South Carolina Law Review

Volume 71 | Issue 2 Article 10

Winter 2019

An Information Operations Theory of Domestic Counterterrorism Efforts

Tung Yin
Lewis & Clark Law School

AN INFORMATION OPERATIONS THEORY OF DOMESTIC COUNTERTERRORISM EFFORTS

Tung Yin*

---

* Professor of Law, Lewis & Clark Law School. Thanks to participants at the Southwest Criminal Law Workshop, especially Carissa Hessick, for helpful thoughts on an early version, and to Keightley Wilkins (class of 2020) for research assistance.

I. INTRODUCTION

A day after terrorists hijacked four passenger planes and crashed them into the World Trade Towers and the Pentagon on September 11, 2001, killing nearly 3,000 people, President George W. Bush demanded of Attorney General John Ashcroft, CIA Director George Tenet, and FBI Director Robert Mueller, "Don't ever let this happen again."[1]

Responding to the President's directive, Ashcroft, Tenet, Mueller, and other high-level executive branch leaders embarked on a wide variety of counterterrorism actions, including criminal investigations and prosecutions, immigration enforcement, military attacks in multiple Middle Eastern countries, and imposition of broad surveillance programs inside the United States.[2] President Bush's approval rating in the immediate aftermath of 9/11 skyrocketed to among the highest in Gallup history, but that popularity—and "widespread public support for a war against terrorism"[3]—soon faded. One indication of the drop in support is that in 2004, Michael Moore's *Fahrenheit*

---

1. *See* GARRETT M. GRAFF, THE THREAT MATRIX: THE FBI AT WAR IN THE AGE OF GLOBAL TERROR 395 (2011); JOHN ASHCROFT, NEVER AGAIN: SECURING AMERICA AND RESTORING JUSTICE 130 (2006).

2. *See* ASHCROFT, *supra* note 1, at 131–42; *Structural Changes to Enhance Counter-Terrorism Efforts*, U.S. DEP'T OF JUST. ARCHIVES, https://www.justice.gov/archive/911/counterterrorism.html [https://perma.cc/E65L-N7R4].

3. David W. Moore, *Bush Job Approval Highest in Gallup History: Widespread Public Support for War on Terrorism*, GALLUP (Sept. 24, 2001), https://news.gallup.com/poll/4924/bush-job-approval-highest-gallup-history.aspx [https://perma.cc/YDW5-QWAR].

9/11, a scathing denunciation of the Bush Administration's post-9/11 policies, "becam[e] the highest grossing documentary of all time."[4]

Much of the academic and political criticism of the Bush Administration's counterterrorism strategy centered on the perceived illegality of the "global war on terrorism."[5] One common argument was that a non-state group could not be the target of military force, only law enforcement efforts, and therefore the military attacks against al Qaeda were unlawful.[6] Secondary lines of criticism focused on the methods the United States used to wage war against al Qaeda, such as the indefinite detention of captured fighters at the naval base on Guantanamo Bay,[7] and the use of armed drones to attack suspected terrorists and insurgents in Afghanistan and elsewhere, particularly where the targets were American citizens.[8] The domestic actions were no less controversial. The warrantless electronic surveillance of Americans' e-mails and telephone calls triggered Fourth Amendment objections,[9] while the criminal terrorism prosecutions drew protests of entrapment.[10]

This Article starts from the premise that terrorism is a form of asymmetric warfare and counterterrorism accordingly has elements in common with counterinsurgency. This is, to be sure, not a novel premise;[11] among other things, it was a crucial implication of President Bush's rhetoric of a "war against terrorism."[12] The most obvious analogical comparison of the U.S.

---

4. Owen Gleiberman, *How Michael Moore Lost His Audience*, VARIETY (Sept. 23, 2018), https://variety.com/2018/film/columns/how-michael-moore-lost-his-audience-fahrenheit-11-9-1202953813/ [https://perma.cc/U7T6-Y3NA].

5. *See, e.g.*, President George W. Bush, 9/11 Address to the Nation (Sept. 11, 2001) (audio and transcript available at https://americanrhetoric.com/speeches/gwbush911addresstothenation.htm) [https://perma.cc/YYG9-GZGC].

6. *See, e.g.*, Tung Yin, *Broken Promises or Unrealistic Expectations?: Comparing the Bush and Obama Administrations on Counterterrorism*, 20 TRANSNAT'L L. & CONTEMPORARY PROBS. 465, 475 (2011).

7. *See, e.g.*, Oona Hathaway et al., *The Power to Detain: Detention of Terrorism Suspects After 9/11*, 38 YALE INT'L L.J. 123 (2013).

8. *See, e.g.*, Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010); *but see* Alberto R. Gonzales, *Drones: The Power to Kill*, 82 GEO. WASH. L. REV. 1 (2013) (defending the legality of the drone strike that killed Anwar al-Aulaqi).

9. *See infra* Section IV.C.

10. *See infra* Section IV.D.

11. *See, e.g.*, Aziz Z. Huq, *The Social Production of National Security*, 98 CORNELL L. REV. 637, 664 (2013); Sahar F. Aziz, *Policing Terrorists in the Community*, 5 HARV. NAT'L SECURITY J. 147, 148 (2014); Samuel J. Rascoff, *Establishing Official Islam? The Law and Strategy of Counter-Radicalization*, 64 STAN. L. REV. 125, 137 (2012).

12. *See* President George W. Bush, State of the Union Address to a Joint Session of Congress and the American People (Sept. 21, 2001) (transcript available at

response to 9/11 to traditional warfare are the attacks launched against al Qaeda and the Taliban pursuant to the November 17, 2001, Authorization to Use Military Force (AUMF),[13] with the AUMF being the functional equivalent of a declaration of war.[14]

The most obvious implication of counterterrorism as warfare is the legal ability to use military force to capture or kill the targets of the AUMF.[15] But while that legal position might arguably extend even to the right to attack AUMF targets on U.S. territory, no American president has gone so far (yet) as to order the use of lethal force against a person on U.S. soil.[16] There is, however, another implication of counterterrorism as warfare—namely, information operations, which is to say, the use and control of information as a tool to deceive, confuse, and identify and locate the enemy.

The information operations analogy fits counterterrorism because the primary challenge for counterterrorism officials is locating and identifying domestic terrorists, as opposed to stopping identified terrorists. Locating and identifying them is not only a geographic or spatial matter but also one of discerning intentions and goals. Reading threatening or disturbing public social media postings, following up on tips, and conducting electronic surveillance of e-mails all find analogues in information operations. And using undercover sting operations to discern the intentions and goals of the targets serves a number of the purposes of information warfare, including identification and deception of the enemy. But a critical conclusion of the analogy is that such sting operations need to mimic actual terrorist recruiting, or else they are not accurately identifying and detecting the enemy.

Part II of this Article discusses the threat of terrorism in the United States, with particular emphasis on "lone wolf" attackers. Part III examines the role that information plays in modern warfare, ranging from code breaking, to

---

https://www.theguardian.com/world/2001/sep/21/september11.usa13) [https://perma.cc/V9RX-66RA].

13. Authorization for Use of Military Force, Pub. L. No. 107-40, § 2, 115 Stat. 224 (2001).

14. *See* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047 (2005).

15. *See* Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

16. Then-Vice President Cheney may have been prepared to order American fighter pilots to shoot down hijacked Flight 93 had they intercepted it in time, but it does not appear that the order was actually given. *See* NAT'L COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 40-42 (2004) [hereinafter THE 9/11 COMMISSION REPORT]. Additionally, President Bush did invoke the AUMF to justify military detention of two American persons, citizen Jose Padilla and resident Ali al-Marri, as "enemy combatants." *See* Tung Yin, *Enemies of the State: Rational Classification in the War on Terrorism*, 11 LEWIS & CLARK L. REV. 903 (2007).

target detection, to communications jamming, to deception. Part IV describes domestic counterterrorism policies, laying the groundwork for Part V, in which the Article argues that those counterterrorism policies can be analogized to information operations. Finally, Part VI draws lessons from the information operations analogy for the counterterrorism tactic of undercover sting operations.

II. POST-9/11 DOMESTIC TERRORISM: THE THREAT VERSUS THE HYPE

The September 11, 2001, terrorist attacks in New York and Washington, D.C., were the exclamation point to a series of terrorist attacks launched by organized foreign groups against U.S. targets beginning nearly two decades earlier with two Hezbollah-directed suicide bombings in Lebanon in 1983.[17] Other attacks against U.S. targets overseas included the 1993 ambush of U.S. troops in Somalia (the "Black Hawk Down" mission);[18] the 1996 Khobar Towers bombing in Riyadh, Saudi Arabia, which killed nineteen U.S. Air Force personnel;[19] the 1998 simultaneous bombing of U.S. embassies in Kenya and Tanzania;[20] and the surprise attack on the destroyer *U.S.S. Cole* while it was docked in Yemen in late 2000.[21]

Meanwhile, in 1993, terror struck the homeland when Ramzi Yousef—nephew to 9/11 mastermind Khalid Sheikh Mohammed—carried out a truck bombing of the World Trade Center that killed six and injured over 1,000 people.[22] Yousef was in the midst of testing a follow-up attack that would have bombed eleven airplanes over the Pacific Ocean when he was captured

---

17. *See Beirut Marine Barracks Bombing Fast Facts*, CNN, https://www.cnn.com/2013/06/13/world/meast/beirut-marine-barracks-bombing-fast-facts/index.html [https://perma.cc/4FPH-AXRJ]. Arguably, one could date the beginning of this current wave of terrorism to 1979, with the Iranian takeover of the U.S. embassy in Tehran. *See* MARK BOWDEN, GUESTS OF THE AYATOLLAH: THE FIRST BATTLE IN AMERICA'S WAR WITH MILITANT ISLAM 28–64 (2006); BRUCE HOFFMAN, INSIDE TERRORISM 258 (rev. ed. 2006) ("The pivotal event in the emergence of state-sponsored terrorism as a weapon of the state and an instrument of foreign policy was doubtless the seizure in November 1979 of fifty-two American hostages in at the U.S. embassy in Tehran by a group of militant Iranian 'students.'").

18. American forces were stationed in Mogadishu. *See, e.g.*, MARK BOWDEN, BLACK HAWK DOWN: A STORY OF MODERN WARFARE 3 (1999).

19. LAWRENCE WRIGHT, THE LOOMING TOWER 237 (First Vintage Books ed., Vintage Books 2007) (2006).

20. *Id.* at 306.

21. *Id.* at 360–61.

22. *See* SIMON REEVE, THE NEW JACKALS: RAMZI YOUSEF, OSAMA BIN LADEN AND THE FUTURE OF TERRORISM 6–15 (1999). Yousef and his co-conspirators had hoped to topple one tower into the other, with the ensuing carnage killing as many as tens of thousands. *Id.* at 24.

by Pakistani authorities in 1995 and rendered to the United States.[23] In that same year, Timothy McVeigh parked a truck bomb next to the Murrah Federal Building in Oklahoma City. The blast destroyed the building, killed 168 people, and injured over 500 others.[24]

A. Expert Disagreement on the Nature of the Threat

In the years after 9/11, two of the country's leading terrorism experts embarked on a vociferous debate about the true nature of the terrorism threat faced by the United States.[25] The view that had dominated American counterterrorism policy, as exemplified by RAND (Research and Development) Corporation's Bruce Hoffman, continued to view top-down terrorism directed by al Qaeda and other international groups as the top priority, despite the destruction of al Qaeda's terrorism training camps in Afghanistan and the routing of its Taliban protectors by 2002.[26] According to Hoffman, al Qaeda still represented a serious threat to the United States "more as an ideology that [had] become a vast enterprise" with the capability to plan new attacks.[27] At the time he published the second edition of his book *Inside Terrorism*, al Qaeda still counted among its members "at least eighteen thousand individuals who trained in [its] Afghanistan camps," as well as ample funds.[28]

The challenger to the status quo was Marc Sageman, a former covert CIA officer who spent the late 1980s helping Afghan fighters against the Soviet Union.[29] Sageman then obtained a Ph.D. and became a forensic psychiatrist, specializing in the study of murderers.[30] In 2004, Sageman published *Understanding Terror Networks*,[31] in which he argued that the main threat to the United States from the global jihadist movement came not from al Qaeda and other organized terrorist groups, but small networks of like-minded

---

23. *Id.* at 77–91, 105–07.

24. LOU MICHEL & DAN HERBECK, AMERICAN TERRORIST: TIMOTHY MCVEIGH AND THE OKLAHOMA CITY BOMBING 229–34 (2001).

25. Elaine Sciolino & Eric Schmitt, *A Not Very Private Feud Over Terrorism*, N.Y. TIMES, June 8, 2008, at WK1.

26. *See* HOFFMAN, *supra* note 17, at 263–85.

27. *Id.* at 281–82. While Hoffman did recognize that al Qaeda-inspired individuals and groups also posed a threat to the United States, he nevertheless concluded that "the most salient threat . . . continues to come from al Qaeda Central." *Id.* at 288.

28. *Id.* at 284.

29. MARC SAGEMAN, UNDERSTANDING TERROR NETWORKS, at vii (2004).

30. *Id.* at viii.

31. *See id.* at vii.

friends.[32] Whereas Hoffman saw al Qaeda as having reconstituted itself into a decentralized entity still with considerable access to funds and trained members, Sageman argued that the initial U.S. military response to 9/11 had scattered the surviving al Qaeda leadership and deprived the group of its training camps, financial assets, and communication links.[33]

Hoffman and Sageman argued so vociferously because each perceived a different primary threat and, hence, a different primary response. Based on his assessment of the nature of the continuing terrorist threat to the United States, Sageman argued for more local steps, including attempts to penetrate the jihadist network through friends or family members of an identified individual aligning himself with the ideology of the global movement.[34] Hoffman, meanwhile, pushed for continued pressure (military and otherwise) on al Qaeda and international terrorist groups.

In fact, as Peter Bergen observed in 2016,[35] recent events suggested that Sageman and Hoffman were both correct in terms of assessing the severe threat level posed respectively by lone wolves and organized terror groups,[36] but perhaps both were incorrect in terms of asserting that the other expert's focus was less worthy of concern. To be sure, U.S. counterterrorism policy does not need to focus exclusively on one perceived threat while ignoring the other perceived threat. To the extent that *some* threats emanate from foreign terrorist groups in essentially lawless areas, the United States can and does respond through military action. Similarly, to the extent that there are domestic-based threats, the United States can and does respond through more traditional law enforcement techniques, including the use of electronic surveillance and undercover sting operations.[37]

---

32. *Id.* at 111–12 (arguing that friendship was an important factor in 68 percent of the jihadist cases "on whom there was adequate information").

33. *Id.* at 51–52.

34. *Id.* at 180–81.

35. PETER BERGEN, UNITED STATES OF JIHAD: INVESTIGATING AMERICA'S HOMEGROWN TERRORISTS 105-07 (2016).

36. Indeed, neither Hoffman nor Sageman took the absolutist position that the *only* true threats came from the source focused on. *See, e.g.*, HOFFMAN, *supra* note 17, at 271 (recognizing the threat from loosely networked terrorists); SAGEMAN, *supra* note 29, at 137–38 (discussing the "Central Staff cluster" of al Qaeda—i.e., bin Laden and other key members—as one of the four major clusters of the "global Salafi jihad").

37. Adam Goldman, *Domestic Terror Rises, and FBI Feels Its Limits*, N.Y. TIMES, June 5, 2019, at A1.

B. "Lone Wolf" Terrorists

The Hoffman-Sageman debate concerned the main source of terrorism following the disruption of al Qaeda and the Taliban in Afghanistan—or, more precisely, the mechanism by which radical Islamic terrorism was likely to continue to arise in the United States. (Again, it must be acknowledged that not all terrorism within the United States is perpetrated by Muslims and that there are terrorism experts who believe that white supremacist groups pose an equal, if not greater threat of domestic terrorism than do Muslim extremists.)[38]

Lone wolf terrorists pose a severe societal challenge, because they are often undetectable until they act.[39] They do not require much training, expertise, or resources.[40] A single person carrying firearms and extra ammunition can inflict devastating casualties in a short time span, as has been demonstrated on a discouragingly frequent basis:[41]

- Major Nidal Hasan, an Army psychiatrist, bought a semiautomatic pistol and several hundred rounds of ammunition, and practiced target shooting for several weeks, before opening fire on November 5, 2010, at the Fort Hood military base where he was stationed.[42] In just ten minutes, he fired over 200 shots, killing thirteen and wounding thirty others.[43]

---

38. *See, e.g.*, MIKE GERMAN, THINKING LIKE A TERRORIST 65-66 (2007).

39. *See, e.g.*, DEP'T OF HOMELAND SEC. & FED. BUREAU OF INVESTIGATION, JOINT INTELLIGENCE BULLETIN, USE OF SMALL ARMS: EXAMINING LONE SHOOTERS AND SMALL-UNIT TACTICS 2 (2011) [hereinafter USE OF SMALL ARMS] ("Attacks by lone offenders—which by definition lack co-conspirators, and therefore provide fewer opportunities for detection—may be more difficult for law enforcement and homeland security authorities to disrupt."); David Horsey, Opinion, *Despite Colorado Theater Massacre, a Discussion of Guns is off Limits*, L.A. TIMES (July 24, 2012), https://www.latimes.com/opinion/topoftheticket/la-na-tt-theater-massacre-20120724-story.html [https://perma.cc/VF84-Y2BJ] ("There was nothing that could have prevented that unless someone saw him loading his car with guns.").

40. *See* USE OF SMALL ARMS, *supra* note 39, at 2.

41. *See* GRAFF, *supra* note 1, at 573 (quoting FBI official as saying "[y]ou may not be able to shoot down an airliner with a Stinger, but you can still shoot up a mall"). To be sure, there is a question as to whether mass shootings constitute terrorism, but for current purposes, the shooters' intent to cause mass casualties should be enough to treat these incidents as ones warranting the same law enforcement focus as truck bombs and other more traditional forms of terrorism. Tung Yin, *When Is It Terrorism?*, WASH. POST, June 18, 2017, at B1.

42. Scott Huddleston, *Hasan Sought Gun with 'High Magazine Capacity,'* MYSANANTONIO.COM, Oct. 21, 2010, https://blog.mysanantonio.com/military/2010/10/hasan-sought-gun-with-high-magazine-capacity/ [https://perma.cc/4UEC-ESX4].

43. James Dao, *12 Killed, 31 Wounded in Rampage at Army Post; Officer is Suspect*, N.Y. TIMES, Nov. 6, 2009, at A1.

- Jared Loughner bought a pistol a little more than a month before engaging in a mass shooting in January 2011 at a supermarket in Tucson, Arizona, killing six people (including Chief U.S. District Judge John Roll) and injuring twelve others (including U.S. Congresswoman Gabrielle Giffords).[44]

- James Eagan Holmes bought four guns and several thousand rounds of ammunition in May 2012; two months later, he committed what was then the worst mass shooting in the United States, killing twelve and wounding fifty-eight at a movie theater.[45]

- Stephen Paddock used an arsenal of AR-15 semiautomatic rifles and other firearms to attack attendees at a music festival in Las Vegas on October 1, 2017.[46] From his suite on the thirty-second floor of the nearby Mandalay Bay Hotel, he was able to fire 1,100 rounds, killing fifty-eight and injuring over 500 in the worst mass shooting incident in the United States.[47]

- Omar Mateen stormed a nightclub in Orlando, Florida, on June 12, 2016, and used a semiautomatic rifle and a handgun to kill forty-nine people and wound fifty-eight others.[48]

- Nikolas Cruz used an AR-15 semiautomatic rifle to kill seventeen students and teachers and wound seventeen others in a Florida high school.[49]

---

44. Marc Lacey & David M. Herszenhorn, *19 Are Hit; Six Die*, N.Y. TIMES, Jan. 9, 2011, at A1.

45. *See* Jack Healy, *Theater Gunman is Spared Death in Aurora Case*, N.Y. TIMES Aug. 8, 2015, at A1.

46. C.J. Chivers & Thomas Gibbons-Neff, *Before Onslaught of Gunfire, Attacker Traced Efficient Path*, N.Y. TIMES, Oct. 3, 2017, at A1.

47. *See id.*

48. Rene Stutzman, *Pulse Gunman Was Expert Marksman, His Former Range Instructor Recalls*, ORLANDO SENTINEL, June 23, 2016, at A1.

49. Julie Turkewitz et al., *Florida Shooting Suspect Displayed Flashes of Rage and Other Warning Signs*, N.Y. TIMES, Feb. 16, 2018, at A1; Mark Berman, *Parkland Inquiries Underscore Struggle to Grapple with Massacre's Horrors*, WASH. POST, Feb. 15, 2019, at A2.

Nor are lone wolves limited to shooting their victims. Just as mass shootings occurred before 9/11, so too had there been bombing attacks, including the 1995 destruction of the Murrah Federal Building in Oklahoma City by Timothy McVeigh and Terry Nichols:[50]

- Soon after 9/11, British citizen Richard Reid boarded a transatlantic airline and tried to detonate a bomb built in his shoe.[51] Had the bomb exploded, it could very well have caused the plane to crash, but fortunately Reid was unable to light the fuse and was subsequently subdued by passengers and flight crew.[52]

- Eight years later, Nigerian citizen Umar Farouk Abdulmutallab tried to succeed where Reid had failed: instead of a shoe bomb, however, Abdulmutallab had sewn explosive material into his underwear.[53] Also unlike Reid, Abdulmutallab managed to light his improvised device; again, passengers and flight crew were able to foil the plot.[54]

- In May 2010, Faisal Shahzad attempted to car bomb Times Square in New York City; the bomb failed to explode despite being ignited.[55]

- Rezwan Ferdaus planned to attack the Capitol Building by crashing a remote-controlled model plane filled with plastic explosives.[56]

---

50. *See generally* MICHEL & HERBECK, *supra* note 24, at xi–xxi.

51. *Richard Reid Fast Facts*, CNN (Mar. 25, 2013), https://www.cnn.com/2013/03/25/us/richard-reid-fast-facts/index.html [https://perma.cc/9K9H-S92R].

52. *Id.*

53. Scott Shane, *FBI Interviews Tell of Cleric's Role in Bomb Plot*, N.Y. TIMES, Feb. 23, 2017, at A9.

54. *Id.* Because of Reid's failed attempt, the Transportation Security Agency has been requiring air travelers to remove their shoes during security screening. We are lucky that TSA did not implement similar measures after Abdulmutallab's failed effort.

55. Aaron Katersky, *Faisal Shahzad Pleads Guilty in Times Square Car Bomb Plot, Warns of More Attacks*, ABC NEWS (June 21, 2010), https://abcnews.go.com/Blotter/faisal-shahzad-pleads-guilty-times-square-car-bomb/story?id=10970094 [https://perma.cc/8UDP-FWVK].

56. Press Release, Fed. Bureau of Investigation, Man Sentenced in Boston for Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Detonation Devices to Terrorists (Nov. 1, 2012), https://archives.fbi.gov/archives/boston/press-releases/2012/man-

- Brothers Tamerlan and Dzhokar Tsarnaev were able to detonate two homemade bombs near the finish line of the Boston Marathon in April 2013, killing three and injuring nearly 300 spectators.[57]

By comparison, the 9/11 attacks—admittedly much greater in scope and casualty count—needed nineteen perpetrators, eight of whom had sufficient piloting skills to crash the jet airplanes into the Twin Towers and the Pentagon, as well as $400,000–$500,000 to fund their planning and conducting of the attack.[58] It was so complicated that pieces of the attack aroused the suspicions of various U.S. intelligence analysts before 9/11:

- CIA and FBI intelligence agents had identified Khalid al-Mihdhar, who would later help hijack Flight 77, as a suspected al Qaeda member and urged unsuccessfully in August 2001 that he be put on a watchlist.[59]

- In the summer of 2001, FBI Special Agent Kenneth Williams wrote a memo raising concerns, based on investigation of flight schools in Arizona that al Qaeda had sent members to learn to fly airplanes.[60]

- Contemporaneously with, but independently of, Special Agent Williams's investigation, the FBI office in Minneapolis detained Zacarias Moussaoui, a French national, officially for immigration violations, but in reality due to his suspicious

---

sentenced-in-boston-for-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-detonation-devices-to-terrorists [https://perma.cc/YWJ7-FX7M].

57. Jess Bidgood, *Massachusetts: Nov. 3 Trial is Set for Defendant in Marathon Killings*, N.Y. TIMES, Feb. 13, 2014, at A19.

58. THE 9/11 COMM'N REPORT, *supra* note 16, at 4, 169.

59. Due to the Department of Justice's interpretation of the Foreign Intelligence Surveillance Act, the FBI intelligence analysts believed that they could not share information about al-Mihdhar with FBI agents on the criminal investigation side, and so field agents could not be enlisted to search for him. For more on this intelligence failure, see GRAFF, *supra* note 1, at 302–04.

60. AMY B. ZEGART, SPYING BLIND: THE CIA, THE FBI, AND THE ORIGINS OF 9/11, at 160 (2007). Williams' memo was especially relevant, given an August 6, 2001 presidential daily briefing that noted rumors of an al Qaeda-planned hijacking or other attack on U.S. passenger airlines. *See* THE 9/11 COMM'N REPORT, *supra* note 16, at 260–62.

behavior at a local flight school.[61] The field office was denied permission by the Justice Department to seek a Foreign Intelligence Surveillance Act (FISA) warrant to search Moussaoui's laptop computer, which would have revealed links to al Qaeda.[62]

- Mohammed al-Qahtani, long suspected of being the intended fifth hijacker on Flight 93, was denied entry to the United States on August 3, 2001, by a skeptical U.S. immigration agent due to al-Qahtani's use of a one-way airplane ticket and his lack of money, any hotel or lodging reservations, or any contact information for anyone he knew in the country, and his aggressive demeanor.[63]

Of course, the 9/11 attacks were not stopped, and it is far from clear that they would have been stopped had any or all of the suspicions and warnings been checked out. The counterterrorism czar for the Clinton Administration, Richard Clarke, had presciently foreseen the danger that al Qaeda posed and had continuously agitated in the late 1990s for military action against it and the Taliban to disrupt the threat.[64] In hindsight, Clarke was correct, both as to the imminence and scale of the threat, and also as to the prescription, but he was ignored at the time, and it is not hard to see why; without the 9/11 attacks, there would not have been political will to engage in military action on the other side of the world.[65] The point is rather that, while both may be difficult to detect, between the 9/11 plot and lone wolf terrorism, the latter presents even greater challenges because there are fewer "moving parts."[66]

In the mass shooting lone wolf incidents, the perpetrators used legally purchased firearms.[67] Some practiced extensively or had prior weapons

---

61. *See* THE 9/11 COMM'N REPORT, *supra* note 16, at 273.

62. *See id.* at 273–76.

63. *See* KURT EICHENWALD, 500 DAYS: SECRETS AND LIES IN THE TERROR WARS 10–12 (2012).

64. *See* RICHARD A. CLARKE, AGAINST ALL ENEMIES: INSIDE AMERICA'S WAR ON TERROR 202-03 (2004).

65. *See* STEVE COLL, GHOST WARS: THE SECRET HISTORY OF THE CIA, AFGHANISTAN, AND BIN LADEN, FROM THE SOVIET INVASION TO SEPTEMBER 10, 2001, at 390–91 (2004) (noting pushback against Clarke).

66. Once detected, of course, a lone wolf should be easier to stop than an organized group.

67. Billy Kenber, *At Court-Martial, Psychiatrist Admits to Fort Hood Shootings*, WASH. POST, Aug. 7, 2013, at A3; Alex Lockie, *The Las Vegas Gunman Chose a Terrifying Vantage Point 3-5 Football Fields Away and 32 Levels High that Enabled Him to Shoot People 'Like*

training before engaging in the shooting rampage.[68] The attempted bombers obviously did not use legally obtained weapons, but constructed them from regular chemicals and other supplies.[69] Fewer does not always mean none, however, and many of the mass shooters described above did in fact give some signs of dangerousness. Orlando shooter Omar Mateen had been investigated twice by the FBI, talked to others about his desires to kill co-workers, and frequently expressed his disdain for gays and lesbians (among others).[70] Parkland shooter Nikolas Cruz posted a picture of himself with guns and, in his post, said that he planned to shoot the school that he ultimately attacked; and at least three people had warned law enforcement authorities (including the FBI) that Cruz was dangerous.[71]

Unfortunately, pointing out red flags retrospectively after a terrorism incident is not particularly difficult. Instead, the challenge is determining beforehand whether the red flags merit law enforcement action.

C. Terrorism as Asymmetric Warfare

At its heart, terrorism is a form of asymmetric warfare within Carl von Clausewitz's definition of war as the "continuation of political activity by other means"[72]—that is, the use of violence to achieve geopolitical goals. At least until the 1990s, terrorist groups generally had demands that they issued

---

Fish in a Barrel,' BUS. INSIDER (Oct. 3, 2017), http://www.businessinsider.com/stephen-paddock-las-vegas-shooting-weapons-vantage-point-room-2017-10 [https://perma.cc/6XHB-7XCQ]; *see, e.g.*, Charlotte Alter, *Orlando Shooter Bought Gun Legally, Store Owner Says*, TIME (June 14, 2016), http://time.com/4367592/orlando-shooting-gun-store-owner/ [https://perma.cc/396Z-B9U5].

68. Stutzman, *supra* note 48 (noting Omar Mateen took a firearms course in 2011 and his instructor described Mateen as "an expert marksman"). *See generally* Evan Perez et al., *Orlando Shooting: Killer's Behavior Had Long Been an Issue*, CNN (June 17, 2016), https://www.cnn.com/2016/06/17/us/orlando-shooter-omar-mateen/index.html [https://perma.cc/PP7L-RTAF] (noting Omar Mateen attempted to buy body armor before opening fire at Pulse nightclub.

69. Katersky, *supra* note 55.

70. Lizette Alvarez & Richard Pérez-Peña, *Praising Isis, Gunman Attacks Gay Nightclub*, N.Y. TIMES, June 13, 2016, at A1.

71. *Red flags: The Troubled Path of Accused Parkland Shooter Nikolas Cruz*, WASH. POST (March 10, 2018), https://www.washingtonpost.com/graphics/2018/national/timeline-parkland-shooter-nikolas-cruz/?utm_term=.9965c57512ed [https://perma.cc/VP6W-Q9G5].

72. *See* CARL VON CLAUSEWITZ, ON WAR 87 (Michael Howard & Peter Paret eds. & trans., 1984).

openly; the acts of terrorism were carried out in an effort to coerce the target government to give in to the groups' demands.[73]

Unlike traditional military conflicts, in which the armed forces of nation-states engaged in combat in accordance with the laws of war, terrorists cannot fight directly against the United States (or most other developed nations). They likely would be outnumbered and outgunned by local law enforcement as well as the military.[74] As a result, terrorists now frequently try to hide among and within the general population. For example, during the planning and preparation phase of the 9/11 attacks, the hijackers received training from mastermind Khalid Sheikh Mohammed "on Western culture and travel."[75] After training, the hijackers returned to Germany, from which they would ultimately depart for the United States.[76] While in Germany, the hijackers altered their outward behavior, their dress, and even the company they kept, so as "to avoid appearing radical."[77]

This is not to say that military forces do not conceal themselves from their enemy to avoid being attacked. The difference is that under the laws of war, military combatants may conceal their presence but not their identity from their adversaries.[78] In other words, if military combatants are detected, they are required to be readily identifiable as lawful targets or they risk losing

---

73. *See* Gary LaFree & Laura Dugan, *Research on Terrorism and Countering Terrorism*, 38 CRIME & JUST. 413, 442, 452 (2009). These two characteristics are in fact related, as the terrorism of that era was meant to draw attention to a particular cause, rather than to inflict maximum death and destruction. *Id.* at 452. *See also* HOFFMAN, *supra* note 17, at 238 (noting that right-wing terrorism in Europe in the 1970s was "based not on some pathological obsession to kill or beat up as many people as possible but rather on a deliberate policy of intimidating the general public into acceding to specific demands or pressures").

74. Experts have estimated al Qaeda's membership after 9/11 at a few hundred to a thousand. Carl Bialik, *Shadowy Figure: Al Qaeda's Size Is Hard to Measure*, WALL ST. J. (Sept. 10, 2011), https://www.wsj.com/articles/SB10001424053111903285704576560593124523206 [https://perma.cc/RJ6W-9E6E].

75. THE 9/11 COMM'N REPORT, *supra* note 16, at 157.

76. *Id.* at 167.

77. *Id.*

78. *See* Geneva Convention Relative to the Treatment of Prisoners of War art. 4, Aug. 12, 1949, 6 U.S.T 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention] (defining captured belligerents entitled to prisoner-of-war status as those readily identifiable as such); *see also* JEAN S. PICTET, INT'L COMM. OF THE RED CROSS, COMMENTARY TO THIRD GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 52 (1960) ("It is the duty of each State to take steps so that members of its armed forces can be immediately recognized as such and to see to it that they are easily distinguishable from members of the enemy armed forces or from civilians.").

prisoner of war status.[79] To the extent terrorists are seeking to claim the mantle of "freedom fighters" or other irregular combatants, they are failing to comply with this obligation. In addition, the laws of war prohibit combatants from deliberately attacking civilian targets;[80] yet, terrorists often (but not always)[81] attack "soft" targets such as civilian buildings,[82] passenger aircrafts,[83] and other venues with large gatherings of people.[84]

The primary counterterrorism challenge, therefore, is identifying the would-be terrorist. Stopping a known terrorist plot is, by contrast, much easier. On a number of occasions, government agents identified suspected terrorists and were confident enough in their ability to stop any potential plot that the agents were willing to monitor and wait rather than arrest immediately.[85] For example, after the FBI learned from Scotland Yard in 2009 that al Qaeda leadership had instructed Najibullah Zazi to attack New York subways,[86] federal agents spent weeks patiently listening to intercepted telephone calls, searching motel rooms in which he had stayed, and otherwise

---

79. Protocols Additional to the Geneva Conventions of 12 August 1949 art. 37(1)(c), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocols Additional I]. In fact, a military combatant who attacks while pretending to be a non-combatant commits the war crime of perfidy. Legal definitions of terrorism do not include elements of perfidy expressly, focusing instead on the targets of and the motivation for the attack. 18 U.S.C. § 2331 (2018).

80. Protocols Additional I, *supra* note 79, art. 51.

81. THE 9/11 COMM'N REPORT, *supra* note 16, at 190.

82. Some representative examples of targeted buildings include the World Trade Center in 1993 and 2001 and the Murrah Federal Building in Oklahoma City in 1995. *See, e.g.*, REEVE, *supra* note 22, at 6–15; MICHEL & HERBECK, *supra* note 24.

83. In addition to the four airplanes hijacked on 9/11, other terrorism plots against U.S. civilian aircraft include the attempts by Richard Reid in late 2001 and Umar Farouk Abdulmutallab in late 2009 to detonate explosives in their shoes and underwear, respectively; and a pre-9/11 plot by Ramzi Yousef (the architect of the 1993 World Trade Center bombing) to blow up eleven airplanes simultaneously. *See* REEVE, *supra* note 22, at 6–15; Shane, *supra* note 53; *Richard Reid Fast Facts*, *supra* note 51.

84. *See generally* Jack Healy & John Eligon, *Survivors Relive Horror: 'He Shoots Toward My Head,'* N.Y. TIMES, June 18, 2016, at A13 (describing mass shooting in Orlando nightclub that killed 49 people); Ken Belson et al., *Sniper Inflicts 'Total Chaos' in Las Vegas; Police Seek a Motive as Death Toll Hits 59*, N.Y. TIMES, Oct. 3, 2017, at A1 (describing mass shooting in Las Vegas that killed 58 people). On whether mass shootings should be considered terrorism, see generally Tung Yin, *Were Timothy McVeigh and the Unabomber the Only White Terrorists?: Race, Religion, and the Perception of Terrorism*, 4 ALA. CIV. RTS. & CIV. LIBERTIES. L. REV. 33 (2013).

85. *See infra* notes 86–101.

86. *British Spies Help Prevent al Qaeda-Inspired Attack on New York Subway* TELEGRAPH (Nov. 9, 2009), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/6529436/British-spies-help-prevent-al-Qaeda-inspired-attack-on-New-York-subway.html [https://perma.cc/Z2B4-C8MS].

gathering evidence of his intent.[87] At one point, the FBI asked local New York police to stop Zazi's car under the pretense of a random checkpoint, but when the ensuing search produced no explosives, Zazi was released.[88] FBI agents even interviewed him on three successive days without arresting him, before finally taking him into custody on September 19.[89]

In other instances, terrorists were not identified until after their attempted plot, but were still arrested or captured without incident.[90] Faisal Shahzad built a car bomb whose fuse he lit after parking the vehicle near Times Square in New York, but the bomb failed to detonate due to faulty construction;[91] Shahzad was apprehended a little over two days later when he tried to board a flight from New York to Pakistan.[92]

III. WARFARE AND INFORMATION

The thesis of this Article is that domestic counterterrorism operations are best conceived as a form of information operations (or information warfare) whose value lies primarily in detecting, disrupting, and confusing would-be terrorists, and secondarily in providing a basis for prosecuting those caught in the stings. To the extent warfare is about the controlled application of violent

---

87. Dina Temple-Raston, *Terrorism Case Shows Range of Investigators' Tools*, NPR, (Oct. 3, 2009), https://www.npr.org/templates/story/story.php?storyId=113453193 [https://perma.cc/CMB9-22GJ].

88. *Id.*

89. Frank James, *Afghan Man, Focus of Terror Probe, Arrested with Father and 3rd Man*, NPR (Sept. 20, 2009), https://www.npr.org/sections/thetwo-way/2009/09/afghan_man_focus_of_terror_pro.html [https://perma.cc/Z5WN-FNFZ].

90. *See infra* notes 91–92.

91. Katersky, *supra* note 55.

92. *Id.* Not all of the identified domestic terrorists in recent years were captured so easily. Brothers Tamerlan and Dzhokhar Tsarnaev were identified as suspects within three days of their attack on the 2013 Boston Marathon after they killed a local police officer, carjacked an SUV, and robbed the driver. Joe Tanfani et al., *Boston Bombing [Update]: Door-to-Door Manhunt Locks Down City*, L.A. TIMES (Apr. 19, 2013, 12:00 AM), https://www.latimes.com/nation/la-xpm-2013-apr-19-la-na-nn-boston-bombing-suspects-20130419-story.html [https://perma.cc/2HNY-ECSA]. The older brother (Tamerlan) was killed during a shootout with police when the younger brother ran over him in the carjacked SUV while escaping; over a dozen officers were injured, including one who died nearly a year later. *Id.* For the next day, while Dzhokhar Tsarnaev remained at large, federal and local law enforcement agents conducted a house-by-house search while shutting down most local commercial and public transportation. *Id.* Eventually, the seriously wounded Tsarnaev was found hiding in a boat. Pierre Thomas et al., *Boston Bomb Suspect Captured Alive in Backyard Boat*, ABC NEWS, (Apr. 19, 2013), https://abcnews.go.com/US/boston-bomb-suspect-captured-alive-backyard-boat/story?id=18994511 [https://perma.cc/TG92-X9D9].

force against enemy forces, information operations might be seen as auxiliary in nature—increasing the effectiveness of one's own attacks and degrading the enemy's attacks and defenses. Electronic surveillance, public monitoring of social media, and undercover sting operations similarly serve an auxiliary function of increasing the effectiveness of attacks (prosecution) and degrading the enemy's attacks (prevention).

Accordingly, this part of the Article provides an examination of information operations in the military context. The Department of Defense defines "information operations": "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[93]

According to the Defense Department, concepts related to information operations include electronic warfare and military deception.[94] Electronic warfare is defined as "[m]ilitary action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[95] Military deception consists of "[a]ctions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[96] Separate from electronic warfare and military deception, but also involving information and warfare, is the use of electromagnetic or sound waves to detect the presence and movement of enemy forces.

A. Code Breaking, Radar and Sonar, and Communications Jamming

For nearly the entirety of human history, success in warfare has been driven by technological advances. Archimedes conceived heat ray technology by using polished concave shields to reflect and concentrate the sun's rays on enemy ships, setting them on fire; supposedly, the invading "Roman sailors were sent into deepening panic at each new weapon deployment."[97] The ancient fire weapon known as Greek Fire, a prehistoric forerunner of modern napalm, provided Greek warriors with a nautical advantage over rival

---

93. DEP'T. OF DEF., DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 106 (2019).

94. *Id.*

95. *Id.* at 72.

96. *Id.* at 143.

97. ADRIENNE MAYOR, GREEK FIRE, POISON ARROWS AND SCORPION BOMBS: BIOLOGICAL AND CHEMICAL WARFARE IN THE ANCIENT WORLD 218 (2003).

Byzantines and Arabs and "caused enemies to 'shiver in terror' and capitulate in despair."[98] The development of gunpowder similarly provided a temporary but significant edge to those armed with guns and rifles.[99] The culmination of weapons of mass destruction—nuclear weapons—arguably ended World War II.[100]

Warfare in the twentieth century saw the rise of significance of something besides the increase in destructive capacity: control of information.[101] Modern code breaking, electromagnetic detection systems (like radar), and electronic countermeasures (to jam enemy systems) are aimed at gaining and controlling information relevant to the military theater.[102] While the technological advancement in weapons systems was important to the Allied victory in World War II, so too was the information advantage that the Allies enjoyed, as discussed below.[103]

1. Code Breaking and Deception

Encryption of military messages was known as far back as the time of Julius Caesar, if not earlier, with simple substitution ciphers.[104] For example, one could replace every letter in the plaintext (the original message) with the corresponding letter, say, three spaces forward in the alphabet turns the sentence "the quick brown fox jumps over the lazy dog" into apparent gibberish: "wkh txlfn eurzq ira mxosv wkh odcb grj." By encrypting messages, military personnel could communicate with one another across distance without needing to worry about the possibility of interception of the

98. *Id.* at 242.

99. *See id.* at 17, 213 (noting the inventing of gunpowder in China and its use in weapons).

100. *See* THOMAS C. REED & DANNY B. STILLMAN, THE NUCLEAR EXPRESS: A POLITICAL HISTORY OF THE BOMB AND ITS PROLIFERATION 23–25 (2009).

101. *See* Loren Thompson, *Electronic Warfare: The Part of the F-35 Fighter Story You Haven't Heard*, FORBES (Jan. 9, 2018), https://www.forbes.com/sites/lorenthompson/2018/01/09/electronic-warfare-the-part-of-the-f-35-fighter-story-you-havent-heard/#5eaf2b2968cc [https://perma.cc/TPX9-W5S3] ("Modern warfare is waged largely on the electromagnetic spectrum.").

102. *See id.*

103. Neal Stephenson's techno-thriller novel *Cryptonomicon* makes the point during a theoretical discussion between two characters about the different aspects of warfare represented by the Greek gods Ares and Athena, with the former being "mindless, raging violence," and the latter being "intelligence [and c]unning." NEAL STEPHENSON, CRYPTONOMICON 804–08 (First Perennial ed., HarperCollins 2000) (1999). The U.S. won World War II and Germany lost, one character asserts, because "the Germans worshipped Ares and we worshipped Athena." *Id.* at 807–08.

104. SIMON SINGH, THE CODE BOOK 9 (1999).

messages by the enemy; that is, even if the enemy were to capture the messenger, the message itself would be unreadable.[105]

From that point on, cryptanalysts (i.e., code breakers) and cryptographers have been engaged in a cryptology arms race.[106] The simple substitution cipher noted above is quite vulnerable to a codebreaker familiar with English, since "wkh" is repeated, and there are relatively few common three letter words in the English language. Moreover, sufficiently lengthy ciphertext can be subjected to letter frequency analysis; *e* is the most common letter in plain English, showing up approximately 12% of the time, so any letter in ciphertext that appears around that frequency is almost certainly *e*.[107]

Code breaking played a significant role in the Allied victory in World War II.[108] At the time, German forces used a fiendishly complex machine known as Enigma to encrypt their military communications,[109] while Japanese forces used a similar machine that U.S. cryptanalysts called "PURPLE."[110] Once the Allies were able to decrypt intercepted transmissions in a timely fashion, they had access to Axis attack plans, ship and troop movements, and other military intelligence.[111] For example, during World War II, the United States won the pivotal battle of Midway in part because the Navy was able to prepare for the attack, having had advance warning due to an intercepted and partially decoded Japanese transmission.[112] A year later, American cryptanalysts deciphered a Japanese naval communication informing troops that Admiral Yamamoto, the architect of the Pearl Harbor attack, would be touring Japanese-held Solomon Islands and New Guinea.[113] Armed with Yamamoto's flight plan, U.S. forces ambushed and shot down his plane.[114]

Being privy to a wartime adversary's battle plans is thus incredibly valuable. So too is the ability to manipulate and deceive an adversary through deliberately leaked misinformation, and to assess and evaluate the effectiveness of the deception by reading the enemy's communications. In 1942, American and British forces were preparing to attack German forces in French North Africa; because "[t]here was no way to hide the large buildup

105. *Id.* at 6.
106. *See generally id.* at 6–7.
107. *See id.* at 17.
108. *Id.* at 186–87.
109. *Id.* at 127.
110. DAVID KAHN, THE CODEBREAKERS: THE STORY OF SECRET WRITING 1 (1967).
111. WALTER LORD, INCREDIBLE VICTORY: THE BATTLE OF MIDWAY 20 (1967).
112. *See id.* at 18–23; KAHN, *supra* note 110, at 567–69.
113. STEPHEN BUDIANSKY, BATTLE OF WITS: THE COMPLETE STORY OF CODEBREAKING IN WORLD WAR II, at 319 (2000).
114. *Id.* at 319; KAHN, *supra* note 110, at 595–601.

of naval forces at Gibraltar," the Allies needed to deceive Germany from the actual target.[115] They did so by leaking false attack plans through newspapers and other sources, and then were able to read decoded German communications identifying Malta, Libya, or Italy as the likely targets[116]—which was confirmation that the deception had worked. As one commentator has put it, "[T]he synergy of signals intelligence and deception paid off so richly."[117]

In today's world, military deception need not rely on such crude methods as leaking false attack plans or "building fake airfields to mislead . . . bombers."[118] Instead, assuming a sufficient level of technological advancement on the part of the enemy, it is possible to change or corrupt the enemy's data: "Alter the proper ones and zeroes, and as far as the enemy knows, we've got another bomber wing."[119] Although such a cyberattack does not do physical damage to enemy assets, it can affect the enemy's military strategy, misdirecting or possibly even deterring an attack.[120]

2. *Locating Targets Through Radar or Sonar*

The interception and decryption of military communications with ship movements or aircraft itineraries is not the only way to locate enemy forces. In some instances, such as the interception and decryption of the Japanese battle plan to invade Midway Island, signals intelligence may provide only the adversary's strategic intention, or perhaps tactical plans, but not the exact location of warships.[121] Over the course of a day and a half, the U.S. Navy found Japanese ships through conventional visual spotting by scout aircraft.[122] Electromagnetic detection systems such as radar provided a means to detect enemy aircraft location and velocity beyond the line of sight, or when darkness or weather cut down on visual perception.[123]

---

115. BUDIANSKY, *supra* note 113, at 274.

116. *Id.* at 274–75.

117. *Id.* at 275 ("The landings at Morocco and Algiers the next day achieved total strategic surprise.").

118. DEP'T OF THE AIR FORCE, INFORMATION WARFARE 9 (1997).

119. *Id.* at 11.

120. *See* Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, *in* ELECTRONIC WARFARE: DEFENSE, SECURITY, AND STRATEGY SERIES 166, 169–70 (Adam T. Elsworth ed. 2010).

121. LORD, *supra* note 111, at 20.

122. *Id.* at 65–67.

123. MERRILL I. SKOLNIK, RADAR HANDBOOK 1-2 (1970).

The earliest radar systems worked by sending a radio wave outward, where it would meet a target, and some of the energy would be bounced back toward the radar system.[124] Because the speed of the radio wave was known to the radar system, the distance to the target could be determined based on the delay between the sending of the radio wave and the reception of the bounce back signal.[125] Additional information about the target, such as altitude and radial velocity, could be determined through trigonometry and physics.[126] Sonar is a similar system that uses the propagation of sound waves in water to detect the presence of other objects, including vessels or natural obstacles.[127] The radar or sonar systems described above engage in what is known as active detection because they use energy (or sound) actively.[128]

In contrast to active detection systems are passive detection systems, which do not propagate electromagnetic or sound waves of their own but, instead, rely upon other transmitters in the vicinity.[129] Much in the same way that distant astronomical objects can be detected even when not visible due to their gravitational impact on their neighbors, passive detectors infer the presence of an object due to the impact on known transmissions such as television, radio, and cellular signals.[130] Another system sometimes known as passive coherent location or electronic support system operates by "exploit[ing] active emissions from the target."[131] In other words, these are

---

124. *Id.*

125. Tung Yin, *Game of Drones: Defending Against Drone Terrorism*, 2 TEX. A&M L. REV. 635, 651 (2015).

126. *Id.*

127. *Sonar*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/sonar [https://perma.cc/HX56-8B6Y].

128. *See* Brian H. Maranda, *Passive Sonar*, in HANDBOOK OF SIGNAL PROCESSING IN ACOUSTICS 1757 (Havelock et al. eds., 2008).

129. *See* Antonio Moccia et al., BISTATIC RADAR: EMERGING TECHNOLOGY RADAR: 1 (Mikhail Cherniakov ed., 2008) ("Bistatic radar operates with separated transmitting and receiving antennas."); Ian Steadman, *'Passive' Radar Could Render Stealth Planes Obsolete*, WIRED (Oct. 1, 2012), http://www.wired.co.uk/article/radar-detects-stealth-aircraft [https://perma.cc/4U5W-AKP6] ("Passive radar detects radiation signals emitted by other sources—be they radio broadcasts or mobile phone networks—and analyses distortions to figure out where objects are located.").

130. Steadman, *supra* note 129 ("[T]he detector system looks at a host of signals floating in the atmosphere already (like aforementioned radio and mobile phone signals) and looks for how they're blocked or altered by having to pass through or around objects.").

131. Bill Sweetman, *New Radars, IRST Strengthen Stealth-Detection Claims: Counterstealth Technologies Near Service Worldwide*, AVIATIONWEEK NETWORK (Mar. 16, 2015), http://aviationweek.com/technology/new-radars-irst-strengthen-stealth-detection-claims [https://perma.cc/9PM2-76NG]; Ollie Holt, *Technology Survey: A Sampling of RWRs and ESM Systems*, J. ELECTRONIC DEF., June 2015, at 39 ("As the ES system scans the environment, radar

radar detectors—and by detecting unknown or unexpected radars, passive coherent location systems can alert to the presence of hostile aircraft or ships.[132]

Passive detection systems avoid a major downside of active detection ones, which is that the active radiation or sound emissions of the latter can draw the attention of enemy attackers.[133] In essence, when a radar is turned on and begins sending radio waves outward, it is like turning on a flashlight in a dark room; the person using the flashlight can see, but someone else in the room now knows where the person is located. Active detection systems are thus vulnerable to counterattack. During the first Gulf War, Coalition Forces unleashed British ALARM and U.S. HARM anti-radiation missiles to zero in on and destroy Iraqi radar air defense systems.[134] As one commentator notes, "Nowadays, the existing radar surveillance systems of the Air Defense system have very little chance of surviving the first phase of a military conflict, not to mention surviving its whole duration, which was proved by the few recent ones."[135]

The practical dilemma that radar users face is that there is a tradeoff between active versus passive detection; the former offers more precision and more useful information than the latter but also increases the risk of counter detection.[136]

3. *Interfering with Enemy Communications (Jamming)*

In addition to manipulating or deceiving the enemy, or locating the enemy's position, electronic warfare can take the form of directly attacking

---

signals are detected (pulsed or continuous wave [CW]) and the parameters of the signals are measured."); Maranda, *supra* note 128, at 1757 ("The difference between passive and active sonar is that a passive sonar system emits no signals; instead, its purpose is to detect the acoustic signals emanating from external sources.").

132. *See* Sweetman, *supra* note 131.

133. *See* MARY ROACH, GRUNT: THE CURIOUS SCIENCE OF HUMANS AT WAR 253 (2016).

134. *See* Stanislaw Czeszejko, *Anti-Radiation Missiles vs. Radars*, 59 INT'L J. ELECTRONICS & TELECOMM. 285, 285, 287 (2013); *see also* JOURNAL OF ELEC. DEF., INT'L ELECTRONIC COUNTERMEASURES HANDBOOK 152 (Michael Puttré et al. eds., Horizon House Pub. 2004) ("The missile was designed to be able to beat a SAM to the punch by taking out its guidance radar.").

135. Czeszejko, *supra* note 134, at 291.

136. *The Last Ship*, (TNT television broadcast 2014). *The Last Ship*, a serialized thriller drama on TNT, frequently depicts naval warfare (either surface versus submarine, or surface versus surface) in which the combatant ships have to be careful about using active radar or sonar, because doing so will give away their location.

the enemy's own information gathering, communications, or both.[137] By sending "unwanted signal energy into the receivers in the [enemy's] communication system," the attacker can "cause the receivers to demodulate the signal from the jammer as opposed to the communication transmitter."[138] In other words, the jammer floods the target's receivers with its nonsense signals, thereby overriding the authentic signals, possibly even destroying the equipment.[139] Successful jamming does not deceive or manipulate the enemy. Rather, it interferes with the enemy's use of information, causing radar-guided weaponry to lose their lock on their targets or blocking enemy forces from communicating with one another.[140]

4. Limits on Information Operations

We should be careful not to overestimate the value of intelligence. As John Keegan notes, "Knowledge, the conventional wisdom has it, is power, but knowledge cannot destroy or deflect or damage or even defy an offensive initiative by an enemy unless possession of knowledge is also allied to objective force."[141] As Keegan points out, Polish cryptanalysts were the first ones to decipher the German Enigma code, but their intelligence success did not save Poland from Germany.[142] The United States did better at Midway but, even with advance knowledge of the Japanese attack plans, could have lost the battle.[143] Keegan's observation about the limits of intelligence is important, but of less concern in the context of counterterrorism, where the primary challenge is detecting the terrorist plots and identifying the terrorists; stopping a known threat is considerably easier.

---

137. *See* RICHARD A. POISEL, INTRODUCTION TO COMMUNICATION ELECTRONIC WARFARE SYSTEMS 189 (2002); *see also* DEP'T OF ARMY, *Electronic Warfare in Operations*, *in* ELECTRONIC WARFARE: DEFENSE, SECURITY, AND STRATEGY SERIES 36, 46–47 (Adam T. Elsworth ed. 2010) ("*Electronic jamming* is the deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum.").

138. POISEL, *supra* note 137, at 189.

139. *See* Wilson, *supra* note 120, at 169.

140. *See id.*

141. JOHN KEEGAN, INTELLIGENCE IN WAR: KNOWLEDGE OF THE ENEMY FROM NAPOLEON TO AL-QAEDA 348 (2003).

142. *Id.*

143. *Id.* at 220 ("A little less intuition by McClusky of Bombing 6, a little more intellectual resolution by Admiral Nagumo and it would have been the carriers of TF 16 and 17, not those of Yamamoto's Mobile Force, which would have been left burning and bereft in the bright waters of the Pacific on 4 June 1942.").

IV. POST-9/11 DOMESTIC COUNTERTERRORISM POLICY: TACTICS AND EXAMPLES

The immediate American response to 9/11 consisted of a nationwide sweep of hundreds of noncitizen males from Middle Eastern countries into immigration detention,[144] along with the rounding up of a small number of men as material witnesses.[145] In November 2001, the Bush Administration commenced military attacks in Afghanistan against al Qaeda and Taliban targets pursuant to the congressional Authorization to Use Military Force.[146] Apart from a tiny number of notable exceptions, however, the military response remained distinct from domestic counterterrorism operations.[147] Thus, neither the Bush nor Obama Administrations resorted to drone strikes or indefinite military detention within the United States.[148]

The only person prosecuted in federal court in direct connection to 9/11 was Zacarias Moussaoui,[149] a French national who had been detained since August 2001 on immigration charges.[150] Over the course of nearly six years

---

144. Press Release, Dep't of Justice, Department of Justice Inspector General Issues Report on Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Terrorist Attacks (June 2, 2003).

145. HUM. RIGHTS. WATCH, WITNESS TO ABUSE: HUMANS RIGHTS ABUSES UNDER THE MATERIAL WITNESS LAW SINCE SEPTEMBER 11, at 15 (2005).

146. Authorization for Use of Military Force, Pub. L. No. 107-40, § 1–2, 115 Stat. 224 (2001).

147. The exceptions involved an American citizen captured in Afghanistan (John Walker Lindh), an American citizen arrested at O'Hare International Airport in Chicago (Jose Padilla), and a lawful resident (Ali Saleh al-Marri). United States v. Lindh, 212 F. Supp. 2d 541, 545–47 (E.D. Va. 2002); Padilla v. Hanft, 423 F.3d 386, 388 (4th Cir. 2005); al-Marri v. Pucciarelli, 534 F.3d 213, 217 (4th Cir. 2008) (Motz, J., concurring). Conversely, Padilla and al-Marri were both arrested at first and subsequently detained in military brigs under the jurisdiction of the Defense Department. Tung Yin, *Coercion and Terrorism Prosecutions in the Shadow of Military Detention*, 2006 BYU L. REV. 1255, 1264–68 (2006).

148. *See* Yin, *supra* note 147, at 1290 n.191. (describing the differences between domestic law enforcement and military action).

149. *Timeline: The Case Against Zacarias Moussaoui*, NPR (May 3, 2006), https://www.npr.org/templates/story/story.php?storyId=5243788 [https://perma.cc/6VBS-LVLP]; *see* United States v. Moussaoui, 591 F.3d 263, 266 (4th Cir. 2010). For an archived copy of the indictment, see Indictment, *United States v. Moussaoui*, 292 F. Supp. 2d 480 (E.D. Va. 2003) (No. 01-455-A).

150. *Moussaoui*, 591 F.3d at 266; THE 9/11 COMM'N REPORT, *supra* note 16, at 273–76. Moussaoui had drawn the attention of the FBI field office in Minneapolis because an instructor at the local flight school where he was taking flight lessons found his behavior and intentions suspicious. OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS (2004) https://oig.justice.gov/special/s0606/chapter4.htm [https://perma.cc/YQD8-68DR]. The FBI

of criminal litigation, which included several trips from the district court to the court of appeals and back,[151] Moussaoui eventually pleaded guilty to terrorism-related conspiracy charges and proceeded to the penalty phase of the trial.[152] Although he was eligible for the death penalty, he ultimately received a life sentence.[153]

The bulk of persons charged with terrorism-related federal crimes (i.e., those found in Chapter 113B of the U.S. Code) from September 12, 2001, to early 2004 were indicted for providing material support to designated terrorist organizations in violation of 18 U.S.C. § 2339A or § 2339B.[154] Some of the more notable early cases included a group of Yemeni-Americans from a suburb of Buffalo who pleaded guilty to providing material support to al Qaeda when they traveled to Afghanistan in summer 2001 to participate in the

---

agent who investigated found it further suspicious that Moussaoui had $30,000 in a bank account with no visible means of income. THE 9/11 COMM'N REPORT, *supra* note 16, at 273. Fearing that Moussaoui was planning to hijack a plane, the FBI agent and local immigration agents decided to take Moussaoui into immigration custody for overstaying his visa. *Id.*

151. *See* United States v. Moussaoui, 382 F.3d 453, 458–62 (4th Cir. 2004).

152. *Moussaoui*, 591 F.3d at 266.

153. Timothy Dwyer, *One Juror Between Terrorist and Death: Moussaoui Foreman Recalls Frustration*, WASH. POST, May 12, 2006, at A1.

154. *See* Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 20 (2005). 18 U.S.C. § 2339B (2018) states in its current form:

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

§ 2339B(a)(1). The second sentence in the statutory provision was added in 2004. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6003(c), 118 Stat. 3638 (2004). This clarified the *mens rea* element so as to enable the government to prosecute persons who provided material support to organizations that they knew engaged in terrorism, even if they did not know that the State Department had designated the recipients as terrorist organizations. *See* Intelligence Reform and Terrorism Prevention Act § 6603(c).

terrorist group's training camps,[155] and a different group from Portland who tried to enter Afghanistan after 9/11 and made it as far as Pakistan.[156]

The material support prosecutions were not free of controversy. One line of criticism was that "material support" was defined so broadly by statute that it included cash, so that donating to a group such as Hamas (which the State Department has designated an FTO) would run afoul of the statute, even if the donor had sincerely intended for the cash to be used to provide food, clothing, or social services.[157] The central reason for such a broad prohibition is that money is fungible, so even if the donor specified that his or her donation should be used *only* for humanitarian purposes, such donation would allow Hamas to divert money that otherwise have used for those humanitarian purposes into additional terrorism funds.[158] Under this same reasoning, however, al Qaeda could justify its attacks on American civilians on the grounds that, as taxpayers, those civilians were funding U.S. military operations—which, in al Qaeda's view, were unjust.[159]

Another line of criticism of the material support prohibition was that it went so far as to squelch legitimate free expression. In one notable case, a nonprofit organization wanted to teach a designated terrorist group to use nonviolent avenues of international law to achieve its goals but feared that doing so would constitute providing "expert advice" (which was one category of material support).[160] The Supreme Court eventually ruled that § 2339B did not violate the First Amendment because it did not prohibit independent speech, only coordinated activity with designated terrorist groups.[161]

Since then, U.S. domestic counterterrorism investigations have involved a variety of often complementary tactics, including (1) monitoring of publicly

---

155. *See* United States v. Goba, 240 F. Supp. 2d 242, 244–45 (W.D.N.Y. 2003). For a sympathetic account of the defendants with more background, see generally DINA TEMPLE-RASTON, THE JIHAD NEXT DOOR: THE LACKAWANNA SIX AND ROUGH JUSTICE IN THE AGE OF TERROR (2007).

156. *See* STEVEN T. WAX, KAFKA COMES TO AMERICA: FIGHTING FOR JUSTICE IN THE WAR ON TERROR: A PUBLIC DEFENDER'S INSIDE ACCOUNT 90–96 (2008) (providing background on the Portland defendants from the perspective of the then-Federal Public Defender for the District of Oregon).

157. *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 13–14 (2010) (quoting 18 U.S.C. § 2339B(a)(1) (2006) (current version at 18 U.S.C. § 2339B (2018)).

158. *Id.* at 31 (quoting Declaration of Kenneth R. McKune, App. 128, ¶ 9).

159. Ward Churchill, at the time the chair of the Ethnic Studies department at the University of Colorado, made this very argument in an online essay (later expanded into a book) posted on September 12, 2001. *See* Ward Churchill, *"Some People Push Back": On the Justice of Roosting Chickens*, DARK NIGHT FIELD NOTES, Sept. 12, 2001.

160. *See Holder*, 561 U.S. at 14–15.

161. *Id.* at 38.

available social media postings; (2) following up on tips; (3) collecting e-mail and other communications; and (4) stinging targets.[162]

A. Monitoring Publicly Available Social Media Postings

1. Chat Rooms, Social Media Sites, and Other Internet Pages

One of the primary sources of information for counterterrorism agents has been the public Internet postings of the suspects.[163] Vague statements of violence posted on one's Facebook page without specific targets or details might not provide probable cause to arrest a person,[164] but they may warrant further attention from law enforcement authorities. For example, in 2010, when Antonio Martinez, a twenty-year-old with a theft conviction in his past and an adoptee of a radical interpretation of Islam, posted statements on Facebook that "glorified jihad . . . and warned . . . 'the sword is cummin [and] the reign of oppression is about 2 cease inshallah,'"[165] a government informant brought the postings to the attention of the FBI.[166] The subsequent investigation, which was conducted largely by the informant, led to Martinez's arrest for plotting to blow up a military recruiting center with a car bomb.[167] Nor was Martinez unique in this regard; a few examples of others who publicly exposed their violent intentions include the following:

- Colleen LaRose, known as Jihad Jane, who "used MySpace, YouTube, and e-mails to express her desire to become a martyr for the Islamic cause,"[168] and was convicted of terrorism-related charges in 2010;[169]

---

162. *See* BERGEN, *supra* note 35, at 217 (noting impact of informant and community tips and other traditional law enforcement in counterterrorism).

163. *See infra* notes 163–72.

164. *Cf.* Brandenburg v. Ohio, 395 U.S. 444, 449 (1969) (holding "incitement to imminent lawless action" to be outside First Amendment protection); Virginia v. Black, 538 U.S. 343, 359–60 (2003) (holding that a State may punish a "[t]rue threat" that "communicate[s] a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals").

165. Tricia Bishop, *Guilty Plea in Bomb Plot: Martinez Admits Guilt in Bomb Plot*, BALT. SUN, Jan. 26, 2012, at A1.

166. *Id.*

167. *Id.*

168. *See* JEFFREY D. SIMON, LONE WOLF TERRORISM: UNDERSTANDING THE GROWING THREAT 202 (2013).

169. *See* John Shiffman, *U.S. Woman Known as Jihad Jane Sentenced to 10 Years in Plot*, REUTERS (Jan. 6, 2014), https://www.reuters.com/article/us-usa-jihadjane-

- Joseph Stack, who posted a greater than 3,000-word screed against the Internal Revenue Service, the 2000 dot-com collapse, and more, on his business website, and then crashed his small plane into the building containing the Austin, Texas, office of the IRS in December 2010;[170]

- Richard Poplawski, who "frequented a neo-Nazi chat room on the Internet and was responsible for killing three police officers . . . in April 2009";[171]

- Samir Khan, who authored *Inshallah Shaheed* (A martyr, God willing), a blog in which he "praised attacks by al-Qaeda," "yearned for martyrdom," and continually called for jihad before being killed in the same drone strike that killed Anwar al-Aulaki;[172]

- Zachary Chesser, who "became a star in the small, self-referential world of English-speaking jihadist propaganda," and who was later convicted of providing material support to a designated foreign terrorist organization.[173]

Or a person might go into a public chat room on the Internet and seek to make contact with like-minded (i.e., those seeking to engage in terrorism) individuals for collaboration, support, or instruction.[174] This would be an example of what Eugene Volokh has termed "crime-facilitating speech," and

---

idUSBREA050PC20140106 [https://perma.cc/8AM7-7ENE]; *see also* Susan Candiotti, *Jihad Jane, American who Lived on Main Street*, CNN (Mar. 10, 2010), https://www.cnn.com/2010/CRIME/03/10/jihad.jane.profile/index.html [https://perma.cc/87L5-ZL9L].

170. Richard Fausset, *Suicide Pilot Hid His Anger*, L.A. TIMES, Feb. 20, 2010, at AA1.

171. SIMON, *supra* note 168, at 202.

172. *See* BERGEN, *supra* note 35, at 138–40, 210.

173. *Id.* at 148, 157.

174. MARC SAGEMAN, LEADERLESS JIHAD: TERROR NETWORKS IN THE TWENTY-FIRST CENTURY 115–16 (2008); *see* Cora Currier, *Undercover FBI Agents Swarm the Internet Seeking Contact with Terrorists*, INTERCEPT (Jan. 31, 2017), https://theintercept.com/2017/01/31/undercover-fbi-agents-swarm-the-internet-seeking-contact-with-terrorists/ [https://perma.cc/D32Q-SJ4N] ("Because terror groups have made effective use of online networks to spread propaganda and to connect with troubled individuals, the virtual realm has become a significant counterterrorism theater for the FBI.").

it poses societal dangers above and beyond mere advocacy of criminal conduct because it may be "information that teaches people how to violate the law, and how to do so with less risk of punishment . . . ."[175] As a result, the FBI has taken to monitoring chat rooms that it suspects may provide users with the means to connect with terrorist groups.[176]

One might wonder why lone wolf terrorists in particular (and terrorists in general) would use social media given the possibility, if not likelihood, of government monitoring of public sites. One answer is that, just as many criminal suspects are induced to confess their crimes to police interrogators out of a need to talk despite having been given *Miranda* warnings,[177] potential terrorists feel a need to talk about what they are planning.[178] Another answer is that social media serves more than a modern venue for venting but, in fact, radicalizes potential terrorists through interaction with like-minded participants.[179]

To be sure, social media monitoring will not guarantee detection of all potential domestic terrorists. Some will actively avoid public social media or express their violent intentions offline (such as in a diary).[180] And of course, the government cannot monitor *every* chat room discussion and social media postings *all* of the time.

---

175. Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1107 (2005).

176. *See, e.g.*, RONALD KESSLER, THE TERRORIST WATCH: INSIDE THE DESPERATE RACE TO STOP THE NEXT ATTACK 173 (2007); SIMON, *supra* note 168, at 205; Currier, *supra* note 174; Michael S. Schmidt et al., *Suspects in U.S. Who Don't Travel to Syria Are Even Harder to Investigate*, N.Y. TIMES, Nov. 20, 2015, at A17; *Terrorists in the Chat Room?*, WIRED (Oct. 12, 2004), https://www.wired.com/2004/10/terrorists-in-the-chat-room/ [https://perma.cc/E2FA-4JDS] (discussing government plan to fund a study on surveillance of chat rooms).

177. *See* Mark Bowden, *The Dark Art of Interrogation*, ATLANTIC MONTHLY, Oct. 2003, at 51, 54, 72. *But see* DAVID SIMON, HOMICIDE: A YEAR ON THE KILLING STREETS 207 (Owl Books 2006) (1991) ("[T]he majority of those who acknowledge their complicity in a killing must be baited by detectives with something more tempting than penitence.").

178. SIMON, *supra* note 168, at 201 ("Lone wolves like to talk a lot. . . . Even loners have a basic human need for contact with others.").

179. *See* SAGEMAN, *supra* note 174, at 115–16; *cf.* CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA 114–15 (2017) (noting that social media can intensify partisanship).

180. *See e.g.*, Amir Vera, *A Teen Wrote About Plans to Shoot Up His Washington High School. But His Grandmother Found His Journal*, CNN (Feb. 16, 2018), https://www.cnn.com/2018/02/15/us/grandmother-foils-school-shooting-plan-everett-trnd/index.html [https://perma.cc/PH3L-MPFX].

2. Privacy Concerns

In general, law enforcement officials have the same right as any member of the public to read or observe nonprivate social media posts or chat room discussions.[181] As far as the Fourth Amendment is concerned, there is no reasonable expectation of privacy over something that is knowingly exposed to the public, and if there is no reasonable expectation of privacy to violate, then there cannot be a search.[182]

Nevertheless, it would be understandable if a person were to feel uneasy knowing or believing that government agents are reading his or her blog postings or keeping tabs on chat room discussions.[183] Indeed, such a person might react by self-chilling himself or herself as if the government had prohibited such speech.[184] During the height of the Vietnam War, antiwar protesters learned that U.S. Army intelligence agents had been attending and writing reports about their public meetings.[185] They argued that "[t]he 'deterrent effect' on First Amendment rights by government oversight marks an unconstitutional intrusion,"[186] but the Supreme Court concluded otherwise in *Laird v. Tatum*, holding that the plaintiffs had failed to show an actual or threatened injury; they showed only a speculative one.[187]

Subsequently, in response to the Church Committee's investigation, led by Senator Frank Church, of alleged civil rights abuses before and during the

---

181. *See* Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool*, CNN (Aug. 30, 2012), https://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html [https://perma.cc/MA6Y-3CXY].

182. *See* Katz v. United States, 389 U.S. 347, 351 (1967). Some particular types of trespass also constitute a search wholly independently of the expectation of privacy analysis. *See* United States. v. Jones, 565 U.S. 400, 402, 413 (2012) (holding that unconsented placement of GPS tracking device on suspect's car constituted a search); Florida v. Jardines, 569 U.S. 1, 11–12 (2013) (holding that bringing a drug-sniffing dog to a suspect's front porch constituted a search even though a previous case held that the dog's sniff did not violate a reasonable expectation of privacy).

183. One might even call it "stalking."

184. For example, not long after 9/11, I began researching an article contrasting moral arguments against capital punishment with the willingness to live under the nuclear deterrence umbrella. I did find myself wondering if some government agent had been tracking my library borrowing, which consisted of several books on nuclear weapons and nuclear warfare theory.

185. *See* Laird v. Tatum, 408 U.S. 1, 6 (1972).

186. *Id.* at 25 (Douglas, J., dissenting) (citing Lamont v. Postmaster General, 381 U.S. 301, 307 (1965)); *see also Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.").

187. *Laird*, 408 U.S. at 13–14 ("Allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm.") (citing United Pub. Workers of Am. (C.I.O.) v. Mitchell, 330 U.S. 75, 89 (1947)).

Vietnam War,[188] Congress enacted the Privacy Act of 1974, which, among other things, prohibited government agencies from keeping records about "how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."[189]

Observing an individual's public writings (or chats) is not the same as maintaining a record of that person's writings (or chats). The particular threat the Privacy Act seemed to be aimed at was that posed by former FBI Director J. Edgar Hoover, who kept quasi-personal files on "enemies of the United States"—a group that included leaders of the American Civil Liberties Union, Helen Keller, Dr. Martin Luther King, gays, and more.[190] These files contained, among other things, information "on the places where these people gathered, the publications they read, and the political groups they joined."[191] Armed with such information, Hoover was able to impose his will throughout Washington, D.C., including over the occupants of the White House.[192]

Admittedly, there is still a concern that the government might go beyond observing and monitoring public social media posts and, instead, maintain its own records of those observations. The social media posts could be copied and stored on government servers so that they would be available indefinitely, even if the originals were deleted. Congress has recognized that retention of material about or by an individual may present a distinct civil liberties threat separate from the initial gathering of that material. The Foreign Intelligence Surveillance Act, for example, permits U.S. officials to conduct electronic surveillance for foreign intelligence purposes without the need to demonstrate probable cause to believe that a crime has been or is being committed.[193] Among the material that FISA authorizes collection of are "call detail records"—phone numbers and time and duration of calls, but not their

---

188. *See* SELECT COMMITTEE TO STUDY GOV'T OPERATIONS, S. REP. NO. 94-755, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES 7–10 (1976).

189. 5 U.S.C. § 552a(e)(7) (2014), *held unconstitutional as not severable by* Texas v. United States, 340 F. Supp. 3d 579 (N.D. Tex. 2018).

190. TIM WEINER, ENEMIES: A HISTORY OF THE FBI 61–62, 176 (2012); *The History of the FBI's Secret 'Enemies' List*, NPR (Feb. 14, 2002), https://www.npr.org/2012/02/14/146862081/the-history-of-the-fbis-secret-enemies-list [https://perma.cc/2373-74F2].

191. WEINER, *supra* note 190, at 23–24.

192. *See id.* at 232.

193. 50 U.S.C. § 1805 (2012). The required standard is, instead, probable cause to believe that the target is an agent of a foreign power. *Id.*

contents[194]—but with the additional proviso that judicial orders approving such collection must include "minimization procedures" that require the government to destroy promptly any "call detail records produced under the order that the Government determines are not foreign intelligence information."[195]

B. Following up on Tips

Sometimes counterterrorism officials learn about potential suspects through third-party tips. Those tips might come from a teen or adult child's parents or other relatives, or peers, teachers, or neighbors. In the best case scenario, government agents will act on the tip, conducting any necessary investigation to corroborate the tip.[196]

One tip that resulted in an arrest before the suspect could carry out a potential attack occurred in Washington in early 2018, when a grandmother called the police after reading a number of disturbing journal entries by her grandson along with finding a semiautomatic rifle.[197] Local law enforcement officials arrested the grandson on charges of attempted murder, with the diary and the rifle providing enough probable cause for the arrest.[198] In many other instances, the tip brought someone to the attention of government agents for further investigation.[199]

Informants are, of course, an important source of law enforcement information, so much so that the Supreme Court has, over decades, issued

---

194. 50 U.S.C. § 1861(k)(3) (2012).

195. 50 U.S.C. § 1861(c)(2)(F)(vii) (2012). Such call details are generally not protected under the Fourth Amendment. *See* Smith v. Maryland, 442 U.S. 735, 735 (1979). FISA sets a limit on how long those call details can be retained.

196. *Cf.* Illinois v. Gates, 462 U.S. 213, 237–38 (1983) (noting that tips, "particularly when supplemented by independent police investigation, frequently contribute to the solution of otherwise 'perfect crimes'").

197. Vera, *supra* note 180. The diary entries included the following: "I need to make this shooting/bombing infamous. I need to get the biggest fatality number I possibly can. I need to make this count. . . . I'm learning from past shooters/bombers mistakes, so I don't make the same ones" and "I'm preparing myself for the school shooting. I can't wait. My aim has gotten much more accurate. . . I can't wait to walk into that class and blow all those [expletive] away." *Id.*; Eric Wilkinson et al., *Everett 911 Call: He's Planning on Having a Mass Shooting at One of the High Schools*, K5 NEWS (Feb. 15, 2018), https://www.king5.com/article/news/crime/everett-911-call-hes-planning-on-having-a-mass-shooting-at-one-of-the-high-schools/281-518703506 [https://perma.cc/NE6X-B69X].

198. Vera, *supra* note 180.

199. *See, e.g.*, United States v. Mohamud, 843 F.3d 420, 424 (9th Cir. 2016) ("And when [the parents] could not reach Mohamud, they called the FBI and asked an agent to stop their son from leaving the country.").

multiple Fourth Amendment decisions that govern the use of tips in the probable cause analysis.[200] A major concern of the probable cause doctrine has been whether a tipster has sufficient reliability to warrant a conclusion that the target of the tip is likely to be involved in criminal activity. Thus, in *Spinelli v. United States*, the Court suppressed evidence obtained pursuant to a search warrant that was based on an informant's tip because the warrant application failed to provide any basis to evaluate the informant's reliability and credibility.[201] *Spinelli*'s strict requirement of minimum thresholds of informant reliability and credibility was overruled in *Illinois v. Gates*, which adopted a more flexible "totality of the circumstances" analysis;[202] however, informant reliability and credibility remained relevant considerations,[203] especially with an anonymous tip, where there is no way to hold the tipster "responsible if her allegations turn out to be fabricated . . . ."[204]

Tips about potential terrorists are no less vulnerable to these concerns. After 9/11, various government agencies have frequently exhorted the public that "if you see something, say something."[205] Fifteen years after 9/11, with such "say something" notices still appearing in New York transit (among other places), the police department was getting around 100 tips per day about suspicious looking packages, yet according to the *Washington Post*, "[I]t's not clear that the tip line has ever prevented an attack," and "[s]ome people even use the hot line to call in phony bomb threats."[206]

Still, wholly apart from the likely greater reliability and credibility of an identified tipster who knows the suspect personally, one might also keep in mind the caveat from *Florida v. J.L.*, where the Court—in a unanimous opinion—noted, "We do not say, for example, that a report of a person

---

200. *Gates*, 462 U.S. 213; Spinelli v. United States, 393 U.S. 410 (1969); Aguilar v. Texas, 378 U.S. 108 (1964); Nathanson v. United States, 290 U.S. 41 (1933); *see also* Florida v. J.L., 529 U.S. 266, 270–71 (2000) (analyzing role of an anonymous tip in terms of providing reasonable suspicion for a *Terry* stop).

201. *Spinelli*, 393 U.S. at 412–13.

202. *Gates*, 462 U.S. at 230.

203. *Id.* at 233.

204. *J.L.*, 529 U.S. at 270; *see also id.* at 272 (noting the potential for an anonymous tip to "enable any person seeking to harass another to set in motion an intrusive, embarrassing police search of the targeted person simply by placing an anonymous call falsely reporting the target[]").

205. *See, e.g.*, *If You See Something, Say Something*, U.S. DEP. HOMELAND SEC., www.dhs.gov/see-something-say-something [https://perma.cc/UM2V-QWKS]. *See generally* Willian Neuman, *In Response to M.T.A.'s 'Say Something' Ads, a Glimpse of Modern Fears*, N.Y. TIMES, Jan. 7, 2008, at B1.

206. Hanson O'Haver, *Does 'See Something, Say Something' Make Us Safer?*, WASH. POST, Sept. 25, 2016, at B04.

carrying a bomb need bear the indicia of reliability we demand for a report of a person carrying a firearm before the police can constitutionally conduct a frisk."[207]

C. Collecting E-Mail and Other Communications

In addition to checking up on publicly available social media postings and chat room discussions and following up on tips, counterterrorism agents have conducted secret surveillance of nonpublic communications such as e-mails.[208] Unlike the monitoring of social media postings and chat room discussions, such surveillance implicates privacy rights because the communications are not knowingly exposed to the public.[209]

Of course, if law enforcement agents have sufficient probable cause that a suspect has committed or is committing a crime, they may be able to obtain a judicial order to intercept the suspect's oral, wire, or electronic communications.[210] Alternatively, if federal agents have sufficient probable cause to believe that a target is an agent of foreign power, they may be able to obtain a foreign intelligence surveillance warrant to intercept that target's oral, wire, or electronic communications.[211] These are essentially the electronic equivalent of physical search warrants.

Not all of the government's electronic surveillance was directed at specific individuals.[212] Since 9/11, several broad programs collectively known as Stellar Wind have scooped up massive amounts of telephone and e-mail information for data mining purposes.[213] In the abstract, such surveillance sounds like a reasonable step. When the *New York Times* revealed the existence of a government program to engage in warrantless surveillance of

---

207. *J.L.*, 529 U.S. at 273–74.

208. Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, INTERCEPT (Nov. 30, 2017), https://theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ [https://perma.cc/6W4B-VW64] ("The government intercepts Americans' emails and phone calls in vast quantities using this spying law and stores them in databases for years.").

209. *Cf.* Katz v. United States, 389 U.S. 347, 351, 361 (1967).

210. *See* 18 U.S.C. § 2518 (2018).

211. 50 U.S.C. § 1805 (2012).

212. *See* James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012), https://www.wired.com/2012/03/ff-nsadatacenter/ [https://perma.cc/HT95-6VE9].

213. *See id.*; ERIC LICHTBLAU, BUSH'S LAW: THE REMAKING OF AMERICAN JUSTICE 153 (2008).

calls involving some U.S. citizens,[214] President Bush defended the program on the grounds that it was necessary to detect and listen in on calls from al Qaeda operatives on one end to persons in the United States on the other end "[t]o save American lives."[215]

In a famous incident in 2003, two key members of the Bush Justice Department (acting Attorney General James Comey and Assistant Attorney General Jack Goldsmith) became aware of the details of one of these programs and nearly precipitated a revolt when they determined that the program—known as the Terrorist Surveillance Program (TSP)—was unlawful in its existing form due to the lack of any judicial oversight.[216] The program required the Attorney General's approval for reauthorization.[217] Comey persuaded Attorney General John Ashcroft that the TSP needed to be changed to address the legal problems, but Ashcroft fell severely ill with pancreatitis, leaving Comey as the acting Attorney General.[218] When Comey refused to reauthorize it, President Bush sent Chief of Staff Andrew Card and White House Counsel Alberto Gonzales to Ashcroft's hospital to get Ashcroft to overrule Comey.[219] What resulted then was a frantic race to see who would get to Ashcroft first, Comey and Goldsmith, or Card and Gonzales.[220] Comey and Goldsmith won the race and re-briefed Ashcroft, and then when Card and Gonzales arrived, Ashcroft stated that he did not think the TSP was legal in its current form, "But that doesn't matter, because I'm not the attorney general.[221] There (pointing at Comey) is the attorney general."[222] Two days later, when summoned by the White House to discuss the TSP, Comey—along

---

214. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

215. President George W. Bush, The President's News Conference (Dec. 19, 2005), *in* 41 WEEKLY COMP. PRESS DOC. 1885; *see also* President George W. Bush, Remarks to the Military Officers Association of America (Sept. 5, 2006), *in* 42 WEEKLY COMP. PRESS DOC. 1563 ("If Al Qaida is calling somebody in America, we need to know why in order to stop attacks.").

216. *See* JACK GOLDSMITH, THE TERROR PRESIDENCY 182 (2007) (alluding to the issue but unable to provide details, presumably due to pre-publication clearance requirements); GRAFF, *supra* note 1, at 484 (quoting Goldsmith as "conclud[ing] that the surveillance program 'was the biggest legal mess I'd seen in my life,'" and noting Goldsmith's disclosure of the program to Comey).

217. Colleen Shalby, *Comey, Mueller and the Showdown at John Ashcroft's Hospital Bed*, L.A. TIMES (May 17, 2017), https://www.latimes.com/politics/la-na-pol-mueller-comey-ashcroft-domestic-surveillance-20170517-story.html [https://perma.cc/99BY-9WG9].

218. GRAFF, *supra* note 1, at 485.

219. *Id.* at 487.

220. *Id.* at 487–88.

221. *Id.* at 488.

222. *Id.*

with FBI Director Robert Mueller, Goldsmith, Ashcroft, and several other high-ranking Justice Department lawyers—was prepared to resign rather than reauthorize the program without necessary changes.[223] President Bush agreed to let Comey implement those changes.[224] The Obama Administration continued a version of this program, which was leaked to *The Guardian* in 2013 by a government contractor named Edward Snowden.[225] The Obama Administration defended the surveillance program as "a critical tool in protecting the nation from terrorist threats."[226]

D. Stinging Targets

Almost three years after the 9/11 attacks, the Bush Administration added undercover sting operations to its counterterrorism toolkit.[227] To be sure, the line between the earlier § 2339B cases and the subsequent sting cases is not a bright one, considering that some of the earlier cases also involved government informants and many of the initial sting cases resulted in § 2339B charges.[228] Beginning in 2004, however, the degree of interaction between informants (or even undercover agents) and targets shifted from the passive end of the spectrum toward the active one.[229]

1. From Early Material Support Stings to Later Fake Bomb Stings

Thus, in 2004, when thirty-four-year-old Yassin Aref and forty-nine-year-old Mohammed M. Hossain were arrested for money laundering, conspiring to provide material support to terrorism, and making a false statement to a federal agent,[230] the government's confidential informant acted as more than a mere conduit of overheard conversations. Instead, the

---

223. *Id.* at 489–492.

224. *Id.* at 492.

225. Glenn Greenwald, *US Orders Phone Firm to Hand over Data on Millions of Calls*, GUARDIAN, June 6, 2013, at 1.

226. Dan Roberts & Spencer Ackerman, *U.S. Admits Surveillance of Calls Has Gone on for Years*, GUARDIAN, June 7, 2013, at 4.

227. *See* Jon Sherman, *'A Person Otherwise Innocent': Policing Entrapment in Preventative, Undercover Counterterrorism Investigations*, 11 U. PA. J. CONST. L. 1475, 1477–78 (2009).

228. *See* CTR. ON LAW & SEC., N.Y.U. SCH. OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001–SEPTEMBER 11, 2011, at 26 (2011), https://www.lawandsecurity.org/wp-content/uploads/2011/09/TTRC-Ten-Year-Issue.pdf [https://perma.cc/ZE95-TYH6].

229. *See* Sherman, *supra* note 227, at 1475–78.

230. Criminal Complaint, United States v. Aref, No. 04-M-330-DRH, 2007 WL 603508 (N.D.N.Y. Feb. 22, 2007).

informant, who faced prosecution on unrelated charges as well as removal proceedings by Immigration and Customs Enforcement,[231] engaged in actions without which the defendants could never have completed any of the objects of the conspiracy.[232] According to the government, Hossain and the informant agreed to a scheme to sell a portable surface to air missile (SAM) for $50,000, with the proceeds to be laundered through Hossain's pizzeria.[233] Aref became involved as a witness to the agreement.[234]

While Hossain willingly discussed violent jihad with the informant (though Hossain stated that "now was not the time for" it),[235] it was the informant who proposed the SAM-money laundering scheme.[236] Hossain was ripe for the proposal, as he was in need of money, having previously asked the informant for a financial loan,[237] but was primarily reactive rather than proactive. At trial, Hossain raised an entrapment defense unsuccessfully, and on appeal, the Second Circuit affirmed with the briefest of reasoning: "The government's evidence of predisposition sufficed [to defeat the entrapment defense] because it showed 'the accused's ready response to the inducement' to commit the crime."[238]

Aref and Hossain were not the first terrorism defendants ever to be caught through a sting,[239] but they did help usher in the post-9/11 use of such operations at an increasing level in terms of frequency as well as aggressiveness. One critic of terrorism sting operations observed in 2013 that "federal prosecutors announce arrests from terrorism stings at a rate of about one every sixty days, suggesting either that there are a lot of ineffective terrorists in the United States, or that the FBI has become effective at creating the very enemy it is hunting."[240]

---

231. *Id.* ¶ 5.

232. *See id.* ¶ 3.

233. *Id.* ¶¶ 11.

234. *Id.* ¶¶ 7–11.

235. *Id.* ¶¶ 7–8.

236. *Id.* ¶¶ 9, 11.

237. *Id.* ¶ 8.

238. *See* United States v. Aref, 285 F. App'x 784, 791 (2d Cir. 2008) (citing United States v. Salerno, 66 F.3d 544, 547 (2d Cir. 1995)).

239. In *The Terror Factory*, Trevor Aaronson identifies Imran Mandhai as the first target of the "aggressive terrorism sting operations . . . that the FBI would replicate over the next decade." TREVOR AARONSON, THE TERROR FACTORY: INSIDE THE FBI'S MANUFACTURED WAR ON TERRORISM 65 (2013). Though convicted in 2002 via guilty plea, Mandhai's criminal conduct—conspiracy to bomb local electrical transformers in Florida based on the work of two FBI informants—occurred before 9/11. *See* United States v. Mandhai, 375 F.3d 1243, 1245–47 (11th Cir. 2004).

240. AARONSON, *supra* note 239, at 34.

V. COUNTERTERRORISM AS INFORMATION OPERATIONS

If we think of domestic terrorism as asymmetric armed conflict and counterterrorism as our military response, then we can map the various aspects of information operations into their law enforcement analogues. Recall that information operations are aimed at achieving three strategic goals: (1) determining enemy plans (code breaking of intercepted communications); (2) locating enemy forces (radar, sonar); and (3) disrupting enemy information gathering (jamming, deception). Domestic counterterrorism operations are aimed at similar goals of (1) identifying potential terrorist attacks and potential terrorists; (2) determining whether potential terrorists intend to carry out attacks; and (3) disrupting those potential attacks and capturing those potential terrorists.

A. Detecting and Identifying the Enemy

In conventional warfare, the enemy must be detected and identified before it can be attacked. Detection is primarily an exercise in spotting—whether visually or through some other means such as radar or sonar—potential military vehicles or personnel before they might attack, and identification is an exercise in ascertaining whether those vehicles or personnel are indeed hostile combatants. Unfortunately, conventional warfare provides a limited analogy to counterterrorism. This is true because conventional warfare is governed by the laws of war, which, among other things, require combatants to wear uniforms (or distinctive signs and to carry arms openly) when fighting.[241] This requirement ensures that combatants can be distinguished from civilians, who cannot be lawfully targeted for attack.[242]

Terrorists, on the other hand, typically blend in even when they are carrying out their attacks.[243] The 9/11 hijackers were dressed like ordinary passengers and indeed were coached by mastermind Khalid Sheikh Mohammed to blend in with Americans.[244] The perpetrators of the other two

---

241. *See* Geneva Convention, *supra* note 78; OFF. OF THE GEN. COUNSEL, U.S. DEP'T OF DEF., LAW OF WAR MANUAL § 5.5.8 (2016) ("Combatants have certain obligations to distinguish themselves that include, but are not limited to, those times when they conduct attacks.").

242. Toni Pfanner, *Military Uniforms and the Law of War*, 86 INT'L REV. RED CROSS 93, 94 (2004).

243. Jim McKay, *The Changing Face of Terror in the U.S.*, EMERGENCY MGMT. (Feb. 7, 2011), https://www.govtech.com/em/safety/Face-Terror-US-Home-Grown.html [https://perma.cc/BDF2-D5Z5].

244. THE 9/11 COMM'N REPORT, *supra* note 16, at 167.

post-9/11 airline attacks—"shoe bomber" Richard Reid and "underwear bomber" Umar Farouk Abdulmutallab—similarly passed themselves off as regular passengers.[245] In fact, one of the only terrorists who wore a uniform during his attack was the Fort Hood shooter, Nidal Hasan;[246] however, in this instance, the uniform helped conceal his deadly intentions, because he was attacking the military base at which he had been stationed just prior to his anticipated deployment to Afghanistan.[247]

Hence, there is an important difference between terrorism and guerilla warfare. The guerilla fighter conceals himself among the civilian population so as to avoid being attacked, but wears a uniform or otherwise displays a distinctive sign while engaging in actual hostilities.[248] True, the guerilla fighter is detectable for only brief periods of time and on his own timetable, advantages that seem to run afoul of the general laws of war. Thus, when Protocol I to the Geneva Convention was adopted in 1977, granting prisoner of war status to guerilla fighters, the United States signed the treaty, but subsequently, President Reagan refused to ratify it due to concerns that it "grant[ed] guerillas a legal status that is often superior to that accorded to regular forces."[249]

By eschewing any distinguishing clothing or fixed signs, the terrorist goes one step beyond the guerilla fighter. Both are difficult to detect because they hide among the general population when dormant, but vigilant counterinsurgency military personnel can at least identify guerilla fighters when they attack—and not merely because they are attacking but because, at that moment, they are identifiable as combatants due to uniforms or fixed signs.[250] This means that the counterterrorism agent's challenge is an order of

---

245. *See* David Ariosto & Deborah Feyerick, *Christmas Day Bomber Sentenced to Life in Prison*, CNN (Feb. 17, 2012), https://www.cnn.com/2012/02/16/justice/michigan-underwear-bomber-sentencing/index.html [https://perma.cc/JSZ5-R376]; *see also Richard Reid Fast Facts*, *supra* note 51.

246. Philip Sherwell & Nick Allen, *Fort Hood Shooting: Inside Story of How Massacre on Military Base Happened*, THE TELEGRAPH (Nov. 7, 2009), https://www.telegraph.co.uk/news/worldnews/northamerica/usa/6521578/Fort-Hood-shooting-inside-story-of-how-massacre-on-military-base-happened.html [https://perma.cc/9SK6-78UB].

247. Helen Pidd & Ewen MacAskill, *Fort Hood Gunman Shouted 'Allahu Akbar' as He Opened Fire*, GUARDIAN, Nov. 6, 2009, at 17.

248. *See* Pfanner, *supra* note 242, at 94.

249. Message from the President of the United States Transmitting the Protocol II Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, S. Treaty Doc. No. 100-2, at IX (Jan. 29, 1987).

250. To use a science-fiction pop culture analogy, it's as if the guerilla fighter has cloaking technology but has to de-cloak to attack, just like the Romulan warship in the *Star Trek* episode

magnitude more difficult than the soldier's because the counterterrorism agent must generally identify the enemy by divining their intentions through observation of statements and actions.

1. Passive Detection

As discussed earlier, passive detection systems work by analyzing the disruption of known transmissions by an interfering object (i.e., the target).[251] Passive detection thus requires an understanding or expectation of what the background transmissions would look like in the absence of any temporary disruption.[252] Fixed physical transmitters such as television and radio broadcast stations and cellular towers provide a clear basis for ascertaining such background transmissions.[253] The analogical equivalent of passive detection in the counterterrorism context would be the disruption to the local community caused by noticeable and concerning behavior by a community member. Perhaps the member has recently begun showing signs of radicalization or expressing thoughts of violence. Or perhaps the person moved recently and alarmed the local community due to his radicalism.

In 2006, a man named Farouk al-Aziz began showing up at mosques in southern California, attempting to blend in with the other Muslims.[254] Soon, al-Aziz began talking about *jihad* and martyrdom, and asking if there were others who were similarly interested.[255] One community member told the Los Angeles chapter of the Council on American-Islamic Relations (CAIR) about al-Aziz; the CAIR in turn reported al-Aziz to the FBI as a possible terrorist.[256] As it turned out, al-Aziz was a false identity assumed by FBI informant Craig Monteilh, whose alarming behavior was, he claimed, the product of aggressive coaching by his government handlers.[257]

Admittedly, there are limits to this analogy. The human rhythms of a local community are a far cry from electromagnetic transmissions. A community

---

"Balance of Terror," whereas the terrorist can attack while cloaked. *See Star Trek: Balance of Terror*, (NBC television broadcast Dec. 15, 1966).

251. *See* Steadman, *supra* note 129.

252. *Id.*

253. *Id.*

254. *See* Paul Harris, *The Ex-FBI Informant with a Change of Heart: "There is No Real Hunt. It's Fixed."* GUARDIAN (Mar. 20, 2012), https://www.theguardian.com/world/2012/mar/20/fbi-informant [https://perma.cc/9XXU-837E]; *see also* AARONSON, *supra* note 239, at 106.

255. Harris, *supra* note 254.

256. AARONSON, *supra* note 239, at 106.

257. *Id.*; Harris, *supra* note 254.

may have its own distinct ethnic, or racial, or religious character,[258] but such character is still more mutable than fixed electromagnetic transmissions. In the absence of de jure segregation (which is, of course, unlawful), communities are not legally bound to remain fixed by ethnicity, race, or culture. For example, Baldwin Hills, a southern California community described as "the heart of L.A.'s black community," in recent years has seen its African-American population decline as its Latino population increases, forcing the local city councilperson to adapt, as well as to face the possibility of being the last African-American representative for that district.[259]

There are thus several lessons to draw from the limits of the analogy to passive detection. First is the importance of good relationships between counterterrorism authorities and the relevant communities expected to provide the background for passive detection. Even if the community character is sufficiently distinctive and cohesive so as to register the disturbance by a potential terrorist in its midst, there is a separate question of whether a counterterrorism agent would be able to detect that disturbance, much in the same way that a passive detector must be sensitive enough to detect electromagnetic interference. The agent would need to have a sufficiently detailed understanding of the neighborhood to be able to detect such disturbances directly or, more likely, have some relationship with community members such that the latter would feel comfortable reporting their concerns.

This cooperative relationship between law enforcement and community is one of the desired outcomes of so-called community policing. Although there is not a settled definition of community policing, James Forman Jr. has described it as "an organizational strategy for running a [police] department,"[260] thus encompassing a variety of tactics that police departments have used in an effort to develop stronger relationships with local communities.[261] Other scholars have defined community policing by the types

258. *See* Tung Yin, *Is "Diversity" Diverse Enough?*, 21 ASIAN AM. L.J. 89, 120–23 (2014).

259. Angel Jennings, *Reaching Out: In the Heart of L.A.'s Black Community, a Councilman Must Win Over a Fast-Growing Latino Community*, L.A. TIMES, Jan. 24, 2016, at B1.

260. James Forman, Jr., *Community Policing and Youth as Assets*, 95 J. CRIM. L. & CRIMINOLOGY 1, 7 (2004).

261. *Id.* (citing Tracey Meares and Dan Kahan for their discussions of "neighborhood prayer vigils, gang loitering ordinances, and 'order maintenance' strategies" as examples of community policing).

of collaborative activities that police officers engage in with community members.[262]

Notwithstanding its intuitive appeal as a counterterrorism tool, community policing has limitations. Since 9/11, the federal government has largely assumed the primary counterterrorism role, with the FBI ranking counterterrorism as its top priority.[263] Yet, the sheer size of a typical federal law enforcement agency's jurisdiction makes it difficult to develop the same kind of community relationship that a local law enforcement agency can. The FBI has approximately 13,500 special agents spread across fifty-six divisions in the entire United States;[264] New York City has nearly three times as many law enforcement officers responsible for policing only the city limits.[265] Local law enforcement officers are more involved in the local communities and therefore have greater opportunities to engage in community policing, particularly given their responsibility to investigate or prevent a variety of common street crimes.[266]

Perhaps in response to the fact that local police have a comparative advantage in community policing, the FBI has embarked in the last decade or so on a number of Joint Terrorism Task Forces (JTTFs), in which local police officers are assigned to work with federal agents to investigate and prevent acts of terrorism.[267] Such JTTFs merge the resources and intelligence assets

---

262. *See* Tracey L. Meares, *Praying for Community Policing*, 90 CAL. L. REV. 1593, 1594–95 (2002); Dan M. Kahan, *Reciprocity, Collective Action, and Community Policing*, 90 CAL. L. REV. 1513, 1513 (2002).

263. *See, e.g.*, Rebecca Davis O'Brien, *A Former Teacher Returns to Lead FBI's NYC Office*, WALL ST. J., Mar. 7, 2015, at A13; *FBI Portland History*, https://www.fbi.gov/history/field-office-histories/portland [https://perma.cc/6KPZ-9Y3K] ("The attacks of September 11 immediately made preventing terrorist attacks the top priority of the FBI and the Portland Division"); *cf.* GRAFF, *supra* note 1, at 20, 23–25 (noting that the FBI has long been engaged in counterterrorism, with the notable post-9/11 shift being an expansion into global counterterrorism).

264. GRAFF, *supra* note 1, at 521.

265. *Id.* This is not to say that federal officials are unable to develop community relationships; *see, e.g.*, Allan Brettman, *Fire at Corvallis Mosque that Portland Bomb Plot Suspect Attended Causes Little Physical Damage, Big Symbolic Wound*, OR. LIVE (Nov. 29, 2010), https://www.oregonlive.com/pacific-northwest-news/2010/11/fire_at_corvallis_mosque_that_portland_bomb_plot_suspect_attended_causes_little_physical_damage_big.html [https://perma.cc/J4AZ-NWFB] (noting that the FBI special agent in charge and the acting U.S. Attorney "not only visited the scene of [an anti-Muslim arson] but also delivered a message of support and tolerance to the Islamic center's leaders and members").

266. *See* Tung Yin, *Joint Terrorism Task Forces as a Window into the Security vs. Civil Liberties Debate*, 13 FLA. COASTAL L. REV. 1, 4–5 (2011).

267. *See, e.g.*, *id.* at 3.

of federal agents with the regional expertise of the local police;[268] over 100 American cities have entered into JTTFs with the FBI.[269] But JTTFs are not without downsides. The local law enforcement officers are subsumed within the task force as federal actors, which can place them in a difficult position if the JTTF requires them to take actions that satisfy federal law but violate state law—which can happen if the state happens to provide a greater level of protection for civil liberties than the U.S. Constitution and federal law do.[270] In 2011, when the city of Portland, Oregon, debated rejoining the JTTF (from which it had withdrawn in 2005 over concerns about the participating Portland officers' inability to share everything they learned with the mayor due to the latter's lack of top secret security clearance), the local chapter of the American Civil Liberties Union argued that the JTTF could force Portland police officers to violate a state law prohibiting law enforcement officers from collecting or maintaining "information about the political, religious or social views, associations or activities" of anyone absent "reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct."[271] Because of the Supremacy Clause, federal agents might not be obligated to comport with this state law and could take the JTTF in a direction that would violate the law.[272] Ultimately, the city decided to rejoin the JTTF on an as-needed basis—a compromise that seemed to allow city councilmembers on either side of the debate to believe that they had achieved their goals.[273] Notably, the mayor explained that his willingness to drop his prior opposition to rejoining the JTTF stemmed from the change in White House administration (from President Bush to President Obama).[274] If, on the other hand, local government officials distrust (or outright oppose) the current White House, then it is unlikely that a city with concerns such as those that Portland had in 2005–2011 would be willing to rejoin a JTTF—thereby depriving federal counterterrorism officials of the expertise of local law enforcement agencies.[275]

---

268. *Id.* at 4–5.

269. *Id.* at 3.

270. *See id.* at 20–21.

271. *Id.* at 18–20 (citing OR. REV. STAT. ANN. § 181A.250 (2017)).

272. *Id.* at 21.

273. *Id.* at 22.

274. *Id.* at 19 (quoting then-Mayor Sam Adams). Another motivating factor besides the change in Presidency was a highly publicized undercover sting operation in Portland the previous year, in which FBI agents arrested a young man for plotting to detonate a car bomb at the city's annual Christmas tree-lighting ceremony. *Id.* at 18.

275. There are numerous examples of local municipalities that have refused to cooperate with the Trump Administration due to disagreement with its policies, including the various

A corollary to the need to maintain strong relationships with relevant communities is the importance of not focusing on only a few communities as passive detectors while ignoring other ones from which terrorists might also emerge. The obvious reason is that ignoring relevant communities is akin to shutting off passive detectors facing certain directions. For example, the Government Accountability Office has reported that between September 12, 2001, and December 31, 2016, domestic terrorist incidents perpetrated by "radical Islamist" attackers killed 119 persons, while those perpetrated by "far right extremists" killed 106 persons.[276] Former FBI Special Agent Mike German, who specialized in infiltrating white supremacist groups, has argued that the United States has focused far too little attention on domestic right wing terrorist groups due to the overemphasis on the Muslim community.[277] This is not a matter of community policing in all neighborhoods in an effort to show that law enforcement authorities are not bigots or racists (though there is something to be said for imposing burdens across the board, as opposed to singling out a discrete minority group; abusive policing is less likely to be tolerated when it is conducted on a widespread basis).[278] It is an attempt to detect potential terrorism in all communities.

Additionally, focusing only on a subset of communities—or a single community, such as American Muslims—even with seemingly benign interactions such as community policing or relationship building can backfire. Saher Aziz has criticized the use of community policing in Muslim communities for counterterrorism purposes, primarily on the grounds that it is not true community policing but rather a degenerate version that has co-opted local law enforcement into supporting the federal government's

---

localities that have designated themselves as so-called sanctuary cities for undocumented aliens. *See, e.g.*, Liz Robbins, *Even in a 'Sanctuary City,' Immigrants Risk Being Deported*, N.Y. TIMES, Feb. 28, 2018, at A21; *see also* Veena Dubal, *The Demise of Community Policing? The Impact of Post-9/11 Federal Surveillance Programs on Local Law Enforcement*, 19 ASIAN AM. L.J. 35, 38 (2012) (arguing that local law enforcement must remain accountable to their constituents rather than support federal counterterrorism policies at odds with local values).

276. U.S. GOV'T ACCOUNTABILITY OFF., COUNTERING VIOLENT EXTREMISM: ACTIONS NEEDED TO DEFINE STRATEGY AND ASSESS PROGRESS OF FEDERAL EFFORTS 3 (2017). This report has drawn criticism as misleadingly equating the toll of radical Islamist terror with that of far-right extremists by beginning the period of assessment the day after 9/11, thus seeming to ignore al Qaeda's 2977 victims. However, the point of the study was not to downplay the threat posed by radical Islamists, but rather to highlight that posed by another group in light of counterterrorism steps taken since 9/11.

277. *See* Mike German, Opinion, *What We Don't Get About the Far Right*, CNN (Nov. 20, 2018), https://www.cnn.com/2018/11/20/opinions/what-we-dont-get-about-far-right-violence-german/index.html [https://perma.cc/2YNP-7RMS].

278. *See* RANDALL KENNEDY, RACE, CRIME AND THE LAW 160–61 (1997).

aggressive and adversarial approach.[279] According to Professor Aziz, community policing in the Muslim community—as currently practiced—cannot succeed because it forces the victims of civil rights abuses to cooperate with their abusers.[280] Community policing in this context ends up leveraging members of the Muslim community into spying on their neighbors and friends.[281] Amna Akbar is similarly skeptical of community policing in the counterterrorism context, contending that the end result is to "provid[e] police with greater power and discretion over marginalized communities."[282] It is merely an observation that policing resources—including community outreach efforts—should be expended in some general proportion to the scope of the threat that the community may be able to assist in preventing.[283]

The concerns that Professors Aziz and Akbar raise about the actual effect of community policing and counterterrorism cannot be dismissed. The concerns go to both the efficacy as well as the morality of the government's practices. Singling out the Muslim community alone for community policing and relationship building in the name of counterterrorism cannot help but create the false impression that only Muslims are terrorists.[284] That false impression in turn can bias law enforcement, counterterrorism agents, and the public toward immediately suspecting the Muslim community whenever there is an apparent act of terrorism, which in turn can reinforce investigative efforts on that particular community.[285] The problem is exacerbated by the fact that the media and government have often been quicker to label alleged perpetrators of mass killings as "terrorists" when they are Muslims (or of Arab descent) than when they are not.[286] And perhaps not surprisingly, an empirical study by Tom Tyler, Stephen Schulhofer, and Aziz Huq of Muslim communities in parts of New York City concluded that the perception of fairness (i.e., procedural justice) of how counterterrorism policies were carried out was positively correlated with willingness to cooperate and to

279. *See* Aziz, *supra* note 11, at 156–57.

280. *Id.* at 152.

281. *Id.* at 186–87.

282. Amna Akbar, *National Security's Broken Windows*, 62 UCLA L. REV. 834, 845 (2015).

283. *See generally* DAVID SCHANZER ET AL., TRIANGLE CTR. ON TERRORISM & HOMELAND SEC., THE CHALLENGE AND PROMISE OF USING COMMUNITY POLICING STRATEGIES TO PREVENT VIOLENT EXTREMISM, at i–iv (2016) (noting that communities respond to policing differently).

284. *See* Yin, *supra* note 84, at 59.

285. *See id.* at 61.

286. *See id.* at 69 (comparing media labeling of analogously situated Muslim and non-Muslim mass shooters and bombers).

report suspected terrorists, while the perception of having been discriminated against was negatively correlated with such willingness.[287] What is remarkable about this study is that it determined that the positive and negative effects of perception were better able to predict willingness to cooperate with authorities than the traditional deterrence-based rational expectations analysis.[288] A more recent study corroborated the findings of the Tyler study, with various respondents reporting perceptions of being singled out for unequal scrutiny.[289]

2. *Passive Coherent Location (and Electronic Surveillance)*

Passive coherent location, which relies on detection of active signals emitted by the target,[290] can be analogized to reading social media and other forms of public communications as well as electronic surveillance of the contents of potential targets' e-mails and phone conversations. It can also be analogized to monitoring lawful activities that nevertheless might be precursors of potential terrorism, such as buying quantities of materials consistent with bomb making as opposed to legitimate uses.

These forms of detection are passive because the counterterrorism agents are simply reading or listening to what the surveillance target is broadcasting or doing without taking any actions that would be observable or noticeable by the target. (Note that it is technologically possible to track the IP addresses—and hence domains—of visitors to particular websites,[291] so reading blog posts might not perfectly analogous to passive coherent location. Still, government agents who are monitoring public social media and other communications can take steps to mask their domains by using virtual private networks or taking other steps to anonymize their Internet presence).

For the purposes of the analogy, it does not matter that some communications (such as e-mails and phone conversations) are not intended for public consumption, as opposed to social media posts, published writings, or public interviews; the same may well be true of the electronic signals and

---

287. Tom R. Tyler et al., *Legitimacy and Deterrence Effects in Counterterrorism Policing: A Study of Muslim Americans*, 44 L. & SOC'Y REV. 365, 368–69 (2010).

288. *Id.*

289. SCHANZER ET AL., *supra* note 283, at 19–20.

290. *See* Steadman, *supra* note 129.

291. *See* Adam Tanner, *Here are Some Companies Who Unmask Anonymous Web Visitors (And Why They Do It)*, FORBES (July 1, 2013), https://www.forbes.com/sites/adamtanner/2013/07/01/heres-some-companies-who-unmask-anonymous-web-visitors-and-why-they-do-it/#4465b59f4115 [https://perma.cc/6QHA-3XUB].

other information picked up by passive detectors in information warfare. Of course, the private nature of a communication is relevant from a legal standpoint, for it would mean that the speaker or writer likely had a reasonable expectation of privacy; thus, interception of the communication would constitute a search for Fourth Amendment purposes.[292] But in this context, that just means certain types of passive detection would require advance judicial approval. The distinction between passive and active detection is based not on legal requirements but on technological capabilities.

This sort of passive detection has the advantage of drawing information directly from the suspected enemy target, especially where it consists of interception of electronic transmissions. Reading social media postings by suspected terrorists crosses over as an analogy from passive detection to interception of enemy communications, but still counts as a tactic aimed at detecting and identifying terrorists.

As with passive detection, military use of passive coherent location has limitations as an analogy to counterterrorism. During war time—at least, in traditional nation-state armed conflicts—active signals themselves may be an indication of potential enemy activity, particularly where the opposing sides have territorial integrity such that the enemy can be expected to attack from certain directions.[293] Domestic counterterrorism does not fit neatly within this paradigm; and thus, passive coherent location in such circumstances would entail the interception of vast amounts of signals from potential hostiles as well as nonhostiles.

When it comes to interception of enemy or adversary military communications, the U.S. government need not worry about the requirements and prohibitions of the Fourth Amendment;[294] all enemy communications are fair game for interception.[295] Left to its own devices during wartime, the government would intercept and attempt to read any communications potentially from the enemy. If anything were to keep the government from realizing this goal, it would be the sheer volume of messages and the

---

292. *See* Katz v. United States, 389 U.S. 347, 353 (1967). Wiretapping of phone lines or electronic surveillance of e-mails would generally require that government agents obtain a warrant, 18 U.S.C. §§ 2511–18 (2018).

293. *See* U.N. Charter art. 2, ¶ 4.

294. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (holding that Fourth Amendment protections did not apply to government conduct in Mexico directed against a non-resident alien); *see also* Johnson v. Eisentrager, 339 U.S. 763, 777–78 (1950) (holding that non-resident aliens facing military trials in Germany could not seek redress in federal court).

295. *See* JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 1–3 (2008).

encryption protecting those messages.[296] Even after the British and Americans managed to crack the German Enigma and Japanese Magic codes, decryption did not occur in real time because, each day, the German and Japanese military changed the daily code inputs; the Allied cryptanalysts needed to deduce those inputs before they could resume decrypting intercepted messages.[297] Relatedly, the 9/11 Commission's investigation of the terrorist attacks revealed that the National Security Agency had intercepted a message on September 10, 2001, stating "[T]omorrow is zero hour"; however, the message was not translated from Arabic until two days later.[298]

Interception of more communications or signals is, therefore, not always better, because there is a finite limitation to how much information the government can process effectively and in a timely fashion. The National Security Agency (NSA) has been aware of the technological challenges involved in decrypting and analyzing massive amounts of voice and data.[299] At the beginning of the twenty-first century, the NSA was building enormous buildings to house the supercomputers and data storage banks needed to process all of the information that the agency was accumulating.[300]

Another limiting factor besides computing (i.e., decryption) power is the finite number of federal judges, who are needed to issue electronic surveillance warrants.[301] Moreover, unless the counterterrorism agents already can demonstrate probable cause to believe that the target "is committing, has committed, or is about to commit a particular offense,"[302] they will need to proceed under the FISA,[303] where the standard—probable cause to believe that the target of the search is an agent of a foreign power[304]—may be easier to satisfy.[305] Only judges on the FISA court can issue FISA warrants—and there are only eleven FISA judges at any given time.[306] As a

296. On the challenge of decrypting encrypted messages, *see supra* notes 104–120 and accompanying text.

297. KAHN, *supra* note 110, at 587–88.

298. Walter Pincus & Dana Priest, *NSA Intercepts on Eve of 9/11 Sent a Warning*, WASH. POST, June 20, 2002, at A01.

299. *See* BAMFORD, *supra* note 295, at 2.

300. *Id.* at 3.

301. *See* 50 U.S.C. § 1803(a)(1) (2012).

302. 18 U.S.C. § 2518(3)(a) (2018).

303. *See* 50 U.S.C. § 1803(a)(1).

304. *Id.* § 1805(a)(2(A).

305. In fact, this very concern led the Clinton Justice Department to adopt a "wall" to "regulate[] the manner in which [foreign intelligence] information could be shared from the intelligence side of the house to the criminal side." THE 9/11 COMM'N REPORT, *supra* note 16, at 79.

306. 50 U.S.C. § 1803(a)(1).

further bottleneck, FISA requires the Attorney General's signature on every warrant application.[307]

3. *Active Detection*

In contrast to passive detection, active detection systems send out directed electromagnetic waves of their own and then interpret the interference of other objects with those same waves.[308] By analogy, passive counterterrorism is made up of surreptitious surveillance and monitoring, while active counterterrorism involves interaction by government agents within the relevant community, particularly with the one or more targets.[309] The interaction can range from consensual interviews of the target to undercover operations where an agent or informant pretends to be an extremist seeking to ally with the target.[310] Strictly speaking, though, such direct interaction is not really analogous to the use of active radar or sonar because it would typically focus on individuals who came to the attention of the counterterrorism agents through other means, such as the passive detection forms discussed above.

Compared to the passive detection methods, direct interaction provides the government with a better opportunity to refine its assessment of a target's intentions because the agents can adjust their operation in reaction to the target's responses. The potential for more accurate assessment of a target's intentions is not, however, without possible downsides. If the target is indeed intent on committing a terrorist act, direct interaction of any type may change his or her behavior. In this context, it might mean alerting the target that law enforcement authorities are suspicious. The target might respond by abandoning the planned act of terrorism, which might be considered a solid victory if the abandonment is permanent but only a mixed one if it is temporary; or the target might accelerate the act of terrorism, improvising if necessary. The leader of the New York subway bombing plot, Najibullah Zazi, discarded his explosive material when he learned from his father that

---

307. *Id.* § 1804(a).

308. SKOLNIK, *supra* note 123, at 1–2.

309. *Compare* Temple-Raston, *supra* note 87 (utilizing surveillance and wiretaps to monitor targets), *with* Ian Cummings, *FBI Undercover Stings Foil Terrorist Plots—but Often Plots of the Agency's Own Making*, KAN. CITY STAR (Mar. 2, 2017), https://www.kansascity.com/news/local/crime/article135871988.html (contacting potential targets via social media to activate sting operations).

310. *See, e.g.*, Larry Lazo et al., *Court Papers Show Maryland Bomb Plot Suspect Spooked by Oregon Sting*, CNN (Dec. 9, 2010, 5:22 AM), https://www.cnn.com/2010/CRIME/12/08/maryland.plot/index.html [https://perma.cc/3HWC-VPU4].

New York police officers had questioned a Muslim cleric about him.[311] A codefendant, Adis Medunjanin, on the other hand, when confronted by a search warrant, reacted by driving away and trying to crash his car on a crowded freeway.[312]

While deception operations such as undercover stings do not run the same risk of directly alerting would-be terrorists that they might be dealing with a government operative, the fact that such stings have been disclosed publicly (both in government press releases and media accounts)[313] nevertheless may alert a perspicacious target that he or she is being ensnared in a law enforcement scheme. For example, the FBI's arrest of Mohamed Mohamud on November 26, 2010, for attempting to bomb a Christmas tree lighting ceremony in Portland, Oregon, resulted in national news coverage.[314] One person who caught wind of the news coverage was Antonio Martinez, who at that very instant was plotting with two others (one an informant, the other an undercover agent) to bomb a military recruiting station in Maryland.[315] Martinez reportedly told the informant that "he needed to know 'who this brother [i.e., the undercover agent] is. . . . I'm not falling for no b.s.'"[316] In the end, Martinez did fall for the sting operation—but with awareness of the possibility that he was dealing with government operatives.[317]

Continued and (relatively) widespread use of undercover sting operations may therefore seem analogous to active detection in that they provide the user with the opportunity to zero in on a particular target, but they may also tip that target off that someone is testing him or her. In wartime, this double-edged nature of active detection means that it must be used carefully, if at all, in

311. Press Release, U.S. Dep't of Justice, Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad, and Providing Material Support to al Qaeda (Feb 22, 2010), https://www.justice.gov/opa/pr/najibullah-zazi-pleads-guilty-conspiracy-use-explosives-against-persons-or-property-us [https://perma.cc/SFU2-G5DP].

312. *See* William K. Rashbaum, *F.B.I. Seizes Passport of Queens Man Scrutinized in Plot*, N.Y. TIMES, Jan. 8, 2010, at A22.

313. *See, e.g.*, Cummings, *supra* note 309; Press Release, U.S. Att'ys Office N. Dist. of Ohio, Five Men Arrested in Plot to Bomb Ohio Bridge (May 1, 2012), https://archives.fbi.gov/archives/cleveland/press-releases/2012/five-men-arrested-in-plot-to-bomb-ohio-bridge; Press Release, U.S. Dep't of Justice, Foreign Nationals Charged with Attempting to Provide Material Support to Terrorists and Alien Smuggling (Jan. 27, 2006), https://archives.fbi.gov/archives/cleveland/press-releases/2012/five-men-arrested-in-plot-to-bomb-ohio-bridge [https://perma.cc/J94P-3A9Z].

314. *See* Yin, *supra* note 84, at 44–45.

315. Lazo, *supra* note 310.

316. *Id.*

317. *Id.*

situations calling for stealth and secrecy, lest the user give away its location. Although the stakes of counterterrorism are high—potentially life or death—the consequences of giving away the fact that there was an active counterterrorism operation are not necessarily as dire as those in wartime but might lead to accelerated execution of terrorist plots that, even if incomplete in their planning, could still cause death and destruction.

B. Determining the Intentions of Potential Terrorists

Once soldiers in open armed conflicts have detected and identified opposition forces, they generally need not ascertain the intentions of those enemy forces before attacking.[318] Traditional armed forces can be attacked even if they are not engaged in hostilities at that moment because the laws of war predicate eligibility for being attacked on combatant status, not on actual intent to fight.[319] Counterterrorism agents, on the other hand, stand in a different position; for them, surveillance, community tips, and online monitoring cannot always provide a clear indication of whether the target is in fact intent on carrying out a mass attack. Community members who provide tips might be mistaken or, worse yet, might be trying to cause trouble for the suspect. Online statements might sound alarming, but the writer might simply be venting with no intention of carrying out an actual attack. Unlike the soldier, the counterterrorism agent cannot identify an antagonist by uniform or other fixed sign, and thus cannot "attack" (i.e., arrest) such a suspect absent probable cause to believe that a crime is being or will be committed.

Yet many of the mass shooters and bombers discussed earlier in this Article did give warning signs that they were dangerous and potentially violent.[320] In the aftermath of a mass shooting (or bombing), there were a number of questions raised about whether something could have been done to prevent the attack. For example, after Jared Loughner's shooting rampage killed six and wounded fourteen others, *Time Magazine* asked: "[C]ould anything have been done to prevent the violence? What signs that trouble lay ahead were missed? What signs were observed but ignored? In short, what

---

318. *See* PICTET, *supra* note 78, at 46–48 (quoting 1907 Hague Regulations, Annex to the 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, T.S. No. 539, 623).

319. *See id.* (quoting 1907 Hague Regulations, Annex to the 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, T.S. No. 539, 623).

320. *See supra* notes 165–73 and accompanying text.

can be done to prevent a potentially ill or unstable person from harming others?"[321]

In March 2018, the U.S Secret Service National Threat Assessment Center released a report that analyzed twenty-eight mass attacks occurring in 2017 in public places in the United States, concluding that 79% of the attackers had "engaged in communications or exhibited behaviors that caused concern in others."[322] The concerns resulted in a variety of responses ranging from complaints to employers or law enforcement, to firing the person, to avoiding him altogether,[323] but notably not detention, since all the suspects were at liberty to carry out their deadly attacks.[324]

Hindsight tells us that the red flags in those three cases indeed foreshadowed their violent actions, but there is no doubt red flags were raised involving many other persons who did not act out violently. Not only would it be infeasible to detain every person who flashes signs of dangerousness, but also it would result in the unreasonable detention of numerous persons who should not be detained. Indeed, a "finding of dangerousness, standing alone, is ordinarily not a sufficient ground upon which to justify indefinite involuntary commitment."[325] There must be some kind of mental illness or abnormality in addition to the dangerousness to justify civil commitment.[326]

Rather, the lesson is that we need some approach for determining *which* persons raising red flags in fact pose real dangers to society. Further monitoring of the suspect might resolve the uncertainty over the suspect's intentions, but definitive resolution is more likely to occur in the direction of confirming intent to commit terrorist acts than refuting such intent. This is true because activity that goes beyond speech into the realm of preparation—such as acquiring weapons or precursor material for homemade bombs—require the suspect to take affirmative steps that are distinctively separate from mere speech.[327] By contrast, failure to take any affirmative steps toward preparation of an actual attack is consistent not only with lack of intention but also with intent to attack without being ready to do so yet.

---

321. Kate Pickert & John Cloud, *If You Think Someone Is Mentally Ill: Loughner's Six Warning Signs*, TIME, Jan. 11, 2011.

322. U.S. DEP'T OF HOMELAND SEC., U.S. SECRET SERV., NAT'L THREAT ASSESSMENT CTR., MASS ATTACKS IN PUBLIC SPACES – 2017, at 1, 6 (2018).

323. *Id.* at 6.

324. *See* Pickert & Cloud, *supra* note 321 ("In most states, including Arizona, it's predictably difficult to detain someone involuntarily due to mental illness").

325. Kansas v. Hendricks, 521 U.S. 346, 358 (1997).

326. *Id.*

327. *Cf.* 18 U.S.C. § 371 (2018) (establishing an overt act in furtherance of an unlawful agreement as an element of criminal conspiracy).

Counterterrorism agents may find themselves facing a similar situation to that which Detective McFadden of *Terry v. Ohio* found himself—namely, having suspicions about what certain individuals were up to but not having probable cause to arrest.[328] McFadden observed three people possibly casing a store for a later burglary attempt.[329] Lacking probable cause to arrest, he approached the trio for a not entirely consensual encounter, which resulted in the discovery of a handgun on Terry, leading to the arrest of all three.[330] The Supreme Court approved the "stop-and-frisk."[331] The result of the stop-and-frisk should be either that the officer develops probable cause from the responses given by the suspect (or from evidence seized during the frisk), or the reasonable suspicion is dissipated because the suspect's answers satisfy the officer that there is no criminal activity taking place.[332] *Terry* is admittedly an imperfect analogy because the stop-and-frisk encounter is not voluntary and it requires that the officer have reasonable suspicion of criminal activity.[333] However, it demonstrates that the legal regime contemplates direct interaction as an alternative to observing and waiting.

Thus, instead of relying on further surveillance and monitoring, government agents might seek to expedite their assessment of the suspect's intentions through direct interactions with the suspect (i.e., the counterterrorism equivalent of active detection)—such as overt interviews or undercover sting operations. An interview might dispel the agents' suspicions about the target, or it might intensify those suspicions, and possibly even provide a basis for arresting the person.[334]

The undercover sting operation has a number of advantages in this regard. In a typical undercover sting operation, one or more law enforcement officers conceal their true status and instead assume a criminal persona in order to assess whether the target has similar criminal intentions.[335] Undercover police officers have thus pretended to be illegal drug buyers or sellers, men in search

328. Terry v. Ohio, 392 U.S. 1, 7–8, 22 (1968).

329. *Id.* at 6.

330. *Id.* at 6–7.

331. *Id.* at 10, 29–30.

332. *See id.* at 28.

333. *Id.* at 30.

334. *Cf.* Bowden, *supra* note 177 (discussing how a New York homicide detective managed to get a suspect to give "him three voluntary statements in a single day, each one signed, each one different, each one slightly closer to the truth"); *see also* Stansbury v. California, 511 U.S. 318, 320 (1994) (discussing a situation where suspect voluntarily appeared at police station and proceeded to incriminate himself).

335. GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA 7, 52 (1988).

of prostitutes, prostitutes, or sellers or fences of stolen property.[336] When a person attempts to engage in the unlawful transaction, he finds himself arrested.

Political corruption is another area in which undercover sting operations have been used to secure criminal convictions.[337] Like vice crimes, bribery is an activity defined by law as an offense but one where the participants are voluntarily and consensually engaged.[338] In the late 1970s, the FBI initiated an undercover sting operation to investigate potential bribery of U.S. congresspersons.[339] Known as ABSCAM, the two-year operation involved an FBI agent posing as a wealthy Arab sheikh, assisted by a con artist, who ultimately caught a U.S. senator, several U.S. representatives, and other public officials such as mayors and city councilmembers accepting fictitious bribes.[340] The FBI also used undercover operations to investigate violent criminals, beginning with Joseph Pistone's infiltration of the Mafia in the late 1970s.[341] For six years, Pistone (known as Donnie Brasco) played an expert jewel thief who worked his way into a mob family, eventually reaching the position where he was ready to be sponsored for full membership.[342] As a result of Pistone's undercover work, the federal government indicted hundreds of Mafia members and convicted over 100 of them.[343] Not surprisingly, law enforcement agencies began to use undercover agents to infiltrate domestic terrorism gangs (often white supremacists) well before 9/11.[344]

---

336. The possibility of undercover operatives 'stinging' each other on opposite sides of an illegal transaction is not unheard of. *Id.* at 173–75 (recounting numerous instances of undercover law enforcement agents trying to arrest other undercover law enforcement agents).

337. *Id.* at 42.

338. Howard J. Alperin, Annotation, *Elements of Offense Proscribed by the Hobbs Act (18 U.S.C.A. § 1951) Against Racketeering in Interstate or Foreign Commerce*, 4 A.L.R. Fed 881 § 6[f] (1970). On the other hand, where a political official demands an "under the table" payment in exchange for an official favor, and the other party complies out of fear that the official would otherwise retaliate, we would describe the crime as extortion. *Id.*

339. *See generally* ROBERT W. GREENE, THE STING MAN: INSIDE ABSCAM (1981).

340. *See, e.g.*, *id.* at 5–11.

341. Pistone recounted his experiences in JOSEPH D. PISTONE WITH RICHARD WOODLEY, DONNIE BRASCO: MY UNDERCOVER LIFE IN THE MAFIA 27 (1988).

342. *Id.* at 31–33. To gain full membership, Pistone would have had to murder someone targeted by the mob family, although he believed he could have avoided actually doing so, and that his sponsor would have lied to cover for him. *See id.* at 323, 346–47. The FBI believed that the undercover operation was becoming too dangerous for Pistone and set an end date. *Id.* at 348.

343. JOSEPH D. PISTONE & CHARLES BRANDT, DONNIE BRASCO: UNFINISHED BUSINESS 33 (2008).

344. *See, e.g.*, GERMAN, *supra* note 38, at 3–4, 19–23.

If the target of the terrorism sting operation definitively refuses to propose criminal activity, then there may be a basis for concluding that he poses little to no threat.[345] If, on the other hand, the target of the sting reveals his criminal intentions by proposing some violent plan, then the undercover operation can generate evidence sufficient to prove beyond a reasonable doubt that he attempted to engage in a terrorist attack—and hence, provide a legal justification for incapacitating that person.

To be sure, critics of terrorism sting operations have disputed the significance of this conclusion on the ground that government agents entrapped (i.e., manipulated) the target into the end result.[346] The fact that a target intentionally tried to detonate a bomb at the end of the sting operation does not, it is true, prove that the target initially had such an intention before the sting operation commenced. However, the entrapment defense in theory, or at least in practice, exists to ensure that terrorism defendants convicted after sting operations were "predisposed" to commit acts of terror.[347]

A full-scale analysis of the entrapment defense is beyond the scope of this Article, but it is worth noting how entrapment does not fall neatly within the information operations analogy. In federal courts, entrapment focuses on the subjective mindset of the defendant.[348] The objective conduct of the government agents is typically not relevant, because the predisposition question goes to the defendant's mindset before interaction with the government.[349] Thus, in *Jacobson v. United States*—the Supreme Court's most recent decision on the doctrine—the government inundated the defendant for two years with offers to sell child pornography, at the end of which the defendant ended up trying to buy some.[350] The Court did not dispute

---

345. *See, e.g.*, MARX, *supra* note 335, at 93. There is, of course, the possibility that the target either is very clever and wary of being caught in a sting operation or prefers to work alone. *See e.g.*, *id.* at 72.

346. *See, e.g.*, AARONSON, *supra* note 239, at 226; Glenn Greenwald, *The FBI Again Thwarts Its Own Terror Plot*, SALON (Sept. 29, 2011), https://www.salon.com/2011/09/29/fbi_terror/ [https://perma.cc/RRX2-25XP] ("[I]n order to justify this Endless War on civil liberties (and Terror)—the FBI has to search for [young male Muslims] . . . they can recruit, convince, and direct to carry out plots.").

347. *See* Jacobson v. United States, 503 U.S. 540, 540 (1992) (requiring the prosecution, when entrapment is raised as a defense, to prove that the defendant was predisposed independent of government attention to commit the charged crime).

348. *See* PAUL MARCUS, THE ENTRAPMENT DEFENSE 36–39 (2d ed. 1995).

349. *See generally id.* at 38–40. (explaining that a minority of state courts use the objective test, focusing on the reasonableness of the conduct of the government agents). Some scholars have argued that in practice, there is no difference between the two approaches. *See* Ronald J. Allen et al., *Clarifying Entrapment*, 89 J. CRIM. L. & CRIMINOLOGY 407, 409 (1999).

350. *Jacobson*, 503 U.S. at 540.

that the defendant became predisposed to acquire child pornography after the two year campaign, concluding that the defendant was not predisposed at the beginning of the campaign—and thus he had been entrapped.[351]

Entrapment thus tests whether the defendant would have been willing to carry out this planned attack without any coercion by the government.[352] This is an important question because there is a moral appeal to the proposition that the government should not be manufacturing crimes.[353] However, the proposition should perhaps be restated as the government should not be manufacturing crimes *that would not otherwise occur if the target were left alone*. The critical distinction between the originally stated proposition and the modified one is that the latter contemplates that, even if never approached by the government, the target might still attempt to engage in an act of terrorism if approached and persuaded by other persons intent on carrying out such an attack.[354] This modified proposition can be justified on the ground that if the target is malleable enough to agree to a terrorist plot with undercover agents, then he is malleable enough to agree to a terrorist plot with actual terrorists—so long, of course, as there are such actual terrorists capable of such recruitment.

C. Deception and Confusion Operations

Besides gathering information about the enemy, information operations are also about confusing or deceiving the enemy. Electronic jamming systems can overwhelm radars, and false information can be leaked to trick the enemy into acting in a certain way or not to act.[355] Many counterterrorism activities such as electronic surveillance take place and, hence, would be unlikely to confuse or deceive the target, but undercover stings can deceive as well as confuse potential targets.

The deception element is obvious: the undercover agent pretends to be a fellow terrorist but, in reality, is a law enforcement officer, a fact that, if known, would cause the target to avoid the agent. As a result, the target is tricked (or induced) into revealing that he would carry out a terrorist attack if

---

351. *Id.* at 553.

352. *See* AARONSON, *supra* note 239, at 197.

353. *See, e.g.*, *id.* at 16–17.

354. *Cf.* Jessica A. Roth, *The Anomaly of Entrapment*, 91 Wash. U. L. Rev. 979, 982 (2014) (discussing the government's justification "that law enforcement and the real terrorists are competing to find those who would be willing to join the terrorist cause").

355. SCOTT GERWEHR & RUSSELL W. GLENN, THE ART OF DARKNESS: DECEPTION AND URBAN OPERATIONS 25 (2000).

he had the means to do so. The effect of the sting (though not necessarily the mechanism) is similar to that of the Midway ruse, which tricked the Imperial Japanese Navy into revealing that Midway Island was its target.[356]

There is an important distinction between wartime information operations and counterterrorism when it comes to the certainty that the target of the deception is in fact the enemy. The Midway ruse not only was directed at the Japanese Navy but also would not have deceived any Americans because, in that theater of war, only the Japanese Navy would have been seeking information about the conditions on Midway Island.[357] With an undercover sting operation, on the other hand, one goal may be to deceive or trick the target, but another goal—as discussed earlier—is to determine whether the target is actually a would-be terrorist. This means that the sting operation, if improperly executed, may end up deceiving someone who did not pose an actual threat of becoming a terrorist before the government interaction.

With respect to confusion, domestic sting operations can, to the extent their existence is known publicly, jam the "signals" of actual terrorists in a similar way to how electronic jammers overwhelm detectors by flooding the airspace with electromagnetic radiation.[358] Someone looking to engage in domestic terrorism who happens to find seemingly like-minded individuals must now ponder whether he is dealing with true terrorists or with government agents.[359] As a result, a concerned target may back out of what would be an actual (i.e., not a sting) operation or, even if deciding to take part in an operation, may spend time and effort trying to determine whether the co-conspirators are government agents. For example, in other criminal contexts, drug dealers may abandon sales that would otherwise have been made out of fear that the buyers were undercover agents; similarly, prostitutes may forego sexual encounters.[360] By sapping the concentration of criminals and forcing

---

356. Mark Munson, *The Battle of Midway: The Complete Intelligence Story*, WAR ON THE ROCKS (June 3, 2016), https://warontherocks.com/2016/06/the-battle-of-midway-the-complete-intelligence-story/ [https://perma.cc/AN3E-6653].

357. *Id.*

358. *See* P. Anjaneyulu et al., *A Mini Review on Radar Fundamentals and Concept of Jamming*, 8 INT'L J. ADVANCED RESEARCH IN COMPUTER SCI. 763, 765 (2017).

359. *See, e.g.*, Samuel J. Rascoff, *Counterterrorism and New Deterrence*, 89 N.Y.U. L. REV. 830, 854 (2014) (quoting Julian Sanchez, *Why Sting?*, JULIAN SANCHEZ (Sept. 30, 2011), http://www.juliansanchez.com/2011/09/30/why-sting/ [https://perma.cc/E8H2-GL4P]) ("[T]he steady stream of news reports will eventually force any candidate for jihad to assume that an 'Al Qaeda recruiter' who approaches them is much more likely to be an FBI informant or undercover agent than a genuine operative."); *see* AARONSON, *supra* note 239, at 29–30.

360. *See, e.g.*, MARX, *supra* note 335, at 76 (noting how in some cities, prostitutes would not propose sexual transactions but would instead wait for the johns to do so, under the belief

them to spend time monitoring one another, undercover operations deter some criminal activity and undermine the success of other activity. This is one of the normative arguments in support of American conspiracy law, that it "disrupt[s] trust and social order within the conspiracy."[361]

Interestingly, the confusion aspect of sting operations conflicts directly with the active detection aspect of it. Greater public awareness of undercover sting operations means that targets may be more guarded than they otherwise would be, and thus might successfully conceal their terrorist intentions by not falling for the stings. At the same time, greater public awareness of undercover stings may make potential terrorists more paranoid about everyone they deal with and, hence, less likely to engage in coordinated terrorism with others.

VI. LESSONS FROM THE INFORMATION OPERATIONS ANALOGY FOR UNDERCOVER STING OPERATIONS

Undercover law enforcement operations have been in existence long enough that the basic arguments for and against them have been well-developed. Supporters of undercover operations argue that, without them, certain types of crimes would escape detection and prosecution.[362] The vice crimes that were traditionally the target of undercover operations typically had no victims, at least not in the traditional sense of someone who was unwillingly harmed physically or financially, because the transaction between buyer and seller was consensual.[363] Of course, rampant drug sales or prostitution in a neighborhood may depress property values or spur local property crimes, thereby harming the residents of the area. This sort of harm has been described by the Supreme Court as "secondary effects."[364] If these secondary effects are severe enough, then local residents may be motivated to

---

that undercover agents were prohibited from doing so). *But see id.* at 123–24 (discussing research studies finding no deterrent effect from sting operations).

361. Neal Kumar Katyal, *Conspiracy Theory*, 112 YALE L.J. 1307, 1346 (2003).

362. *See, e.g.*, MARX, *supra* note 335, at 118–19, 124–25.

363. *Id.* at 7. Of course, not all sex workers may have chosen their line of work freely of their own will. Sex trafficking remains a serious problem in the United States and is separate criminal conduct. *See* 18 U.S.C. § 1591 (2018) (criminalizing sex trafficking of minors); 18 U.S.C. § 1590 (2018) (criminalizing trafficking in general). Also, one who has voluntarily chosen to become a prostitute does not give up the right to choose to withhold consent for sex. *See* Hagins v. United States, 639 A.2d 612, 616 (D.C. 1994) (quoting Brewer v. United States, 559 A.2d 317, 320 (D.C. 1989).

364. *See* City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 47 (1986).

complain to the police. Short of that, however, such crimes may go undiscovered.[365]

On the other hand, opponents respond that undercover operations entail the manufacturing of crimes by the police.[366] As the Supreme Court has noted, "[T]he function of law enforcement is the prevention of crime and the apprehension of criminals. Manifestly, that function does not include the manufacturing of crime."[367] Whether viewed as a due process violation of a moral outrage, it does seem problematic if apparent criminal conduct occurs *only* because police officers are instigating it. That may burnish arrest and conviction statistics, but it does not make the community safer. However, the line between crime prevention or apprehension and crime manufacturing is often blurry where the undercover agent must do more than be a simple purveyor or buyer of illegal goods or services. The entrapment defense arose as a means of guarding against government overreach.

One important point about the entrapment defense is that it is *not* a constitutional requirement.[368] The Supreme Court case that established the defense as a matter of federal law, *Sorrells v. United States*,[369] did so through statutory interpretation of legislative intent, reasoning that Congress could not have intended to enable law enforcement officials to abuse their power by "lur[ing]" innocent persons to commit crime.[370] As a consequence, state courts are not required to follow the federal version of the entrapment defense if they interpret their criminal statutes differently, and in fact, some states have opted for objective approaches that focus on the conduct of the law enforcement officers, rather than the defendant's mindset.[371]

A. Undercover Operations in Non-Law Enforcement Contexts

Undercover operations have not been limited to law enforcement agents. Journalists, activist muckrakers, corporate businesses, housing and

---

365. Even critics of the entrapment doctrine have conceded that some undercover operations may be necessary to detect victimless crimes. *E.g.*, United States v. Russell, 411 U.S. 423, 445 (1973) (Stewart, J., dissenting).

366. Sherman v. United States, 356 U.S. 369, 372 (1958).

367. *Id.*; *see also* Casey v. United States, 276 U.S. 413, 423 (1928) (Brandeis, J., dissenting) ("The Government may set decoys to entrap criminals. But it may not provoke or create a crime and then punish the criminal, its creature.").

368. *See* MARCUS, *supra* note 348, at 38.

369. Sorrels v. United States, 287 U.S. 435 (1932).

370. *Id.* at 446–48 ("Literal interpretation of statutes at the expense of the reason of the law and producing absurd consequences or flagrant injustice has frequently been condemned.").

371. *See* MARCUS, *supra* note 348, at 38–39.

employment discrimination testers, and airport security agents, among others, have conducted investigations while concealing their true identities and goals from their targets.[372] Because these actors typically lack the arrest powers that law enforcement agents possess,[373] the direct result of the investigation is not prosecution; nevertheless, the general goal of exposing unknown misconduct or wrongdoing is similar.

One type of non-law enforcement undercover work is performed by covert "testers" who purport to apply for housing or employment but whose true interest lies in determining whether the targeted landlord or employer discriminates against minorities or other disfavored persons.[374] In evaluating whether housing discrimination exists, for example, the testing agency might send two "applicants"—one white and one African-American—with identical financial backgrounds, job histories, and references to see whether they are treated similarly by landlords.[375] The white tester serves as the control; if the landlord offers a unit to the white tester but not to the African-American one, one could reasonably suspect racial discrimination as the cause of the disparate treatment.[376] The African-American testers have no actual interest in renting the apartment, a fact that, if known, would provide a clear reason for the landlord to reject the rental application.[377] Very similar to housing and employment testers are "secret shoppers," who pretend to be customers with the secret goal of evaluating the service, appearance, and other relevant

372. *See, e.g.*, UNIV. OF IOWA CLINICAL LAW PROGRAMS, THE USE OF UNDERCOVER TESTERS TO IDENTIFY AND ELIMINATE DISCRIMINATION IN THE SELECTION AND HIRING OF EMPLOYEES (2010); Ashley Halsey, III & Missy Ryan, *Secret Observation of Air Travelers' Behavior Began in 2010*, WASH. POST, July 31, 2018, at A3; *Fair Housing Enforcement Organizations Use Testing to Expose Discrimination*, EVIDENCE MATTERS, Spring–Summer 2014, at 16 [hereinafter *Fair Housing*]; *Muckrakers*, U.S. HISTORY, http://www.ushistory.org/us/42b.asp [https://perma.cc/T43K-7XJU].

373. The federal government gives the power to arrest to multiple different agencies, but that authority does not extend to the actors listed above. *See, e.g.*, 18 U.S.C. §§ 3041, 3051–53, 3056, 3056A, 3062 (2018).

374. *See, e.g.*, *Fair Housing*, *supra* note 372, at 18.

375. *See, e.g.*, *id.*

376. *See, e.g.*, Havens Realty Corp. v. Coleman, 455 U.S. 363, 368 (1982).

377. Notwithstanding their lack of actual interest in renting, the Supreme Court held that such testers do have legal standing to sue landlords who falsely tell them that no units are available. *See id.* at 373–75 ("That the tester may have approached the real estate agent fully expecting that he would receive false information, and without any intention of buying or renting a home, does not negate the simple fact of injury."). There are, of course, alternatives to covert testing for determining housing or employment discrimination. In the employment context, Title VII allows employment discrimination plaintiffs to use statistical data to prove that a particular employment practice has a disparate impact on a protected class. *See* 42 U.S.C. § 2000e-2(k)(1)(A)(i) (2012).

business factors of stores and restaurants.[378] By keeping their status as an evaluator secret, they avoid having the store or restaurant provide unusual and exceptional service so as to secure a favorable review.[379]

Some government agencies that do not typically investigate and interdict criminal activity also engage in undercover operations.[380] The Department of Homeland Security (DHS), for example, tests the effectiveness of its airport security personnel by attempting to sneak forbidden items such as firearms through security checkpoints.[381] Like restaurant reviewers, a DHS official who overtly announced his or her status would render the test of security procedures totally worthless.

Journalists have had a history of disguising their identities in order to gain access to explosive stories, dating back at least to 1887 when Nellie Bly published an account of her feigned insanity and stay in Blackwell's Island Insane Asylum, exposing the awful conditions within.[382] It is difficult to believe that Bly could have written the same story through reliance on direct face-to-face interviews with the asylum administrators.

In the 1970s, the *Chicago Sun-Times* secretly purchased a Chicago bar named the Mirage Tavern, which it then operated as a private establishment.[383] As a result, the paper was able to publish a series of articles detailing the rampant corruption among Chicago city inspectors soliciting

---

378. *See, e.g.*, Laura Blinkhorn, *Secret Shoppers and Conflicts of Interest*, 15 AMA J. ETHICS 119, 119 (2013).

379. This is also why restaurant critics should not identify themselves as food critics when eating at a restaurant for the purpose of reviewing it. *See, e.g.*, Desnick v. Am. Broad. Co., 44 F.3d 1345, 1351 (7th Cir. 1995) (noting that without the concept of "deemed consent" where some people can conceal their intentions, "a restaurant critic could not conceal his identity when he ordered a meal, or a browser pretend to be interested in merchandise that he could not afford to buy"); *see also* Robert Sietsema, *Everyone Eats . . . But That Doesn't Make You a Critic*, COLUM. JOURNALISM REV., Jan.–Feb. 2010, https://archives.cjr.org/feature/everyone_eats.php [https://perma.cc/L4Z2-67S4].

380. *See* Eric Lichtblau & William M. Arkin, *More Agencies Are Using Undercover Operations*, N.Y. TIMES, Nov. 16, 2014, at N1.

381. *See* Michael Goldstein, *TSA Misses 70% of Fake Weapons but That's an Improvement*, FORBES (Nov. 9, 2017), https://www.forbes.com/sites/michaelgoldstein/2017/11/09/tsa-misses-70-of-fake-weapons-but-thats-an-improvement/#395ab2372a38 [https://perma.cc/B9EF-7DZS]; Eric Bradner & Rene Marsh, *Acting TSA Director Reassigned After Screeners Failed Tests to Detect Explosives, Weapons*, CNN (June 2, 2015), https://www.cnn.com/2015/06/01/politics/tsa-failed-undercover-airport-screening-tests/index.html [https://perma.cc/4KY9-JT8Y].

382. NELLIE BLY, TEN DAYS IN A MAD-HOUSE 3 (1887).

383. *See* Pete Grieve, *40 Years Later, Reporters Remember How They Bought a Bar to Expose Corruption*, CHI. SUN-TIMES, Jan. 26, 2018, at 3.

bribes to overlook code violations.[384] The movie *Fast Times at Ridgemont High* was based on Cameron Crowe's book of the same name,[385] which depicted the twenty-two-year-old author's year-long undercover experience as a high school senior.[386]

In 1992, two TV reporters for ABC's *PrimeTime Live* news magazine show went undercover at the supermarket chain Food Lion in order to document alleged unsanitary food handling practices.[387] The reporters successfully applied for jobs with Food Lion stores in North Carolina and South Carolina, using made-up identities, fake resumes, and false references to conceal their true identities as ABC employees.[388] Then, at their "new" jobs, the reporters secretly filmed what appeared to be stomach-turning food-handling practices: "Food Lion employees repackaging and redating fish that had passed the expiration date, grinding expired beef with fresh beef, and applying barbeque sauce to chicken past its expiration date in order to mask the smell and sell it as fresh in the gourmet food section."[389]

Another example of journalistic sting operations was the *Dateline NBC* program "To Catch a Predator," which aired from late 2004 to late 2007.[390] In this show, members of a group known as Perverted-Justice pretended to be teenage girls under the age of consent and would frequent online chat rooms, eventually attracting the attention of purported sex predators.[391] Some chats would turn explicitly sexual, and if the sting target proposed a physical encounter, the Perverted-Justice member would name a location.[392] Waiting at that location would be a young-looking actress playing a decoy, who would invite the target inside the home.[393] Typically, she would tell the target to relax while she would go to change; at that point, host Chris Hansen would step out to confront the target with printed transcripts of the sexually explicit chat conversation.[394] For the target, the situation would only get worse from there

---

384. *Id.*

385. *See generally* CAMERON CROWE, FAST TIMES AT RIDGEMONT HIGH: A TRUE STORY (1981).

386. *Id.* at 9.

387. Food Lion, Inc. v. Capital Cities, 194 F.3d 505, 510 (4th Cir. 1999).

388. *Id.* at 510.

389. *Id.* at 510–11.

390. Maurice Chammah, *The Return of 'To Catch a Predator,'* MARSHALL PROJECT (Jan. 22, 2017), https://www.themarshallproject.org/2017/01/22/the-return-of-to-catch-a-predator [https://perma.cc/4KAY-L5BV].

391. Luke Dittrich, *Tonight on Dateline This Man Will Die*, ESQUIRE, Sept. 1, 2007, at 233, 235.

392. *Id.*

393. *Id.*

394. *Id.*

because the police would be waiting outside to arrest him whenever he tried to leave.[395]

The mere fact that a particular undercover operation turned out to be successful from the standpoint of achieving the intended goal—such as delivering a shocking expose to the readership—has not always resulted in unqualified accolades. The *Chicago Sun-Times'* series based on its secret ownership and operation of the Mirage tavern (documenting the astounding level of corruption and graft among Chicago inspectors) won the Pulitzer Prize jury's vote, but the Pulitzer board, led by *Washington Post* editor Ben Bradlee, overrode that vote, believing that the newspaper had entrapped the city officials, acted deceptively, or both.[396]

Similarly, the *PrimeTime Live* segment on Food Lion embroiled ABC in protracted litigation over the news program's use of deception to secure the undercover positions for the two reporters.[397] The jury returned a verdict in favor of Food Lion on its counts of fraud, trespass, and breach of the duty of loyalty, and based on the jury's special findings, the district court found in favor of Food Lion on its contention that ABC had engaged in unfair business practices in violation of state law.[398] Food Lion was awarded $1 on its breach of duty of loyalty claim, $1 on its trespass claim, $1,400 in compensatory damages, and over $5 million in punitive damages on the fraud claim.[399] (The court reduced the punitive damages award to $315,000.) After the trial, the jury foreman reportedly told ABC: "You did not have guidelines before . . . . You now have them. Let's find a way to work within those guidelines."[400]

And, despite its seemingly laudatory goal of identifying child sex predators and helping law enforcement prosecute them, MSNBC's "To Catch a Predator" program drew criticism on a variety of fronts, including charges that the show over sensationalized the issues,[401] entrapped the alleged

---

395. *Id.*

396. *See Chicago Tribune Goes Undercover for Stunning Exposé*, PULITZER PRIZES, https://www.pulitzer.org/article/chicago-tribune-goes-undercover-stunning-expose [https://perma.cc/36WV-DWQ7].

397. Food Lion, Inc. v. Capital Cities, 194 F.3d 505, 511 (4th Cir. 1999).

398. *Id.*

399. *Id.* The court had also awarded $1,500 on the unfair business practices claim but forced Food Lion to choose between that and the fraud claim. *Id.*

400. Susan Paterno, *The Lying Game*, AM. JOURNALISM REV., May 1997, at 40.

401. *See* Dittrich, *supra* note 391, at 241; Craig Silverman, *Gotcha! Dateline's Predator Problem and the Lobotomy that Caused It*, HUFFPOST: THE BLOG (June 12, 2006), https://www.huffpost.com/entry/gotcha-datelines-predator_b_22840 [https://perma.cc/62GA-KMP5]; *Ethics of NBC's Sting Show 'To Catch a Predator,'* NPR (Jan. 16, 2007, 10:00 AM), https://www.npr.org/templates/transcript/transcript.php?storyId=6870926 [https://perma.cc/KE6B-Q4QP].

predators, arrogated to itself the right to punish perpetrators by exposing them to public humiliation without the benefit of trial, and essentially bought stories by paying Perverted-Justice for its role.[402] In one notable instance, a district attorney refused to prosecute any of the targets of a "To Catch a Predator" operation out of evidentiary concerns over the authenticity of the chat logs.[403]

We should be hesitant to draw any definitive conclusions based on the reactions to these disparate incidents, as they span several years and different contexts. Nevertheless, it appears that the degree and type of interaction between the undercover operative and the target is correlated with the general response to that undercover operation. Where the undercover operation consists primarily of concealing one's identity but otherwise interacting with the target in much the same way as any other member of the public, there has been little, if any, controversy over the operation.[404] Restaurant reviewers, housing testers, and TSA agents checking whether DHS screeners will notice forbidden items exercise very little discretion in terms of how they interact with those whom they are testing. The DHS agent does not influence how the TSA scanner performs his or her duties, but rather merely observes the competency of that performance.[405] Indeed, but for the fact that one might risk being detained or arrested for attempting to sneak a weapon on board a flight, an ordinary traveler could perform the same test. In the same way, the restaurant reviewer has no effect on the kitchen staff's food preparation and presumably little, if any, effect on the wait staff.[406] Undercover journalist Nellie Bly's instructions from her editor describe passive, rather than active, engagement with the subject of the story:

---

402. *See, e.g.*, Douglas McCollam, *The Shame Game*, COLUM. JOURNALISM REV., Jan.–Feb. 2007, at 31, https://archives.cjr.org/feature/the_shame_game.php [https://perma.cc/EC4D-5624]; Brian Montopoli, *Does "Dateline" Go Too Far "To Catch a Predator?,"* CBS NEWS (Feb. 7, 2006, 11:20 AM), https://www.cbsnews.com/news/does-dateline-go-too-far-to-catch-a-predator/ [https://perma.cc/KE6B-Q4QP].

403. *See* Associated Press, *Texas DA Won't Prosecute Any Pedophiles Nabbed in NBC "Predator" Show*, FOX NEWS (June 28, 2007), https://www.foxnews.com/story/texas-da-wont-prosecute-any-pedophiles-nabbed-in-nbc-predator-show [https://perma.cc/6YWM-BTPT]. An additional complicating factor was that one of the targets was a prosecutor from another district who committed suicide when facing arrest. *Id.*

404. *See, e.g.*, Jack Shafer, *Is it Ever OK for Journalists to Lie?*, POLITICO MAG. (Nov. 30, 2017), https://www.politico.com/magazine/story/2017/11/30/fourth-estate-project-veritas-james-okeefe-215991 [https://perma.cc/DE5Y-DCU2].

405. Goldstein, *supra* note 381.

406. Of course, a reviewer who was so inclined could go out of his or her way to treat the wait staff unusually well or unusually poorly in an attempt to affect the service provided. But it is difficult to see why a reviewer would do so; any reviewer who was so unscrupulous could simply write a false review. Goldstein, *supra* note 381.

> I was to chronicle faithfully the experiences I underwent, and when once within the walls of the asylum to find out and describe its inside workings, which are always, so effectually hidden by white-capped nurses, as well as by bolts and bars, from the knowledge of the public. "We do not ask you to go there for the purpose of making sensational revelations. Write up things as you find them, good or bad; give praise or blame as you think best, and the truth all the time."[407]

In other words, these sorts of undercover operations are the functional equivalent of passive observation. They are also the equivalent of the sort of law enforcement "[a]rtifice and stratagem" that the Supreme Court has explicitly condoned as "merely afford[ing] opportunities or facilities for the commission of the offense . . . ."[408] On the other hand, some of the more controversial incidents and programs involve undercover operatives who crossed beyond mere observation into direct influence, if not manipulation, of those they were targeting. The ABC news reporters in the *Food Lion* case did not just use their deceptively obtained jobs to record what they (but not the general public) were in a position to see; there was evidence, preserved in outtake footage but not aired, showing that "the undercover ABC producers performed much of the food handling mischief captured by their concealed cameras" and that "ABC producers tried to lure Food Lion workers into violating company rules on the handling of food."[409]

B. Stings as Mimicry

Because undercover sting operations in the counterterrorism context typically involve a degree of interaction between the undercover operative and the target,[410] they will rarely constitute passive surveillance. As a form of active detection, a sting operation is aimed at ascertaining whether the target indeed harbors any terrorist intentions—*current or latent*.[411] For the purposes of this analysis, a target who has current intentions to engage in terrorism

---

407. BLY, *supra* note 382, at 2.

408. *See* Sorrells v. United States, 287 U.S. 435, 441 (1932) (citing Price v. United States, 165 U.S. 311, 315 (1897)); Rosen v. United States, 161 U.S. 29, 42 (1896); Andrews v. United States, 162 U.S. 420, 423 (1896); Grimm v. United States, 156 U.S. 604, 610 (1895); Goode v. United States, 159 U.S. 663, 669 (1895); United States v. Reisenweber, 288 F. 520, 526 (2d Cir. 1923); Aultman v. United States, 289 F. 251, 252 (5th Cir. 1923); Bates v. United States, 10 F. 92, 97 (Ill. Cir. Ct. 1881)).

409. JOSEPH C. GOULDEN, ABC'S FOOD LION LIES: A STUDY IN TV DECEPTION (1997).

410. *See supra* notes 334–44 and accompanying text.

411. *Id.*

would be someone who would attempt an act of terrorism notwithstanding any intervention by the undercover operatives. A target with latent intentions, on the other hand, would be someone who would likely not engage in any terrorism absent external persuasion.

When conceived as a traditional law enforcement operation, the sting operation is tempered by the need to avoid entrapment. If we use terminology from the entrapment defense, the target with latent intentions is not predisposed to engage in terrorism. In *Jacobson v. United States*, the government spent two years targeting the defendant with various child pornography catalogs and other material before he agreed to place an order.[412] The Supreme Court reversed his conviction, noting that "although he had become predisposed to break the law by May 1987, it is our view that the Government did not prove that this predisposition was independent, and not the product of the attention that the Government had directed at petitioner . . . ."[413] In other words, that the sting operation resulted in the target's attempt to commit a crime is not by itself sufficient to defeat a claim of entrapment because the attempt demonstrates only that the defendant was predisposed to commit the crime at that instant and not necessarily that the defendant was predisposed to commit the crime before the undercover operatives began interacting with him or her.[414]

Whether the government should be required to prove predisposition in domestic terrorism sting cases when entrapment is raised as a defense is an interesting question. A target with only latent intentions who is susceptible to manipulation by undercover government operatives is presumably susceptible to similar manipulation by terrorist recruiters. If such recruiters actually exist,[415] then whether the target will be induced into attempting an act of terrorism will turn on whether the sting operation finds the target before a recruiter would have (if at all).

There is, to be sure, a *The Minority Report*-like aspect to this argument. In the Philip K. Dick novella (and subsequent movie based on the story), a future society controlled crime by arresting suspects before they even attempted their crimes, based on the predictions of psychics who could see the future.[416] The philosophical question raised by the story is whether society is justified in punishing people before they have committed crimes if there is

412. 503 U.S. 540, 540 (1992).

413. *Id.* at 550.

414. *See id.*

415. *See supra* notes 352–61 and accompanying text.

416. *See* PHILIP K. DICK, *The Minority Report*, in 4 THE COMPLETE STORIES OF PHILIP K. DICK, at 71, 91–92 (2013); MINORITY REPORT (20th Century Fox 2002).

enough reason to believe that they will commit those crimes in the future.[417] This is a question that is beyond the scope of this Article as it is primarily a policy issue, and it is worth noting that, at least in regards to counterterrorism, the United States has embraced preventative policing.[418] John Ashcroft, President George W. Bush's first Attorney General, stated in a speech in support of the USA PATRIOT Act:

> It falls to the men and women of justice and law enforcement to engage terrorism at home. History's judgment will be harsh—and the people's judgment will be sure—if we fail to use every available resource to prevent future terrorist attacks.
>
> . . . .
>
> . . . . Our single objective is to prevent terrorist attacks by taking suspected terrorists off the street.[419]

Ashcroft referenced the Kennedy Administration's aggressive law enforcement tactics against organized crime, often relying on pretextual prosecutions "to get the job done."[420]

Even if one accepts the philosophy of preventative policing (i.e., the importance of stopping certain crimes from occurring, rather than identifying and prosecuting the perpetrators afterward), the assumption is that the government has correctly assessed the future. In *The Minority Report*, the team of psychics splits on whether the protagonist will commit the predicted murder, calling into question whether the system of convicting defendants for crimes that they have not yet committed is justified.[421] Similarly, even if one accepts the theoretical legitimacy of counterterrorism sting operations on the ground that they can identify and stop would-be perpetrators of mass casualty attacks, that legitimacy is also grounded on the assumption that the sting operation has correctly identified such a target.

If the target is someone with current intentions to commit an act of terrorism, and the undercover operatives are seemingly to facilitate the attack, then it seems unlikely that the sting operation has inaccurately identified the

---

417. DICK, *supra* note 416, at 92–93.

418. *See* Attorney Gen. John Ashcroft, Prepared Remarks for the US Mayors Conference, (Oct. 25, 2001) https://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10_25.htm [https://perma.cc/ZZJ4-JWQW].

419. *Id.*

420. *Id.*

421. DICK, *supra* note 416, at 120–21.

person as a would-be terrorist. For the person who is predisposed to commit an act of terrorism, the sting operation simply reveals that predisposition.

However, if the sting operation manipulates the target into attempting the act of terrorism, the government's justification for such manipulation must be that in the absence of the sting operation, the target would likely have been manipulated by actual terrorist recruiters at some point in the future. Under this justification, the government is effectively acting as a "market participant" in competition with terrorists to find and mobilize potential recruits.[422] The market participant justification in turn depends critically on two assumptions: (1) the undercover operatives were mimicking terrorist recruiters; and (2) there existed some non-trivial possibility that the target and actual terrorist recruiters would have made contact had the government agents not reached the target first.

C. Mimicking Terrorist Recruiters

The information operations analogy to counterterrorism suggests that counterterrorism operations can be used to detect and identify targets, and to confuse and deceive those targets. Thus, the first assumption underlying the validity of the market participant justification is that the government operatives were mimicking terrorist recruiters. In other words, the sting operation must be a substitute for actual terrorism recruiting in terms of types of plots, method of recruitment, resources and support provided, and manipulation.

From the standpoint of detecting and identifying targets at risk of being manipulated and mobilized by actual terrorist recruiters, an ideal counterterrorism operation will be practically indistinguishable from the real deal because a positive response (i.e., agreement to carry out the plot) demonstrates that, under those circumstances, the target could become a terrorist. Preventative policing would then call for incapacitating that person.[423] However, the more that the counterterrorism operation deviates from the practices of actual terrorist recruiters, the less confident we can be that the target is, so to speak, shopping in the correct market. As an easy example, suppose government operatives successfully manipulate a target by threatening the target with prosecution unless he agrees to engage in an act of terrorism; the target would be shown to be susceptible to pressure based on legal punishment. However, such an operation would utterly fail at showing

422. *See* Roth, *supra* note 354, at 982.

423. MARK H. MOORE, ET AL., NAT'L INST. JUSTICE, CRIME AND POLICING 4 (1988).

that the target could have been manipulated by terrorists because terrorists would lack the ability to threaten anyone with prosecution.

To be sure, this example is extreme in its starkness, and in practice, whether an undercover sting operation is sufficiently indistinguishable from actual terrorism recruiting may present challenges on the margins. Since the early 1990s, major terroristic acts (successful or not) have involved truck bombings of buildings, mass shootings, or attacks on aircraft.[424] In 2011, as a result of an undercover sting operation, Rezwan Ferdaus was charged with attempting to bomb the Pentagon and the U.S. Capitol with remote controlled planes packed with explosives.[425] There has not been a publicly known prior terrorism attempt involving remote controlled planes or drone aircraft, so one might ask whether the sting operation was an adequate substitute for actual terrorism recruiting at the time. Perhaps it is enough to say that the precise delivery mechanism of explosives (truck bomb parked at the target location versus remote controlled plane) is not as important as the broad goal of the attack (mass casualties and destruction of a public building).

Or consider the 2010 sting operation against Mohamed Mohamud, in which undercover operatives pretended to be connected to the terrorists that Mohamud was trying to contact.[426] The government claimed (and the jury accepted) that Mohamud originated the idea of parking a truck bomb near a light rail station on the evening of Portland's annual Christmas Tree lighting ceremony;[427] however, Mohamud had no resources of his own with which to carry out the plot and did not know how to build such an explosive device.[428] The undercover agents provided Mohamud with cash to buy bomb-making materials and to rent a safe house, and then they provided him with the purported bomb.[429] It seems safe to conclude that Mohamud would not have been able to realize his plot to bomb the tree lighting ceremony on his own. Thus, the relevant question is whether terrorist recruiters provide cash and build bombs for their recruits or other substantially equivalent material assistance.

When it comes to method of recruitment, one immediate difference is that between the target who reaches out and seeks contact with terrorists versus

---

424. *See, e.g.*, *US Terrorist Attacks Fast Facts*, CNN (Sept. 2, 2019), https://www.cnn.com/2013/04/18/us/u-s-terrorist-attacks-fast-facts/index.html [https://perma.cc/2TBA-C96K].

425. *See* Jess Bidgood, *Massachusetts Man Gets 17 Years in Terrorist Plot*, N.Y. TIMES, Nov. 2, 2012, at A17.

426. United States. v. Mohamud, 843 F.3d 420, 425 (9th Cir. 2016).

427. *Id.* at 427.

428. *See id.* at 428.

429. *Id.* at 428–29.

the one who waits passively until being found by others. Again, there may be a spectrum rather than a binary distinction; a target may draw attention to himself through public social media postings without actually seeking anyone directly and then be contacted by like-minded persons.[430]

D. Actual Possibility of Recruitment

Even if the undercover operation mimicked the tactics of actual terrorist recruiters, the government should show some nontrivial possibility that the target of the sting would have connected with such actual terrorist recruiters. Otherwise, the government is prosecuting a person based on a potentiality that probably would never have occurred. It would be same as if, in the fictional world of *The Minority Report*, the psychics made an incorrect prediction that nevertheless led to the arrest and conviction of a suspect.

Whether the defendant who was caught in terrorism sting operation would likely have connected with actual terrorist recruiters depends on an assessment of how long the defendant would have remained interested in terrorism, how persistent the defendant was about trying to contact terrorist recruiters, and how active terrorist recruiters were in the defendant's physical geographic location and social media circles. These are relevant factors because a prediction that the defendant would likely have connected with terrorists is essentially a stochastic inquiry: in any given time unit, there is some minute chance that the defendant would have made contact with (or been contacted by) actual terrorists. The longer the period of the defendant's interest in terrorism, the more such time units exist, and hence more chances to connect.

Of course, predicting the likelihood of future events where human beings are involved is unlike an exercise in classical physics, where, with perfect information, one can predict the future movement of all physical bodies.[431] Still, courts do have experience with trying to determine, in some circumstances, what would have happened had particular law enforcement agents not gotten involved. The prime example is the inevitable discovery doctrine, under which evidence obtained through an illegal search will not be

---

430. Note that Mohamed Mohamud wrote articles for the al Qaeda-connected online magazine *Jihad Recollections*. *Id.* at 423.

431. In the realm of Newtonian physics (i.e., classical mechanics), if one could know the position and momentum of every particle in the universe, that person could calculate perfectly where each particle has been in the past and where it will be in the future. *See generally* PIERRE SIMON, MARQUIS DE LAPLACE, A PHILOSOPHICAL ESSAY ON PROBABILITIES (Dover Publ'ns ed. 1995) (1814).

excluded from the prosecution's case in chief if the prosecution can establish that other law enforcement agents would have found the same evidence without any reliance on the illegal search.[432] In *Nix v. Williams*, the case establishing the doctrine, two police detectives were transporting a prisoner suspected of murdering a little girl whose body had not been found.[433] During the drive, the detectives spoke directly to the prisoner, exploiting his empathy and religious background to induce him to take them to the location of the body.[434] Because the suspect was already represented by counsel, the detectives were prohibited from eliciting incriminating statements in the absence of the defense lawyer.[435] Thus, the defendant's statements directing the detectives to the victim's body, as well as the body itself (as fruit of the poisonous tree), should have been subject to suppression due to the violation of the his Sixth Amendment right to counsel.[436] The trial court, however, noted that there were multiple police teams searching for the girl's body and concluded that one of those teams, being only 2.5 miles away, would have found the body had the search not been mooted by the suspect's cooperation.[437]

Application of the inevitable discovery doctrine therefore requires that a court construct the counterfactual world in which the police did not violate the defendant's rights.[438] The key language from the opinion is that the police "would have" discovered the evidence through lawful means.[439] In a footnote to the majority opinion, the Court explained that "inevitable discovery involves no speculative elements but focuses on demonstrated historical facts capable of ready verification or impeachment . . . ."[440] In the case, the historical facts consisted of the location of the search parties at the time the defendant agreed to tell his escorts where the body was, the instructions the search teams had been given about where to search, and the intended future direction of the search.[441] According to the Court, it was "clear that the search

---

432. *See* Nix v. Williams, 467 U.S. 431, 444 (1984).

433. *Id.* at 435.

434. *See* Brewer v. Williams, 430 U.S. 387, 392–93 (1977). The detective delivered what has come to be known as the Christian Burial speech, in which he implored the prisoner to take them to the little girl's body before the anticipated snowstorm might prevent it from ever being discovered, and thus preventing the parents from giving her a proper Christian burial.

435. *Nix*, 467 U.S. at 435–38.

436. *Id.* at 437–38.

437. *See id.* at 448–50.

438. *See id.* at 437–38.

439. *Id.* at 444.

440. *Id.* at 444 n.5.

441. *Id.* at 448–49.

parties were approaching the actual location of the body" and would have discovered it on their own.[442]

That determination, however, contains a number of assumptions. A prosecution witness testified that it would have taken the closest search party three to five more hours to reach the body, and that the body was in a culvert, which was one of the types of locations that the search parties had been instructed to look in.[443] It seems likely that the search party would have continued on, but there is no way of knowing for certain that (1) the searchers would have spent up to five more hours before giving up; and (2) they would have continued in that direction without veering away.[444] *Nix* held that the prosecution needed to prove by a preponderance of the evidence that the police would inevitably have discovered the evidence.[445]

At one level, this may sound like a strange proposition. The government's burden is to persuade the judge that it is more likely than not (i.e., preponderance of the evidence) that the police would certainly have found the evidence in the absence of the unlawful search or seizure. Is that burden materially different from having to persuade the judge that it is certain that the police more likely than not would have found the evidence in the absence of the unlawful search or seizure? Law is not mathematics, but this is an instance where the associative property would seem to apply: a greater than 50% chance (preponderance of the evidence) multiplied by a 100% certainty (inevitable discovery) is functionally the same as a 100% certainty (absolute proof) multiplied by a greater than 50% chance (likely discovery). Legal standards are neither addition nor multiplication, so the associative property is only an analogy; however, the point is that if the government makes a strong case that the police would have found the evidence, but the judge still has some doubt, can the judge meaningfully allocate that doubt specifically to the burden of proof; or to the inevitability of discovery?

Yet, in practice, courts have been able to apply the inevitable discovery doctrine.[446] The inevitable discovery doctrine is not the only instance in which a trial court must construct a counterfactual world. When the police commit an illegal search or seizure, the exclusionary rule calls for exclusion of not just the direct evidence obtained as a result of the illegal action, but also certain

442. *Id.* at 449.

443. *Id.*

444. *See* RONALD JAY ALLEN ET AL., COMPREHENSIVE CRIMINAL PROCEDURE 740 (4th ed. 2016) ("How long would the search have gone on? What directions would it have moved? How far?").

445. *See Nix*, 467 U.S. at 449.

446. *E.g.*, United States v. Silvestri, 787 F.2d 736, 746 (1st Cir. 1986).

derivative evidence that the police would not have discovered elsewhere or later.[447] Derivative evidence will not be suppressed, however, if the connection between the illegal police action and that evidence has been "attenuated."[448] A prime example of attenuation is *United States v. Ceccolini*, in which the defendant sought to suppress the testimony of a key government witness on the grounds that the FBI agent had come to know of her existence only because of a previous illegal search by a police officer.[449] The Court held instead that the connection between the illegal search and the witness's testimony had been attenuated by the witness's "free will": "Witnesses are not like guns or documents which remain hidden from view until one turns over a sofa or opens a filing cabinet. Witnesses can, and often do, come forward and offer evidence entirely of their own volition."[450] Of relevance in this case was the fact that the witness was, at the time, studying police science and had indicated a willingness to help the FBI agent.[451] Thus, the Court concluded that it was likely that the witness would have ended up helping the FBI on her own, even if the FBI had not known to approach her—a plausible conclusion, but one that necessarily involved a degree of speculation.[452]

Courts have been able to reach the opposite conclusion when warranted. In *United States v. Ghailani*, the defendant in a terrorism case successfully moved to suppress a key prosecution witness on the ground that the government learned of this witness through its coercive interrogation of the defendant.[453] In rejecting the prosecution's argument that the effects of the illegal interrogation had been attenuated, the district judge found that the witness was not a "willing" one, and that his "motive in testifying is purely to avoid prosecution and other feared adverse consequences to himself."[454]

The inevitable discovery and attenuation of fruit of the poisonous tree doctrines thus demonstrate that trial judges can, when presented with adequate evidence, make determinations about the likelihood that a defendant would have made contact with an actual terrorist had the government not caught him in a sting operation.

---

447. *See* Wong Sun v. United States, 371 U.S. 471, 487–88 (1963).
448. *Id.* at 487 (citing Nardone v. United States, 308 U.S. 338, 341 (1939)).
449. 435 U.S. 268, 270 (1978).
450. *Id.* at 276–77.
451. *Id.* at 272.
452. *See id.* at 272, 280.
453. 743 F. Supp. 2d 261, 265, 275 (S.D.N.Y. 2010).
454. *Id.* at 281.

E. Court Hearings

If a domestic terrorism defendant raises the issues of whether the sting operation mimicked actual terrorism recruiting and whether there was a reasonable possibility of contact between recruiter and target, the trial court must resolve the matter. But resolution could be left to the jury as the trial factfinder, or to the judge; and if the latter, the presentation of evidence to support the prosecution's position could be adversarial or ex parte.

1. Judge or Jury?

A criminal defendant is entitled to trial by jury if the maximum sentence that could be imposed for conviction is more than six months, meaning that the ultimate issue of guilt is decided by a jury.[455] There are, however, many subissues that are potentially decided by the judge during pretrial hearings, and some of those may end the case.[456] A successful motion to dismiss the indictment due to the expiration of the statute of limitations, for example, results in a court order barring any reindictment of the defendant for the same alleged conduct.[457] Theoretically, government conduct might become rise to a level of outrageousness so as to warrant dismissal of an indictment with prejudice.[458]

When the defense raises entrapment, the burden shifts to the prosecution to prove either that law enforcement agents did not induce the defendant to commit the crime in question or that the defendant was predisposed to commit the crime even before interaction with the law enforcement agents.[459] Notably, predisposition to commit the crime must be proven beyond a reasonable doubt to the jury.[460] Predisposition is essentially the flip side of *mens rea*. If the government agents induced the defendant to commit the crime, and the

---

455. *See* Duncan v. Louisiana, 391 U.S. 145, 159 (1968) (citing Cheff v. Schnackenberg, 384 U.S. 373 (1966)).

456. *See* FED. R. CRIM. P. 14.

457. *See* 18 U.S.C. § 3288 (2018).

458. *See* United States v. Russell, 411 U.S. 423, 431–32 (1973) ("[W]e may some day be presented with a situation in which the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction.").

459. *See* Jacobson v. United States, 503 U.S. 540, 548–49 (1992) (citing United States v. Whoie, 925 F.2d 1481, 1483–84 (D.C. Cir. 1991)). The predisposition requirement is part of the subjective version of the entrapment doctrine and is used in federal courts as well as a majority of the states. *See* MARCUS, *supra* note 348, at 669–706.

460. *Jacobson*, 503 U.S. at 551 n.3.

defendant was not already predisposed to do so, then the defendant did not really have the requisite *mens rea* to be guilty. Therefore, it makes sense that entrapment (at least, the subjective version) is a jury issue. Accordingly, it might seem that whether a sting operation adequately mimicked actual terrorism recruiting and whether there was a reasonable possibility that the defendant would have connected with those recruiters should also be matters for the jury to decide.

In fact, that inquiry bears strong resemblance to the objective version of entrapment, which focuses on the government's conduct and is used by a minority of states.[461] As it turns out, of the states that use the objective version of entrapment, some treat it as a jury issue, while others leave it to the judge to decide.[462] The argument for having the judge decide the issue is that the objective version of entrapment focuses on law enforcement misconduct, and "[j]udges are thought to be better able to decide issues involving deterrence of governmental overreaching and establishing standards for future police conduct."[463] Under the same reasoning, the degree of mimicry and the possibility of actual contact with terrorists are matters that are best left to the judge. The focus of the inquiry is on the conduct of the sting operation, not the defendant's mental state.

Even more of a reason to treat the inquiry as one for the judge to determine is that it can be resolved in pretrial hearing, similar to, say, a suppression hearing. The majority of criminal defendants plead guilty,[464] so a jury-based defense (such as the subjective version of entrapment) has very little practical impact. If the adequacy of the government's mimicry of actual terrorism recruiting is a pretrial matter for the judge to determine, however, the defendant can litigate the issue and, if unsuccessful, can resolve the case through a plea negotiation, thus avoiding the dilemma of choosing only one at the expense of the other. Furthermore, the terrorism sting defendant who challenges the sting operation unsuccessfully could plead guilty conditionally with the permission of the prosecution and the court, and thus be able to appeal the adverse ruling.[465]

---

461. *See* MARCUS, *supra* note 348, at 43.

462. *Id.* at 184.

463. *Id.* at 185.

464. *See* ALLEN ET AL., *supra* note 444, at 1231–32 (noting that about 64% of those charged with felonies in the seventy-five largest counties pleaded guilty, while only 3% went to trial, with the rest having charges dismissed or resolved non-adjudicatively; and that when looking at those who were convicted, 97% pleaded guilty).

465. *See* FED. R. CRIM. P. 11(a)(2).

2. Adversarial or Ex Parte Proceeding?

Most hearings before judges in criminal cases involve both the defense and the government present.[466] In fact, upon "the start of adversary judicial proceedings,"[467] the defendant's Sixth Amendment right to counsel attaches, and it is an infringement of that right if the defendant is denied counsel at any critical stage.[468]

There are, to be sure, instances where criminal matters proceed ex parte, notably when law enforcement officers apply for search or arrest warrants, or wiretap orders, as well as grand jury proceedings. These applications typically take place during the investigative stage, before the start of formal adversarial judicial proceedings, when the right to counsel has not yet attached.[469] More importantly, these proceedings generally require secrecy in the moment, which could not be accomplished in an adversarial hearing.[470] The target of a search warrant who has advanced warning about a potential forthcoming search may be able to conceal or destroy evidence, while a person who learns about the existence of a wiretap may use other telephones to avoid surveillance.[471]

Those considerations do not apply to a defendant who seeks to litigate the degree that a terrorism sting operation mimicked actual recruiting efforts and the possibility that the defendant would have made contact with actual terrorists. While the government may well wish to keep the details of the operation from the public and from terrorists, the defendant is necessarily aware (now) of the sting operation tactics used against him. Thus, secrecy in the moment is not a justification for permitting the government to defend the mimicry of the sting operation ex parte. Moreover, even when the government proceeds ex parte to obtain search warrants, wiretaps, or grand jury indictments, the defendant subsequently is entitled to challenge the underlying legal and factual determinations in an adversarial proceeding; the defendant can, for example, try to suppress evidence gathered during the execution of a

466. *See* Rothgery v. Gillespie County, 554 U.S. 191, 213 (2008).

467. *Id.* at 209.

468. *Id.* at 212.

469. *See id.* at 208–09.

470. *See* United States v. Aguilar, 515 U.S. 593, 602 (1995).

471. *Id.* at 596 (discussing defendant's disclosure of wiretap of target to defendant's nephew—a friend of the target—with the implication that the nephew was to warn the target).

search warrant by challenging the probable cause alleged in the supporting affidavit.[472]

Still, the government does have a plausible claim that it needs to keep the scope of its knowledge about terrorist recruiting tactics from the public—and in particular, other terrorists distinct from the defendant. Too much public disclosure of what the government knows about terrorism recruiting tactics could lead terrorists to alter their recruiting tactics so as to avoid being mimicked by undercover operatives. Moreover, such disclosure could also reveal the sources and methods by which the government obtained the information, and thereby enable terrorists to evade surveillance or other intelligence gathering.[473]

The defense lawyer has a duty and obligation to provide the client a zealous defense,[474] which in this context could mean mounting a vigorous challenge to the sting operation. It would be difficult, on the other hand, to see how a defense lawyer would be representing the client legitimately by indiscriminately disclosing classified information to the public or, more instrumentally, agreeing not to disclose classified information in exchange for favorable plea-bargaining terms.

Although not exactly the same situation, the federal conviction of Lynne Stewart provides an example of a defense lawyer gone wrong in the representation of a terrorism client.[475] Stewart was a famous criminal defense lawyer known "for representing the poor and the reviled, usually for modest, court-paid fees," and who "sympathized with clients who sought to fight that system, even with violence, although she did not always endorse their tactics, she said."[476] Stewart's client, Omar Ahmad Ali Abdel Rahman, also known as the Blind Sheikh, was one of the leaders of the foreign terrorist organization Islamic Group, as well as a key conspirator in the 1993 World Trade Center truck bomb attack.[477] Upon his conviction, the Bureau of Prisons imposed

---

472. Granted, the good faith exception to the exclusionary rule will result in the admission of such evidence even if the trial court finds a lack of probable cause unless that lack of probable cause was plainly obvious to the police officers. *See* United States v. Leon, 468 U.S. 897, 904 (1984).

473. A well-known example is how al Qaeda founder and leader Osama bin Laden stopped using a satellite phone after a newspaper reported in 1998 that the National Security Agency was following his movements based on the phone. *See* David E. Rosenbaum, *Bush Account of a Leak's Has Support*, N.Y. TIMES, Dec. 20, 2005, at A24.

474. MODEL RULES OF PROF'L CONDUCT, pmbl. (AM. BAR ASS'N 2018).

475. *See* Joseph P. Fried, *Lynne Stewart Dies at 77; Leftist Lawyer Convicted of Aiding Terrorism Case*, N.Y. TIMES, Mar. 8, 2017, at B16.

476. *Id.*

477. *See* United States v. Stewart, 590 F.3d 93, 101 (2d Cir. 2009).

Special Administrative Measures on Abdel Rahman to limit his contact with the outside world; Stewart signed a form agreeing that she would bring a translator for the sole purpose of communicating legal matters with Abdel Rahman, and that she would not use meetings with Abdel Rahman to pass messages to and from third parties.[478] Nevertheless, Stewart was convicted of providing material assistance to a foreign terrorist organization by allowing members of the Islamic Group to communicate with Abdel Rahman through messages smuggled by Stewart and her translator, as well as smuggling out a message from Abdel Rahman to the public.[479] While Stewart had defenders who believed that she had been prosecuted unfairly to chill zealous representation of terrorism defendants, "[m]any mainstream lawyers . . . believed that Ms. Stewart had acted criminally,"[480] and the Second Circuit not only upheld her conviction but also reversed the district court's original sentence of twenty-eight months on the ground that the judge failed to consider a terrorism sentencing enhancement; on remand, the district court imposed the ten-year sentence that the appeals court had strongly suggested was appropriate.[481]

National security concerns in other criminal contexts have given rise to solutions that could ameliorate the problem identified here. Federal courts have upheld conditioning a defense lawyer's access to classified information about actual terrorist recruiting practices only where that lawyer has been granted security clearance.[482] Security clearance is, of course, not an absolute guarantee that the recipient will not disclose the classified material, as recent high-profile, security-cleared leakers Reality Winner, Edward Snowden, and Chelsea Manning have demonstrated.[483] But a security clearance requirement to be able to access classified information should reduce the likelihood of both inadvertent as well as intentional disclosures.

---

478. *Id.* at 102–03.

479. *Id.* at 107–08.

480. *See* Fried, *supra* note 475, at B16.

481. *See id.*

482. *See, e.g.*, United States v. Bin Laden, 58 F. Supp. 2d 113, 122–23 (S.D.N.Y. 1999) (rejecting defense counsel's claim that court could not require security clearance to be able to access classified information); United States v. Al-Arian, 267 F. Supp. 2d 1258, 1267 (M.D. Fla. 2003); United States v. Al-Arian, 267 F. Supp. 2d 1258, 1267 (M.D. Fla. 2003); United States v. Abdi, 498 F. Supp. 2d 1048, 1087–88 (S.D. Ohio 2007).

483. *See, e.g.*, Ken Dilanian, *How Did Accused NSA Leaker Reality Winner Get Security Clearance?*, NBC NEWS (June 6, 2017), https://www.nbcnews.com/news/us-news/how-did-accused-nsa-leaker-reality-winner-get-security-clearance-n768816 [https://perma.cc/5H93-P3HS].

A requirement of security clearance for defense counsel does raise concerns that the Justice Department—which issues such clearances—will have "the ability to control who will work on classified matters for the defense. To eliminate a particularly troublesome opponent, the Justice Department may deny a security clearance to a specific attorney, investigator, or expert witness . . . who needs access to classified information to be effective."[484] Federal courts have not, however, been receptive to defense arguments against security clearance requirements.[485]

The alternative would be to deny the defense access to any classified information about terrorism recruiting tactics. The defense would remain free to argue that the sting operation did not mimic actual terrorism recruiting, but the defense would be hampered by being able to present only one piece of the puzzle, that being the defendant's account of what was done to him. The other piece of the puzzle is the recruiting practices of actual terrorists. At best, defense counsel might be able to rely on open source materials to construct a sense of how terrorists recruit, but such information is almost certainly going to be incomplete.

VII. CONCLUSION

U.S. domestic counterterrorism policy, in the nearly two decades since the September 11 attacks, has embraced a variety of tactics ranging from widespread electronic surveillance to undercover sting operations. Civil libertarians have decried these tactics as unlawful and unjustified, and in some instances—such as mass warrantless surveillance—courts have reined in the government. On the other hand, the undercover sting operations have resulted in dozens of convictions notwithstanding claims of entrapment.

This Article has suggested a normative reconceptualization of domestic counterterrorism as a form of information warfare aimed at detecting, identifying, confusing, and deceiving potential enemies. Electronic surveillance, public monitoring of social media, and following up on tips can be analogized to radar, and sting operations can be analogized both to radar (in detecting the enemy) and to deception operations (in deceiving the enemy). Detecting the enemy in the context of counterterrorism is really an exercise in determining the intentions of the target, as well as the susceptibility of the target to manipulation and inducement by others. This exercise requires that the government mimic the ways in which terrorism recruiters manipulate and

---

484. Brian Z. Tamanaha, *A Critical Review of the Classified Information Procedures Act*, 13 AM. J. CRIM. L. 277, 289 (1986).

485. *See Al-Arian*, 267 F. Supp. 2d at 1267; *Abdi*, 498 F. Supp. 2d at 1087; United States v. Oakley, No. 3:07-CR-88, 2007 WL 4118298, at *4–5 (E.D. Tenn. Nov. 16, 2007).

induce others into committing acts of terrorism. Although this is primarily a factual inquiry, it is best decided by the judge, rather than the jury, and can be resolved in pretrial litigation, which has the additional benefit of allowing defendants to get a judicial resolution while still being able to enter plea negotiations, as opposed to having to go to trial to raise the defense. Finally, any concerns about disclosing classified information about terrorist recruiting practices can be addressed by requiring security clearances for defense counsel.