits, the judiciary was forced to strike a balance between fundamental rights and national security.[160] To Professor Owen Fiss, the resulting value judgments came at too great a cost to the Constitution.[161] Fiss argues that from 2001 to 2010, lower courts "handed the government victory after victory in suits alleging torture, warrantless, surveillance, and extrajudicial killings."[162] One of the most significant constitutional issues decided in the post-9/11 years was *Holder*, where the Court reflected: "[W]hen it comes to

---

[155] Vermeule, *supra* note 147, at 1131.
[156] *Id.*
[157] Sutton, *supra* note 145, at x.
[158] *See id.* at 148 ("Both Bush and Obama . . . have insisted on the authority to imprison for prolonged, indefinite periods of time anyone that they determine has fought for the Taliban or al-Qaeda.").
[159] President George W. Bush sponsored, and Congress passed, the Foreign Intelligence Surveillance Amendments Act in 2008. *Id.* at 225. The 2008 statute allowed judges to authorize wiretaps, and it has been "thoroughly endorsed" by President Obama. *Id.* at 226.
[160] *Id.*
[161] *Id.* at xii. (calling the decisions "phyrric").
[162] *Id.*

collecting evidence and drawing factual inferences . . . the lack of competence of the courts is marked."[163] This challenge flowed, in part, from the fact that "[n]either the Members of this Court nor most federal judges begin the day with briefings that describe new and serious threats to our Nation and its people."[164]

In sum, scholars challenged the "presumption of executive competence" in *HLP* as overly deferential,[165] but judicial deference was pervasive; it "lighten[ed]" the judicial scrutiny in courts around the country.[166] Before this trend continues further, Congress must ensure there are "properly tailored and constitutionally sound means"[167] for preventing cyber-terrorism that also aim to re-align the judiciary with its constitutional duty. As Professor Alan Williams stated, "More sophistication deserves more accurate language, and the material support statutes were not fashioned with the Internet in mind."[168]

III. CYBER TERRORISM: POLITICAL, LEGAL, AND PRACTICAL OBSTACLES

Since the Court decided *Humanitarian Law Project*, much more has changed in the landscape of terrorism, and one area where law enforcement has struggled is in responding to online threats.[169] There is a vast amount of scholarship addressing the legal implications of possible cyber attacks and cyber warfare, but far less when it comes to cyber-terrorism.[170] None have thoroughly addressed how, or if, § 2339B can be used to prevent it. Before reaching the precise question of § 2339B's response to cyber-terrorism, it is important to

---

[163] *Id.* at 33.
[164] Holder v. Humanitarian Law Project, 561 U.S. 1, 34 (2010) (quoting *Boumediene v. Bush*, 553 U.S. 723, 797 (2008)).
[165] *See* Aziz Z. Huq, *Structural Constitutionalism as Counterterrorism*, 100 CAL. L. REV. 887, 898 (2012).
[166] *Id.*
[167] Williams, *supra* note 85, at 383.
[168] *Id.* at 380.
[169] 2015 INTERNET SECURITY THREAT REPORT 5, (Apr. 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf (highlighting the rapid development of new threats and the challenges of keeping pace).
[170] *See* ANTONIA CHAYES, BORDERLESS WARS: CIVIL MILITARY DISORDER AND LEGAL UNCERTAINTY 160, Cambridge Univ. Press (2015).

understand the legal and practical challenges in regulating cyberspace, as well as the proposals regarding § 2339B in the Internet-era.

With over one billion Internet users around the world, "one area where society is particularly vulnerable is cyberspace."[171] In 2008, a Congressional Research Report explored the connections between cyber-criminals and terrorists and found that "[s]eized computers belonging to Al Qaeda indicate its members are becoming more familiar with hacker tools and services that are available over the Internet."[172] In 2009, President Barack Obama declared that attacks on computer networks are "one of the most serious economic and national security risks we face as a nation."[173] As the capabilities of current terrorist groups have grown, one former Director of National Security Agency (NSA) addressed the new issue of cyber-terrorism, saying that "[t]he warnings are over. It could happen tomorrow."[174]

Traditional terrorist groups have already been using the Internet to develop new ways to recruit, organize operations, and carry out attacks—yet these tactics are not distinct acts of cyber-terrorism.[175] With Al-Qaeda, and now the rise of ISIL, a group that was only recently designated as a "foreign terrorist organization,"[176] social media is especially powerful.[177] What is new to this landscape is that militants are now able to remain anonymous to law

---

[171] Jeffrey F. Addicott, *Cyberterrorism: Legal and Policy Issues*, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR 519 (Carolina Academic Press 2010).
[172] Clay Wilson, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 3, CONG. RES. SERV. (Jan. 29, 2008).
[173] *Id.*
[174] Max Fisher, *Fmr. Intelligence Director: New Cyberattack May Be Worse Than 9/11*, THE ATLANTIC (Sept. 30, 2010), http://www.theatlantic.com/politics/archive/2010/09/fmr-intelligence-director-new-cyberattack-may-be-worse-than-9-11/63849/.
[175] *See, e.g.*, Pamela Engel, *ISIS has Mastered a Crucial Recruiting Tactic No Terrorist Group has Ever Conquered*, BUS. INSIDER (May 9, 2015, 6:29 AM), http://www.businessinsider.com/isis-is-revolutionizing-international-terrorism-2015-5.
[176] *Foreign Terrorist Organizations*, U.S. DEP'T OF STATE, http://www.state.gov/j/ct/rls/other/des/123085.htm (last visited Feb. 7, 2016)
[177] *Id.* (contrasting how al Qaeda struggled to recruit a larger, young audience compared to ISIL).

enforcement, making the challenge even greater.[178] To be clear, ISIL is not a cyber-terrorist organization, but it certainly is a global one—with 20,000 foreign fighters in ninety countries around the world.[179] And indeed, 4,000 of its fighters live in Western countries.[180] However, ISIL will likely not be the the last terrorist organization, and its "hybrid" profile hints that a fully cyber-terrorist organization may be next.

A. Partisanship

Congress has attempted to provide clarity in cybersecurity law with the Cybersecurity Act of 2012—which would have set standards for protecting critical energy, transportation, water, food, and other infrastructure—but Republican senators blocked it.[181] With the current congressional makeup, a regulatory overhaul of cybersecurity law is unlikely at the federal level—but change is needed because the Executive Branch's "pervasive secrecy has left a residue of suspicion that the U.S. government has engaged in covert action using civilian intelligence agencies that operate beyond the law."[182] But amending the material support statute, rather than overhauling it or passing new law, is more likely to gain bipartisan support. On the one hand, it would seek to provide strong enforcement mechanisms for the government, and on the other, it would protect fundamental rights and Internet freedom. Before reaching the amendments, several recent examples of cyber-attacks provide insight on what a refined definition of § 2339B should consider.

B. Legal Challenges in Defining Cyber-Terrorism

---

[178] *See* Mary Anne Weaver, *Her Majesty's Jihadists*, N.Y. TIMES (Apr. 14, 2015), http://www.nytimes.com/2015/04/19/magazine/her-majestys-jihadists.html.
[179] *Id.*
[180] *Id.*
[181] *See* Siobhan Gorman, *Cybersecurity Plan Faulted*, WALL ST. J. (May 27, 2011), http://www.wsj.com/articles/SB10001424052702303654804576345772352365258 (noting that Senators and business interests on the right viewed the bill as an "overreach").
[182] *Id.* at 188-89.

Terrorism does not have a uniform definition under U.S. law,[183] so it may be unsurprising that "cyber-terrorism" does not have one either. [184] In part, this is because there are seemingly endless ways to use computers and Internet capabilities for illicit purposes, some of which include hacktivism,[185] black hat hacking,[186] cyber crime,[187] cyber espionage,[188] and information wars.[189] What, then, is cyber-terrorism? At a broad level, the most greatest obstacle in amending or addressing cyber-terrorism is the difficulty in labeling a "cyber attack" as a "cyber crime" or an act of "cyber terrorism."[190]

Cybercrime is simply "crime that is enabled by, or that targets computers.[191] Much the same as traditional theft, it can target intellectual property, by stealing trade secrets, patents, or other physical data stored on computers or networks.[192] However, cybercrime may also be used to carry out attacks to purposely disrupt the flow of data, or to carry out espionage on classified information—a problem unique to cyberspace.[193] In this respect, the conduct is distinct from a private theft—particularly if it puts national security at risk and is carried out with such intent.[194] Put differently, not all cyber-crime is cyber-terrorism.

---

[183] See *supra* note 30 (listing dozens of predicate offenses that could constitute an act of terrorism if carried out for political or religious reasons).
[184] *See* Lachow, *supra* note 208.
[185] *Id.* (targeting decisionmakers or innocent victims through protests online or distributed denial of service attacks).
[186] *Id.* These attacks target individuals, corporations, and governments with malware, viruses, worms, and hacking scripts for "personal enmity." *Id.*
[187] *Id.* Primarily, "cyber crime" also targets individuals and companies, but for economic gain. *Id.*
[188] *Id.* These attacks use a range of techniques for information-gathering for economic and political gain. *Id.*
[189] *Id.*
[190] Wilson, *supra* note 172 (addressing the difficulty of labeling where there are unknowns surrounding the "identity, intent, or the political motivations" of the alleged attacker).
[191] *See* Lachow, *supra* note 208, at 1.
[192] *Id.*
[193] *Id.*
[194] *Id*

Primarily, cyber-crime differs from cyber-terrorism based on the intent used to carry out the attack.[195] Like with the definition of "terrorism," many would agree that cyber-terrorism should include some political motivations or involve some intent to intimidate or coerce a government or its people.[196] Others believe that some physical attacks should also be considered cyber-terrorism, such as destructive attempts on critical infrastructures.[197] As Professor Jack Goldsmith argues, "the cyber attack that causes deaths" would be an easy case under current law.[198] A more difficult case would be, for example, in 2008, where Russian agents carried out three successive cyber attacks on the Estonian government by using a Distributed Denial of Service (DDoS), which "overload a victim's server" with traffic, which left the entire government, Estonian police, and even the entire Estonian banking system inoperable.[199] Attacks like these show "how crippling and warlike this form of attack can be, even absent wounded or dead."[200]

A 2007 attack shows how a cyber-attack and violent attack might be combined. In 2007, Israel hacked Syrian radar screens as part of an air-raid where Israeli jets flew seventy-five miles into Syrian airspace, destroyed a nuclear reactor, and escaped untouched.[201] Israel's "traditional" act of war was combined with "a cyber attack that cloaked Syrian air defense radar screens with a false image of a clear sky."[202] This example is instructive because The Center for the Study of Terrorism and Irregular Warfare considers it likely that a

---

[195] *Id.*
[196] *Id.* at 4.
[197] *Id.*
[198] *Id.* (citing Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUROPEAN J. INT'L L. 129-38 (2013)).
[199] See Chayes, *supra* note 170, at 131.
[200] *Id.*
[201] *See* Solis, *supra* note 3, at 6.
[202] *Id.*

severe cyber attack will be used "to supplement the more traditional physical terrorist attacks."[203]

Another major tool for cyber-criminals, and potentially cyber-terrorists, is the use of botnets. Botnets are essentially a network of computers that are all infected with malicious code, allowing a user to command them through remote-controlled commands over the Internet.[204] Estimates suggests that millions of computers around the world are infected with bot-malware, and "botmasters" like Jeanson Ancheta, a twenty-one-year-old hacker from California arrested in 2006,[205] rent these fully hacked networks to criminals who wish to commit anonymously carry out their cyber-attacks by paying hundreds of dollars an hour.[206]

Defining exactly what constitutes a cyber-terrorist attack also generates disagreement. The challenge begins with how the use of force should be included in that definition.[207] Irving Lachow, a senior associate with the Center for Strategic and International Studies, proposes that cyber-terrorism "should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism."[208] Other experts argue that it would be unreasonable to require physical destruction,[209] since cyber attacks are capable of

---

[203] Wilson, *supra* note 190, at 19.
[204] *Id.* at 5.
[205] Ancheta made more than $100,000 by advertising his services before FBI agents lured him in a sting operation. *The Case of the "Zombie King,"* FBI (May 8, 2006), https://www.fbi.gov/news/stories/2006/may.
[206] Wilson, *supra* note 190, at 5-6.
[207] Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis?, 25 STAN. L. & POL. REV. 269, 279 (2014).
[208] Irving Lachow, CYBER TERRORISM: MENACE OR MYTH 1, http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-19.pdf (last visited Jul. 5, 17).
[209] Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-defense*, 38 STAN. J. INT'L L. 207, 222 (2002). Jensen's argument involved defining cyber-attacks, not specifically cyber-terrorism.

crippling national infrastructure, which may lead to civilians and military deaths without the use of a "traditional kinetic weapon."[210]

For an international perspective, NATO uses the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which offers a definition that is both geographic and effects-based. It phrases a cyber-attack as "a trans-border cyber operation whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects."[211] The manual provides a useful definition that refines some of the differences between traditional and cyber-terrorism.[212] Particularly relevant, the authors of the Manual arrived at the definition by "drawing a parallel to implanting land mines," which—like cyber-attacks and malware—may or may not cause eventual damage, but the mere act of placing one should constitute an act of terrorism.[213]

C. Practical Issues: Will Attribution Issues Mean Penalizing Support to Unknown Terrorists?

The biggest challenge in punishing cyber-terrorism, from a practical perspective, is known as "the dilemma of attribution."[214] The term refers to the challenge of determining who is responsible in an area where "[l]inks between computer hackers and terrorists . . . may be difficult to confirm."[215] Terrorist groups already use the Dark Web, a non-indexed[216] part of the Internet allowing for almost complete anonymity.[217] Though outside the scope of this Note's proposals, the government uses various tools to track individuals who use cloaking methods to hide their IP addresses.[218] The relevance to this Note, however, is that attribution challenges the ability of law enforcement to use the material support statutes because §

[210] *See* Solis, *supra* note 3, at 16.
[211] MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE Rule 30, at 106 (Cambridge Univ. Press, 2013).
[212] Chayes, *supra* note 170, at 138.
[213] *Id.* at 137.

2339B requires the organization to be foreign.[219] Specifically, Congress and the DOJ will need to consider whether anonymous material support could result in a prosecution.

In summary, political, legal, and practical obstacles converge to highlight the challenge that Department of Justice and the U.S. Attorneys' Office will be forced to confront in future prosecutions. Defining "cyber-terrorism" explicitly would enable the criminal law to prohibit individuals from carrying those attacks out. Similarly, defining the cyber-terrorism problem would enable the USAO to properly apply § 2339B to attempts to support these new types of organizations and the attacks. Ultimately though, definitions alone do not capture how the law would apply in situations where a person anonymously carries out an attack. For the same reason, it would be difficult to punish an individual for supporting, inadvertently, an anonymous online group that happened to be a cyber-terrorist by definition.

Ultimately, however, the "material support" statutes were designed with a preventative vision, with Congress's belief that "isolating and starving these organizations would lessen the risk of terrorism."[220] The question is whether the tools used to combat "traditional" terrorism—like hijacking, kidnapping, and violence—may be toothless when

---

[214] Jeffrey Thomas Biller, *Cyber-Terrorism: Finding a Common Starting Point*, 4 CASE W. RESERVE J.L. TECH & INTERNET 276, 331 (2013).
[215] Wilson, *supra* note 190, at 17.
[216] Non-indexed sites do not appear in web searches. Daniel Messier, *The Internet, the Deep Web, and the Dark Web*, WORDPRESS, https://danielmiessler.com/study/internet-deep-dark-web/, (last visited
[217] Natasha Bertrand, *ISIS is Taking Full Advantage of the Darkest Corners of the Internet*, BUS. INSIDER (July 11, 2015, 11:26 AM), http://www.businessinsider.com/isis-is-using-the-dark-web-2015-7 (describing that Dark Web by comparing how "[j]ust as an onion has multiple layers, onion rooting on Tor protects people's identities by wrapping layers around their communications").
[218] *Id.*
[219] Biller, *supra* note 214, at 347.
[220] Fiss, *supra* note 145, at 202.

they are used to prevent individuals from aiding terrorists in attacking infrastructures such as power grids, emergency services, civilians, or the military.[221]

IV. APPLYING § 2339B TO MATERIAL SUPPORT FOR CYBER-TERRORIST ORGANIZATIONS: LIMITATIONS AND PROPOSALS

There have been significant efforts in scholarship to address new forms terrorism,[222] the First Amendment and online association and speech,[223] and the issue of cybersecurity law generally.[224] Several of these contributions aim to provide new definitions for "cyber-terrorism" and also include ways to distinguish "cyber-crime" from "cyber-terror."[225] However, little scholarship addresses the specific question of how § 2339B can be used to combat the efforts to legitimize cyber-terrorist organizations through the provision of online material support. It is unclear how Congress would have drafted § 2339B if the Internet existed with the pervasiveness that it has today,[226] but scholars have offered some proposals on how the Act might be updated, but they mostly respond to a slightly different problem: online material support to traditional FTO's. Before arriving at a proposal, I briefly critique the reasons that these proposals cannot be used for cyber-terrorism.

A. Limitations in the Plain Language of the Statute

---

[221] Gabriel Weimann, SPECIAL REPORT, CYBERTERRORISM: HOW REAL IS THE THREAT 1, U.S. INST. OF PEACE (Dec. 2004), http://www.usip.org/sites/default/files/sr119.pdf.
[222] *See supra* note 8.
[223] *See supra* notes 104, 121, 124 and accompanying text.
[224] *See generally* Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV 1475.
[225] *See* Williams, *supra* note 85, at 383; Peterson, *supra* note 118, at 304; Tunis, *supra* note 120.
[226] *But see* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW 85-86 (Thomson/West 2012) ("The First Amendment, it is sometimes said, would not apply to the Internet . . . Drafters of every era know that technological advances will proceed apace and the rules they create will one day apply to all sorts of circumstances that they could not possibly envision."). In other words, the meaning of a rule is constant, but the application of the rule will vary, like in *Kyllo v. United States*, 533 U.S. 27 (2001), where the Court applied the "unreasonable search and seizure" language to a thermal imager, despite there being no conception of such technology when the Fourth Amendment was ratified. *Id.*

The Executive Branch is not contemptuous about protecting individual rights,[227] yet in the absence of more effective tools it will be required to use § 2339B. As currently drafted, the statute only applies to "foreign" terrorist organizations, a definition that becomes unclear with potential online terrorist beneficiaries.[228] Second, even if an online beneficiary's identity is known, an individual who provides material support would not have knowledge of "terrorist activity" or "terrorism"—which rely on traditional acts of violence.[229] This problem is not a theoretical one; *Al-Hussayen* shows that online support—like providing website maintenance—could be too abstract for a jury to find an individual intended to knowingly support terrorism.[230] And though *Mehanna* and *Al-Kassir* reached convictions and involved online support, those cases also involved "traditional" material support.[231] However, "combination" cases like these will be unlikely with cyber-terrorist organizations, where substantially all interactions will be online—including the potential attacks.

Jeffrey Biller suggests that Congress should modify § 2339B to explicitly define a cyber-terrorist organization as either a "foreign organization" or one that "conducts operations primarily through cyberspace."[232] The problem with Biller's proposal is that at some level of Internet use, domestic organizations would also fall under § 2339B's ban on material support. This would be problematic because Congress envisioned § 2339A as the tool to prevent support to domestic terrorist groups, evinced by the word "foreign" only in §

---

[227] *See* supra note 140 and accompanying text (noting the Supreme Court's recognition of Congress's vision that § 2339B would not violate the First Amendment).
[228] *See* 18 U.S.C. § 2339(B)(a)(1).
[229] *See supra* Section I.B.
[230] Fick, *see supra* note 90. (describing how one juror said after Al-Hussayen's acquittal, "There was no clear-cut evidence that said he was a terrorist, so it was all on inference.").
[231] *See supra* Section I.C.
[232] Biller, *supra* note 214, at 348.

2339B.[233] That aside, Biller does not address how an individual would "knowingly" provide material support to such a cyber-terrorist organization—despite the fact that "terrorist activity" and "terrorism" do not encompass cyber-attacks.[234]

Professor Alan Williams proposed an Internet-specific addition to the material support statute, titled the "Use of Internet Websites with Specific Intent to Facilitate Terrorism."[235] According to Williams, the government was right to charge the defendants in *Mehanna* and *Al-Hussayen* for using the Internet to support terrorism, but the material support statutes "were the wrong tools for initiating a prosecution."[236] It is true that greater specificity with online terrorism would clearly direct the Executive about using § 2339B for online activities with the material support statute.[237] But the problem is that Williams' definitions are too specific, since they would only criminalize a person who "[e]stablishes or maintains Internet websites or posts . . with the specific intent to recruit persons . . . encourage violent attacks . . . or assist, encourage, or facilitate funding."[238] Consequently, these definitions do not grapple with the new issues that purely cyber-terrorist organizations would present.

Of course, cutting off efforts to maintain websites, recruit, encourage violent attacks, or provide funding is important—whether online or not—cyber-terrorist groups would escape many of these definitions. For example, the Act should be able to prevent hackers like Jeanson Ancheta from renting botnet services to cyber-terrorists and assisting potential cyber-acts of terrorism in the process.[239] It should also consider the varied attacks that an

---

[233] § 2339A requires specific-intent to further a terrorist act, making it more narrow and less likely to trigger First Amendment scrutiny if speech were made in furtherance of a criminal act.
[234] *See* Biller, *supra* note 214.
[235] Williams, *supra* note 85, at 383-84.
[236] *Id.; see also supra* notes 84-91.
[237] Williams, *supra* note 85, at 383-84.
[238] *Id.*
[239] *See* Wilson, *supra* note 190, at 5-6.

organization may use to cripple computer networks or infrastructure without violence—such as with Distributed Denial of Service overloads.[240] Merely relying on prohibitions related to website maintenance, therefore, does not go far enough. Moreover, Williams would not amend the definitions required to "knowingly" provide material support, instead relying on the definitions of "terrorism" and "terrorist activity,"[241] neither of which extend far outside of violent acts and, therefore, fail to adequately prevent a person from inadvertently providing material support to a cyber-terrorist organization.

Others believe that § 2339B is entirely flawed because it misunderstands how modern terrorist organizations operate. These arguments are premised on the view that an organization-focused system that "criminalizes 'material support' based on the identity of the recipient must be certain that it defines the category of forbidden recipients accurately."[242] Andrew Peterson, a member of the NYU Center on Law and Security, argues that such a definition is not possible because it is a misconception to think terrorists are "highly organized groups with members and representatives," or that "'operatives carry membership cards in their wallets.'"[243] Peterson argues that the FTO designation process "provide[s] a strong incentive for existing non-violent organization to remain non-violent."[244] Additionally, the labeling approach of FTO's struggles to handle situations where a group simply changes its name,[245] has no "formal" membership process,[246] or keeps its activities

[240] *Id.*
[241] *Id.* at 384.
[242] Peterson, *supra* note 118, at 338.
[243] *Id.* (quoting Matthew Levitt, *Untangling the Terror Web: Identifying and Counteracting the Phenomenon of Crossover Between Terrorist Groups*, SAIS REVIEW 34 (2004).
[244] *Id.* at 344.
[245] Peterson points to a situation where notorious terrorist, Al Musab al Zarqawi, changed the name of his group two days after it was designated, and the United States did not respond for two months. *Id.* at 347.
[246] *Id.* (noting that al Qaeda has trained 10,000 potential terrorists but had only formally sworn in roughly 10–30 % of them).

anonymous—all of these arguments are cogent issues with cyber-terrorism and, therefore, complicate whether a person knowingly provided material support under § 2339B.

In contrast to both Biller and Williams, Daniel Hoffman argues that no amendments are necessary, and that § 2339B is capable of evolving to meet the challenges associated with online material support.[247] He argues that "new statutes and tests would be redundant to existing law and only confuse and complicate the issue further."[248] Hoffman suggests that though free speech and prosecutions for online terrorism advocacy are in tension, the courts will explore these issues through the development of case law.[249] Hoffman's point is an important counterweight to the suggestion that amending the statute will clarify its application, but his conclusion is difficult to justify given the judicial deference that resulted in relatively weak protection for constitutional rights in the post-9/11 era.

B. Rooted in the Constitution: The First Amendment & Judicial Deference

With online-exclusive organizations, the U.S. Attorneys' Office would be forced to argue that cyber-terrorist organizations are sufficiently "foreign," an undefined term in § 2339B. This definitional "stretching" could fall into the pattern of judicial deference that preceded *Humanitarian Law Project* in one of two ways. Either courts will distinguish cyber-terrorism from traditional terrorism and hold that § 2339B no longer capably delineates criminal acts from independent advocacy and speech, thereby violating the First Amendment. Alternatively, judicial deference will continue, and the Executive Branch's expertise will remain too difficult for generalist courts to meaningfully question, leading to chilled speech

[247] Hoffman, *supra* note 123, at 251.
[248] *Id.*
[249] *Id.* at 204.

and association.[250] Therefore, the law either becomes toothless or it becomes overly restrictive.

In *Humanitarian Law Project*, the Court stated that "in the context of international affairs and national security" the government need not provide a conclusive link between "material support" and a terrorist attack.[251] Rather, it can necessarily paint "with a brush broader" than it uses for domestic areas.[252] These differences cast doubt on whether § 2339B would survive a First Amendment challenge if the courts did not give similar weight to the regulation of foreign affairs.[253] Many scholars have seized on *Humanitarian Law Project* and the regulation of online interactions as problematic, arguing that § 2339B already chills free speech and association,[254] and the law is ineffective.[255] Others suggest that, at a minimum, new amendments are needed[256] and predict that § 2339B would fail if applied to a quasi-domestic organization that uses domestic website domains, like Twitter, to support itself.[257]

In sum, an amendment to § 2339B is necessary but not sufficient. A cyber-terrorist organization may never commit acts of traditional violence, making it difficult to prove that an individual "knowingly" provided support to a group known to engage in "terrorism" or "terrorist activity." Moreover, unless *Humanitarian Law Project* is overruled, amending the statute seems unnecessary if the only argument is that applying the law endangers the First Amendment—an issue resolved in *Humanitarian Law Project* in favor of the government's

---

[250] *See supra* Section II.C.
[251] *Humanitarian Law Project*, 561 U.S. at 34-35.
[252] *Id.* (citing Zemel v. Rusk, 381 U.S. 1, 17 (1965).
[253] *See id.* at 38.
[254] *See* Tunis, *supra* note 120, at 290.
[255] *Id.*
[256] *See* Hoffman, *supra* note 123, 216.
[257] *See* Sutherland, *supra* note 124, 229.

regulation, even where plaintiffs sought to provide unobjectionably harmless legal aid.[258] To be sure, the Internet was not the issue in *Humanitarian Law Project*, and both *Mehanna* and *Al-Hussayen* (the Internet § 2339B cases) show that it is far more difficult to prosecute material support made online, but that's not all. With cyber-terrorist organizations, the mens rea for "knowingly" providing support barely fits, and the beneficiaries are not certainly "foreign" terrorists.

V. A SUICIDE VEST: PROPOSED REFORMS TO PREVENT MATERIAL SUPPORT FOR CYBER-TERRORISM AND TO PRESERVE CONSTITUTIONAL FREEDOMS

The proposals aimed at updating § 2339B do not venture far enough into the difficult territory of online interaction. By remaining tethered to traditional, violent terrorism—they leave gaps for cyber-terrorist organizations to emerge. Congress should amend the Act in light of these grave threats—but an amendment alone will not be sufficient unless it protects the First Amendment concerns that are part-and-parcel to banning material support.

There is no question that § 2339B is deficient when applied to cyber-terrorism. The first step, then, is that Congress should expand coverage not only to FTO's but to CTO's too. While many scholars have attempted to define "cyber-terrorism," the best option is to delegate this issue and certain other definitions to the Department of Justice to resolve in notice-and-comment rulemaking.[259] Second, Congress should also address how a person can "knowingly" provide material support to a CTO—again, by delegating to the DOJ with instructions to clarify how a person should know or reasonably know that they are assisting a potential online terrorist. Third, because the Internet presents a new challenge for law

[258] *Humanitarian Law Project*, 561 U.S. at 38.
[259] *See* § 2339B.

enforcement in attributing responsibility for cyber-attacks carried out anonymously.[260] To the extent practicable, the DOJ would be required to explain how it will use § 2339B with respect to anonymous web traffic—hoping to uncover the sources of cyber crime and the perpetrators.[261]

A. Proposed Legislative Changes

Congress, should begin by providing a broad definition of cyber-terrorism that would be filled in by the agency. One way to explicitly incorporate cyber-terrorism would be to add a provision that takes a practical view of cyber-terrorists. It would exclude the word "organization" in favor of the word "operation," thereby limiting the likelihood that the group could merely change its name and avoid coverage. For example, Congress could amend § 2339B(a)(1) to state:

> Whoever knowingly provides material support or resources to a foreign terrorist organization, *or to a trans-border cyber operation*, or attempts or conspires to do so, shall be fined 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.[262]

One solution that could be used here, particularly because it would also address how a person "knowingly" provided support, would be to add a cyber-specific knowledge provision stating:

> 2339B(k). If a violation is based on providing material support or resources to a trans-border cyber operation, or attempting or conspiring to so provide, a person shall be convicted based upon knowledge that the trans-border cyber operation would be *reasonably expected* to cause injury or death to persons, or damage or destruction to objects.

---

[260] *See* Biller, *supra* note 214, at 331-33.
[261] *See supra* note 218.
[262] *See* § 2339B(a)(1).

This amendment would incorporate a provision that defines cyber-terrorism explicitly, but would delegate to the DOJ an explanation of what circumstances would lead a person to "reasonably" expect their actions to cause injury, death, damage, or destruction.

A significant shortcoming with § 2339B is it relies on knowledge of violence, and scholars disagree about whether cyber-attacks and cyber-terrorism should require some measure of violence. Ultimately, the definition need not be binary.[263] If a cyber operation is "reasonably expected" to cause either injury or death—i.e., like traditional, violent terrorism—or, alternatively, damage or destruction to computers and networks, then the debate about whether the definitions should retain violence can be resolved in favor of a broad definition that incorporates both. The Israeli takeover of Syrian air defense while simultaneously launching an airstrike shows why a broad definition best serves the preventative purpose of the AEDPA.[264] Assume that a terrorist group, interested in carrying out a violent attack on a populated city "rented" the services of an online organization to cripple communications and emergency response services. If the Executive branch required proof of a violent activity to consider the cyber-group's action "cyber-terrorism" shutting down communications would not constitute terrorist activity, and material support could flow freely to that group without prosecution.

As mentioned previously, an amendment alone will not ensure an appropriate response to cyber-terrorism. This is due in part to the judicial phenomenon that occurred in the 9/11 era, which made counter-terrorism law "unusually enduring."[265] To preempt the executive branch from "stretching" aging bodies of law, and to prevent further judicial

[263] *See supra* notes 184-207 and accompanying text.
[264] *See supra* notes 201-203 and accompanying text.
[265] *See supra* note 157.

deference, review of agency rules will ensure better footing for judicial review than is currently available.

B. Statutory "Mending" of Grey Holes: Why Mandatory Rulemaking Can Sharpen § 2339B and Protect First Amendment Rights

If Congress extends the application of § 2339B to cyber-terrorists, then it must ensure protection of the First Amendment for online activities. One solution for ensuring adequate protection of association and speech would be a congressional mandate ordering the Department of Justice to pass a rule clarifying how "material support" might apply online, specifically with cyber-terrorist organizations. Requiring the Department of Justice to explain when online association and speech would cross into illegal activity—such as "training," "expert assistance," "service," or "personnel"—would ensure that First Amendment activities are not chilled.[266] In addition, law enforcement experts, cybersecurity interests, and others would be able to comment on national security concerns in the creation of the rule. The result would be a balanced rule, leaving courts with better footing to judge eventual agency action.

A pervasive assertion has emerged in administrative law that "the rule of law inevitably bends under the demands of state necessity during national emergencies."[267] Adrian Vermeule, argues that during emergencies, courts use flexible interpretive tools, or "grey holes," to "preserve the façade, but not the reality" of judicial review.[268] Professor Evan Criddle challenges Vermeule's theory that grey and black holes are inevitable, by—somewhat ironically—pointing to several post-9/11 terrorism lower court cases that involved

[266] *See supra* Section II.C.
[267] Evan J. Criddle, *Mending Holes in the Rule of (Administrative) Law*, 104 NW. U. L. REV. COLLOQUY 309, 309 (2010).
[268] Vermeule, *supra* note 147, at 1096.

thorough judicial review.[269] Criddle argues these holes can be mended by Congress ensuring proportional, fair, reasonable, and transparent action by federal agencies.[270] Since Criddle's focus is on counter-terrorism law, it follows that in terms of extending § 2339B to cyber-terrorist organizations, it would be beneficial to require the Department of justice "to develop . . . ad hoc administrative procedures for emergencies, subject to broad congressional standards and judicial review."[271]

Distinguishably, the proposal offered here is not meant to suggest that cyber-terrorism is an "emergency," as Vermeule and Criddle use that term. Rather, Vermeule's concerns and Criddle's response are useful here to proactively ensure that grey holes, which are already present in counter-terrorism law, are not carried into cyber-space.[272] Due to the heightened constitutional concerns and greater ambiguity with online interactions, a mandatory order for notice-and-comment rulemaking would ensure that civil-rights activists, free-speech organizations, and other interested parties would have an opportunity to voice concerns about the potential for criminal prosecutions in cyberspace.[273]

Possibilities of material support include social media companies that allow terrorists to use their services.[274] It is arguable that this conduct would already fit into the framework used in non-cyber-terrorist cases, where courts have drawn a line between the *act* of providing support, and the incidental speech that it might include.[275] In these cases, courts

---

[269] Criddle, *supra* note 267, at 312-13 (rejecting the notion that proper judicial review is "institutionally impossible.").
[270] *Id.*
[271] *Id.* at 311.
[272] *See id.*
[273] *See id.*
[274] Emily Goldberg Knox, *The Slippery Slope of Material Support Prosecutions: Social Media Support to Terrorists*, 66 HASTINGS L.J. 95, 95 (2014).
[275] *See supra* note 78 and accompanying text (explaining the distinction).

have held that § 2339B targets conduct, not the speech elements, and therefore, it can be upheld under intermediate scrutiny.[276]

Perhaps though, that example is too easy. Instead, consider whether an online posting requesting assistance in perfecting 3D-printer code might be considered material support if the group requesting it were a "trans-border cyber operation." Assume that these cyber-terrorists—hoping to create a better prototype that could be sold on the black market to violent terrorists who wished to slip by security gates with a non-metal pipebomb—posted their request anonymously on the website 4chan.org.[277] Similarly, terrorists are using the Dark Web, where users use re-routing techniques to ensure their communications are anonymous. Next, assume an individual with benign motives, but who is skilled in 3D-printing, responded to the posting, opened the sample code, and discovered it appeared to be code that would print a generic 3D-cylinder. Based on a review of the coding and programming, the individual notices that the calibration of the printer is slightly off, causing an imperfect curve in the cylinder when it is printed. If the student were to provide her insight, suggesting some changes, would this be considered "expert assistance" or "training?"[278] Moreover, if computer code were classified as speech, has the student acted independently, or in coordination with the purported terrorist organization? These are questions that the DOJ should consider—particularly, should there be a safe harbor for ignorantly provided material support?

---

[276] *See id.*
[277] The hacktivist group, Anonymous, actually originated on this website in 2004. *See* Becca Stanek, *How Did Anonymous Start: The History of the Mysterious "Hacktivist" Group Began Quite Some Time Ago*, BUSTLE (Feb. 20, 2015), http://www.bustle.com/articles/65444-how-did-anonymous-start-the-history-of-the-mysterious-hacktivist-group-began-quite-some-time-ago.
[278] *See* 18 U.S.C. § 2339A.

It would appear that specialized coding techniques fit the definition of expert assistance, yet all "material support" must be knowingly provided to a terrorist organization.[279] The anonymity of a terrorist organization would likely be an issue, yet certain websites—particularly those on the Dark Web—might put a person on reasonable notice that refining what appeared to be a synthetic pipe bomb might be "reasonably expected to cause injury or death to persons, or damage or destruction to objects."

These novel questions require more guidance than was necessary when AEDPA passed, since the traditional acts of terror of that era were concretely tied to variations of already well-known acts of war, like bombings and other violence or use of weaponry. Requiring a rule on the application of § 2339B to cyber-terrorist organizations would enable open discourse about the concerns that cyber-terrorism presents, as well as the First Amendment challenges. At the same time, it would act to reduce the shortcomings of the courts in making value judgments between national security and fundamental rights.

C. Statutory "Mending" of Legal Grey Holes: Re-aligning Judicial Review to Protect the First Amendment

There is a "'strong presumption that Congress intends judicial review' of administrative action,'" rooted in the Administrative Procedure Act and Supreme Court precedent.[280] Yet as many constitutional law scholars have noted, counterterrorism law has proven "unusually enduring" to judicial review.[281] The judiciary faced a difficult situation in balancing constitutional freedom and national security.[282] As the Supreme Court said in *Humanitarian Law Project*, the "competence of the courts" in analyzing, weighing, and

[279] *See* 2339A(b).
[280] *See* VANESSA K. BURROWS & TODD GARVEY, A BRIEF OVERVIEW OF RULEMAKING AND JUDICIAL REVIEW, CONG. RES. SERV. (Jan. 4, 2011), http://www.wise-intern.org/orientation/documents/crsrulemakingcb.pdf.
[281] *See supra* notes 155, 157, 165.
[282] *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 33 (2010).

drawing inferences about the causes of terrorism is markedly inferior to the civil-government actors, namely, officials in the Justice Department, the State Department, the Department of Homeland Security, and others.[283] But the Framers viewed the judiciary as "an intermediate body between the people and the legislature, in order, among other things, to keep the latter within the limits assigned to their authority."[284]

Therefore, statutory reworking is necessary to ensure that not only do the courts exercise judicial review in counter-terrorism cases, but that they do so meaningfully. With judicial review regarding the the constitutionality of §2339B charges at the back-end, when charges are already in place, judicial deference is more likely to occur. Therefore, Congress should seek to "create" judicial review at the front-end of the material support statute's application, the rulemaking stage, where the pressures of deciding between releasing a potential terrorist are less likely to influence the judge's decision to defer to Executive competence.

CONCLUSION

Applying § 2339B to cyber-terrorism will require the USAO to confront new challenges unlike any previously encountered in preventing traditional terrorism. Given the judicial-deference phenomenon that occurred after September 11th, a multi-faceted approach to revising § 2339B is necessary. Without clarification, the material support statute runs the risk of being unconstitutional by restricting the right to associate and speak in online fora. Alternatively, it runs the risk of receiving judicial deference, thereby infringing First Amendment rights. In either situation, the outcome is negative. A toothless law will enable

[283] *See id.*; *see also* CHAYES, *supra* note 170, at 148 (depicting a chart of civil–military actors involved in cyber attacks and cyber warfare).
[284] THE FEDERALIST NO. 78, 394 (Alexander Hamilton) (Ian Shapiro ed., 2009).

terrorism under the shroud of Internet activity—making the First Amendment into a constitutional "suicide vest" because by protecting speech, national security may be watered down. Therefore, to ensure both goals are met, directing the DOJ to initiate rulemaking will create guidelines that consider these obstacles. The result will be a more suitable position for judicial review, more transparency in prosecutions, and strong national security protections.