ARTICLE

National Security Crime

Erin Creegan*

Abstract

Although there is no shortage of attention to each of the varied threats to national security, each of these threats (and the available government responses to them) are most often treated as independent subject matters. Yet there are significant connections between these apparently distinct criminal offenses, although little work has been done to draw such connections and develop a framework for studying national security criminal law as a unified discipline. This Article takes the first step towards building such a curriculum by integrating the criminological and legal aspects of crime in the national security realm. It examines four categories of crimes—treason, espionage, sabotage, and terrorism—and the applicable federal statutes available to prosecutors to combat these threats to national security. The Article then proceeds to draw upon interdisciplinary connections across these disparate crimes to examine why individuals engage in both violent and "white-collar" national security crime. Looking at tools ranging from wiretap authorizations to classification systems, the Article addresses what the Government can do to detect, prevent, prosecute and punish national security crimes.

Introduction

Legal academics have increasingly come under two seemingly contradictory pressures: on one hand, they are compelled to harmonize, centralize, and condense the subjects they teach; on the other hand, they are

* Trial Attorney, U.S. Department of Justice, National Security Division, Counterterrorism Section; Adjunct Professor of International Criminal Law at the University of Maryland—College Park, Criminology and Criminal Justice; Adjunct Professor of Scholarly Writing in International Law at the George Washington University Law School. The opinions represented in this paper are those of the author and do not express the positions of the United States Government in any way.

Copyright © 2012 by the Presidents and Fellows of Harvard College and Erin Creegan

told to offer more highly specialized classes in order to meet a perceived demand for niche legal experts over generalists. The same dynamic exists in many areas of the modern world: in the international state system, regions create more cross-border regulation while localities seek more autonomy; in journalism, mid-level newspapers suffer while international brands thrive and local newspapers proliferate. While it is a worthy endeavor to resist over-compartmentalizing legal education, there are some notable advantages to grouping like subjects together for study. This paper proposes one way to accommodate the twin pressures to be more specialized and more interdisciplinary: it suggests the idea of a subject of "National Security Crime" that will draw on both legal and criminological concepts to analyze a family of seemingly disparate crimes united by their mutual threat to national security.

One related course already exists. In law schools across the country, the relatively new subject of "International Criminal Law" is already being taught. International Criminal Law, as it is understood today, began with the international military tribunals at Nuremberg, but only became a field of study with the creation of the United Nations International Criminal Tribunals in the 1990s. Today, the typical International Criminal Law casebook includes a wide array of topics: hybrid courts built by the cooperation of national states and the international community in the aftermath of national disasters, suppression conventions wherein countries agree to domestically combat transnational threats, the intersection of criminal law and the law of armed conflict, extradition treaties and mutual legal assistance treaties which promote "cop-to-cop" assistance, international law enforcement organizations like Interpol, and so forth. Even while the precise parameters of International Criminal Law are far from settled, the many variations on the subject are bound together by the emergent belief that cooperative use of criminal law can help states redress some of the most egregious international problems.

Indeed, what is typically grouped under the heading of International Criminal Law actually includes two distinct concepts: International Criminal Law (which addresses violations of international law perpetrated by state actors), and Transnational Criminal Law (which entails cooperation between states to tackle threats posed by more "ordinary" criminal activities, for example, terrorism, slavery, human trafficking, and organized crime). In attempting to teach a class that focused on the nexus between international concerns and criminal law, I wanted to teach an International

Criminal Law class that included three concepts: traditional International Criminal Law (Nuremberg and the international tribunals), newly emerging and rapidly growing Transnational Criminal Law (suppression conventions, extradition, transborder cooperation), and National Security Criminal Law (threats against the security of a state and its people as such, whether they come from another state or a transnational or even domestic group). As it turned out, I was totally unable to find any book, article, etc. dealing with this third type of crime, what I have called "National Security Criminal Law" and had to write an insert for a custom text book that, in some part, is a skeletal form of the article that follows.

While there are many law school classes that address the legal issues related to terrorism, nowhere does there seem to be a class—or publication for that matter—dealing with this idea of "National Security Criminal Law," a body of law that would also seem to extend to treason, espionage, disclosure of classified information à la WikiLeaks, and sabotage—alongside terrorism. Yet these concepts are closely connected, not only in their legal profiles (i.e. how they are criminalized, suppressed, tried, and punished) but also in their criminological profiles (i.e. their causes and methods of prevention), as well as the way in which law enforcement officials investigate and detect them. National Security Criminal Law should be treated as a cohesive field of study, one that goes far beyond the contemporary focus on the crime of terrorism. To address the criminological and law enforcement similarities of these (not so) disparate offenses, National Security Criminal Law must at once be compartmentalized and interdisciplinary. That is to say, it must focus on a relatively small family of offenses while, at the same, it must also import a number of insights from other disciplines in order to provide a more global view of these crimes.

With that in mind, this Article endeavors to unify the issues mentioned above under the umbrella of National Security Crime by gleaning insights from the social sciences and from the pragmatic perspective of law enforcement. It does so in the hope that "National Security Criminal Law" or "National Security Crime" may one day be taught by some of this nation's more enterprising law schools. This Article endeavors to show the relatedness of these crimes as a discrete pack of ideas, and the importance of drawing on interdisciplinary concepts in teaching any form of criminal law. I hope that this first attempt to articulate the idea of National Security Crime will be sufficient to set out the blueprint for a new class and a new unifying concept in criminal law.

First, this Article provides an extensive typology of all the offenses that fall under the rubric of National Security Crime. With this typology in place, this Article goes on to show how drawing on interdisciplinary studies can illuminate the causes, detection, prevention, and trial and punishment of national security crime to suggest a coherent and unified strategy for combating these offenses.

I. The Law

A. Treason

An analysis of national security crime must begin with the most serious of all offenses against the nation. Treason is the only crime explicitly defined in the U.S. Constitution. Article III, Section 3, "Treason," states:

> Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court.

The statutory prohibition on treason appears at 18 U.S.C. § 2381, adding to the Constitution:

> Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than $10,000; and shall be incapable of holding any office under the United States.

The crime of treason therefore has a few main elements. First, one may commit treason by supporting an enemy of the United States, or, alternatively, by undermining the United States without actually supporting with a specific enemy. Either action is sufficient. This definition includes activities of the typical turncoat, but also extends to any person or group of people rebelling or raising arms against the United States.

Second, treason has an essential mens rea component, namely, the specific intent to betray one's country.[1] This specific intent—to betray—must be proven.[2] Although difficult to prove in its own right, it is possible to show that a defendant acted with the specific intent to betray by relying on the common law inference that a person may be presumed to intend the natural consequences of his or her actions.[3] Thus, if one intends to turn coat and fight against the United States, or intends to join a rebellion against the United States, that person can be shown to have the specific intent to betray the United States. A person must owe an allegiance to the United States in order to betray the United States, but citizenship is not the only form of allegiance. In some older cases, the parameters of those who owe allegiance to the United States included domiciled aliens.[4] In a state treason case, in which the Commonwealth of Virginia tried and convicted a nonresident of Virginia for treason, Virginia courts found allegiance to be owed by any person in the territory relying on the protection of its laws.[5]

However, under the Constitution, it is not sufficient to simply levy war against the United States or to give aid and comfort to its enemies, even with the specific intent to betray the United States when allegiance is owed. There must also be an "overt act"—the third essential element of treason. The requirement of an overt act is a familiar one in criminal law; conspiracy charges frequently require not just an agreement to do an illegal act, but at least one act in furtherance by at least one member of the conspiracy. The idea is that there must be more than the mere intent to betray one's country—otherwise treason could be a simple thought crime.[6] The act itself must be directed at the objective of treason, which can be proved only one of two ways. The first is testimony by two eyewitnesses to the same overt act; one witness each to two separate overt acts will not do.[7] The second is a

---

[1] JAMES WILLARD HURST, THE LAW OF TREASON IN THE UNITED STATES 193 (Greenwood Pub. Corp. 1971) (summarizing the findings of the Supreme Court in Cramer v. United States, 325 U.S. 1, 31 (1945)).
[2] *Id.* at 205.
[3] *Id.* at 193.
[4] Carlisle v. United States, 8 Cl. Ct. 153 (1863); *In re* Charge to Grand Jury—Treason, 30 F. Cas. 1039 (D. Mass. 1861); United States v. Kawakita, 96 F. Supp. 824 (S.D. Cal. 1950).
[5] Carlton F.W. Larson, *Forgotten Constitutional Law & Enemy Combatants*, 154 U. PA. L. REV. 863, 885–88 (2006).
[6] HURST, *supra* note 1, at 205–11.
[7] *Id.* at 211.

confession given in open court.[8] A confession to police, or even to national media, would technically not suffice.

The evidentiary limits on treason are a reaction to the extensive use of charges of treason in Britain to squelch political enemies, by claiming that opposing political views were somehow unpatriotic.[9] In particular, though the U.S. Constitution's formulation of treason is verbally quite similar to the British formulation, it omits an important part. In British law, one could be found guilty of treason for "compassing the death of the king."[10] This was, essentially, a thought crime. And it could be completed a number of ways, including metaphorically, by wishing some harm to Britain.[11] Over many centuries the British used charges of treason to destroy political rivals. The Framers of the Constitution sought to limit the use of politically motivated treason trials by limiting the definition of the crime, requiring nearly impossible-to-obtain evidence, and putting their proscriptions in the Constitution, where they could not be modified by statute.[12]

Because of the combination of the hefty constitutional requirements of treason and the seeming reluctance of a democracy to punish persons for their political motives, treason indictments have been extremely limited in the history of the United States. There are cases of U.S. nationals joining foreign armies and giving other kinds of support to foreign countries during a time of war, particularly during World War II, when the United States was most active in pursing treason cases. These cases were often troublesome due to issues like dual nationality. Take for example the famous case of Tomoya Kawakita, a Japanese American dual national living in Japan at the time World War II broke out who became a translator for the Japanese. The U.S. Government accused him of visiting extreme savagery on American prisoners-of-war, and ultimately convicted him of treason and sentenced him to death.[13] President Eisenhower commuted the death sentence to life in prison. President Kennedy, however, was disturbed by the

---

[8] *Id.*
[9] *Id.* at 194.
[10] *Id.*
[11] *Id.*
[12] *See* BRADLEY CHAPIN, THE AMERICAN LAW OF TREASON: REVOLUTIONARY AND EARLY NATIONAL ORIGINS 38 (1964); HURST, *supra* note 1, at 11, 154.
[13] *See, e.g.*, Kawakita v. United States, 343 U.S. 717 (1952) (reviewing and affirming Kawakita's conviction and death sentence); *see also* David Rosenzweig, *POW Camp Atrocities Led to Treason Trial*, L.A. TIMES, Sept. 20, 2002, at 2.

implications of convicting a dual-national of Japan of treason, and so he deported Kawakita to Japan.[14]

There are also a few cases from the World War II era that concern U.S. nationals who were found to have supported enemy nations with radio shows meant to demoralize U.S. soldiers or exalt the opposing armies.[15] Examples include the famous indictments of those like Mildred Gillars or "Axis Sally," an American employed by the Third Reich to broadcast Nazi propaganda during World War II to U.S. soldiers (including talking about American mothers crying for their dead sons), Robert Henry Best and Douglas Chandler, other American citizens who became Nazi-employed English language propagandists—cases which came to collectively be known as "The Broadcast Cases."[16] Since these cases, there has been only one indictment for treason in the past sixty years: an indictment for Adam Yahiye Gadahn, an American member of al Qaeda who has created internet video programs exalting the terrorist organization and declaring that the United States should be the subject of violent attack.[17] [18] Thus the only treason indictment in the 21st century is one that follows the rationale of the Broadcast Cases. Only cases such as these seem to give the number of clear witnesses and the level of foreign allegiance necessary to meet the strict constitutional requirements for evidence of treason.

Notwithstanding the high bar posed by the evidentiary requirements of treason, the United States has been reluctant to try or punish treason

---

[14] *See id.*

[15] For more information on the famous Tokyo Rose cases, *see* RUSSELL WARREN HOWE, *The Hunt for "Tokyo Rose"* (1990).

[16] *See* Gillars v. United States, 182 F.2d 962 (D.C. Cir. 1950); Best v. United States, 184 F.2d 131 (1st Cir. 1950), *cert. denied*, 340 U.S. 939 (1950); United States v. Chandler, 72 F. Supp. 230 (D. Mass 1947), *aff'd*, 171 F.2d 921 (1st Cir. 1948), *cert. denied*, 336 U.S. 918 (1949); *see also* Cpt. Jabez W. Loane, IV, *Treason and Aiding the Enemy*, 30 Mil. L. Rev. 43, 60–66 (1965).

[17] *See* Christine Lagorio, *American Charged with Treason*, CBS NEWS (Sept. 10, 2009), http://www.cbsnews.com/stories/2006/10/11/terror/main2082055.shtml; *see also FBI Most Wanted Terrorist—Adam Gadahn* FEDERAL BUREAU OF INVESTIGATION (Oct. 11, 2006), http://www.fbi.gov/news/stories/2006/october/gadahn_101106.

[18] The idea that engaging in what would otherwise be protected First Amendment activity is prohibited when done under the employ of and to aid the enemy has traction today. In *Holder v. Humanitarian Law Project*, 130 S. Ct. 2705 (2010), the Supreme Court ruled that a law prohibiting giving "material support" to a designated foreign terrorist organization, even if that support is just helpful speech, can be outlawed. While the Supreme Court seemed to protect the right to independently express approval for a terrorist organization, they upheld the illegality of working directly for one even in a propaganda capacity.

even in cases in which proof can be established. Pardons or charges on alternate grounds addressing the violence of the crimes, rather than the political motivation to betray one's country, have been common. For example, after the 1794 Whiskey Rebellion, President George Washington pardoned all members of the rebellion in an attempt to undercut support for hardliners against the new Republic.[19] Likewise, in the aftermath of the Civil War, not a single member of the leadership of the Confederacy, nor any soldier who fought for the South, was tried or punished for treason. President Andrew Johnson issued a blanket amnesty in favor of restorative justice with the hope that the Reconstruction of the South would heal a divided nation.[20] As noted above, some of the dual nationals that faced successful treason prosecutions after World War II, the time at which treason prosecutions may have been most active, were pardoned and deported from the United States. John Walker Lindh, the American Taliban who left the United States to fight in Afghanistan and ultimately pitted himself against U.S. forces, was not tried for treason but for other crimes upon capture by the United States.[21]

B. Rebellion, Sedition, and other the Treason-related Crimes

Treason prosecutions are thus very rare. Yet treason itself is not the only crime in its genus. Chapter 115 of the United States Code, entitled "Treason, Sedition, and Subversive Activities," contains a number of related crimes. Treason appears first in the chapter as 18 U.S.C. § 2381, followed by "Misprision of treason," 18 U.S.C. § 2382, a crime punishing any person owing allegiance to the United States who knows of a treasonous plot or act of plot but does not report it. Misprision of treason is punishable by up to seven years in prison and has been punishable in the United States since the

---

[19] *See* Daniel H. Pollitt, *Presidential Use of Troops to Execute the Laws: A Brief History*, 36 N.C. L. REV. 117, 128 (1958).

[20] The utility of restorative justice versus punitive justice in cases of a high level of political violence, like that in a civil war, is still debated and explored. *See* CHRIS CUNNEEN & CAROLYN HOYLE, DEBATING RESTORATIVE JUSTICE (2010); ROSS LONDON, CRIME, PUNISHMENT, AND RESTORATIVE JUSTICE: FROM THE MARGINS TO THE MAINSTREAM (2011); MARGARITA ZERNOVA, RESTORATIVE JUSTICE: IDEALS AND REALITIES (2007); RESTORATIVE JUSTICE: POLITICS, POLICIES AND PROSPECTS (Elrena van der Spuy, Stephan Parmentier & Amanda Dissel, eds. 2007).

[21] Copies of Lindh's plea agreement and its statement of facts are publically available from the Eastern District of Virginia clerk's office and the Department of Justice's website, http://www.justice.gov/opa/pr/2002/July/02_ag_400.htm.

first meeting of the U.S. Congress—criminalized at the same time as treason,[22] but lacks any substantial use.

Rebellion or insurrection, 18 U.S.C. § 2383, comes next in this chapter of the criminal code. The provision criminalizing rebellion or insurrection reads: "Whoever incites, sets on foot, assists, or engages in any rebellion or insurrection against the authority of the United States or the laws thereof, or gives aid or comfort thereto" is subject to up to ten years in prison and is completely ineligible to hold office in the United States. This statute is a reaction to the American Civil War, and the conduct was criminalized by the Second Confiscation Act of July 17, 1862.[23] Again, the statute is largely unused.

Seditious conspiracy appears at 18 U.S.C. § 2384 and is punishable by up to twenty years in prison. The statute was passed a year earlier and also was in response to the American Civil War.[24] It proscribes two or more persons who "conspire to overthrow, put down, or to destroy by force the Government of the United States, or to levy war against them, or to oppose by force the authority thereof, or by force to prevent, hinder, or delay the execution of any law of the United States, or by force to seize, take, or possess any property of the United States contrary to the authority thereof"—a provision closely tracking what treason itself proscribes, with a focus on punishing conspiracy to commit treason; and, importantly for the modern war on international terrorism, requiring no allegiance to the United States.

Conspiracy crimes have been called the "darling of the prosecutor's nursery" by revered judge Learned Hand because of their prosecution-friendly provability.[25] Perhaps for this reason, seditious conspiracy enjoys slightly more use than the other statutes we have reviewed. The crime of seditious conspiracy was challenged in *United States v. Rahman*[26] for mimicking treason without requiring its onerous two-witness proof. The U.S. Court of Appeals for the Second Circuit summarily rejected the claim that seditious conspiracy is essentially treason by another name, a crime written expressly to get around the prosecution difficulties of treason. The

---

[22] Act of April 30, 1790, § 8, 1 Stat. 112 (1790).
[23] Ch. 195, § 2, 12 Stat. 590 (1862).
[24] Act of July 31, 1861, 12 Stat. 284.
[25] Harrison v. United States, 7 F.2d 259, 263 (2d Cir. 1925).
[26] 189 F.3d 88 (2d Cir. 1999).

court found that seditious conspiracy and treason differ not only in name and in stigma, but also in essential elements and punishment.[27] Treason is a substantive crime, whereas seditious conspiracy—like all forms of conspiracy—criminalizes the *agreement* to commit crime, but not the substantive crime itself, with the hope of interdicting the object crime before it is accomplished.

The next group, 18 U.S.C. §§ 2385–86, includes "[a]dvocating overthrow of government" and "[r]egistration of certain organizations." Both were passed in 1940 to protect the United States from a perceived threat from communist infiltrators during World War II.[28] 18 U.S.C. § 2385, known as the Smith Act, was a particularly important statute, with its own dedicated prosecution section within the U.S. Department of Justice. It provides:

> Whoever knowingly or willfully advocates, abets, advises, or teaches the duty, necessity, desirability, or propriety of overthrowing or destroying the government of the United States or the government of any State, Territory, District or Possession thereof, or the government of any political subdivision therein, by force or violence, or by the assassination of any officer of any such government; or Whoever, with intent to cause the overthrow or destruction of any such government, prints, publishes, edits, issues, circulates, sells, distributes, or publicly displays any written or printed matter advocating, advising, or teaching the duty, necessity, desirability, or propriety of overthrowing or destroying any government in the United States by force or violence, or attempts to do so; or
>
> Whoever organizes or helps or attempts to organize any society, group, or assembly of persons who teach, advocate, or encourage the overthrow or destruction of any such government by force or violence; or becomes or is a member of, or affiliates with, any such society, group, or assembly of persons, knowing the purposes thereof—

---

[27] *Id.* at 112.

[28] Section 2385 appeared at 54 Stat. 670–71. Section 2386 was passed October 17 at 54 Stat. 1201–04.

> Shall [be subject to up to twenty years in prison] and shall be ineligible for employment by the United States or any department or agency thereof, for the five years next following his conviction.

Conspiracy to do the same is also prohibited and subject to the same penalties under the section.

The Smith Act precipitated one of the few periods in U.S. history where politically-motivated crimes were zealously prosecuted. Due to a perceived threat from communism, which was growing and overturning societies (from the American public's perspective) all over the world, there was a public cry for protection from communist organizations before America became the target of communist organizations.[29] This included the prosecution of dozens of Socialist Workers Party members and teamsters unions members in Minneapolis in 1941,[30] and trials of over 100 Communist Party leaders in the U.S. beginning in 1949—including legendary communist leader Eugene Dennis.[31] However, as the fervor of this period died down and things like "McCarthyism" came and went in shame, the courts started to limit the application of the provision.[32] In *Yates v. United States*, the U.S. Supreme Court ruled that the First Amendment protects radical and reactionary speech, unless such speech presents "a clear and present danger " of imminent incitement.[33] In *Scales v. United States*, the Supreme Court found that the Smith Act should not be interpreted to proscribe mere membership in a radical or violent organization, but required active membership with knowledge and work to achieve the illegal aims of such a group.[34] Such decisions show how First Amendment considerations in the United States could make us culturally reluctant to use criminal statutes that rely on political motives.

The criminal provision following the Smith Act, 18 U.S.C. § 2386, prescribes a related but much less utilized offense requiring certain organizations to register with the Attorney General, including political

---

[29] For more on the historical conditions precipitating the Smith Act, *see* MICHAL R. BELKNAP, COLD WAR POLITICAL JUSTICE, 9–34 (1977).
[30] Dunne v. United States, 138 F.2d 137 (8th Cir. 1943), *cert. denied*, 320 U.S. 790 (1943).
[31] *See generally* Robert Mollan, *Smith Act Prosecutions: The Effect of the Dennis and Yates Decisions*, 26 U. PITT. L. REV. 705 (1965).
[32] *See id.*
[33] 354 U.S. 298, 303 n.2 & 320 (1957).
[34] 367 U.S. 203, 222 (1961).

organizations subject to foreign control, organizations with both political activity and civilian military activities, and organizations which advocate the violent overthrow of the government. Although § 2386 was passed shortly after the Smith Act, it never became a favored prosecutorial tool.

The next grouping of related concepts in Chapter 115 includes 18 U.S.C. §§ 2387–88: "[a]ctivities affecting armed forces generally" and "[a]ctivities affecting armed forces during war." Section 2388 was first passed during World War I as the Espionage Act of 1917.[35] The main purpose of this part of the act appears to be to criminalize the acts of aliens who owe no allegiance to the United States that might interfere with U.S. forces.[36] These crimes, like seditious conspiracy, also withstood challenges that they too tried to punish treason by another name, outside of treason's strict constitutional requirements.[37]

Section 2388 forbids willfully making or conveying false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies; or willfully causing or attempting to cause insubordination, disloyalty, mutiny, or refusal of duty, in the military or naval forces of the United States; or willfully obstructing or attempting to obstruct the recruiting or enlistment service of the United States, to the injury of the service or the United States; as well as conspiracy to do any of the above. All these acts are punishable by up to twenty years. Harboring a person committing the acts in this section is also punishable by up to ten years.

Section 2387 was codified during World War II along with the Smith Act.[38] Section 2387 proscribes, with the intent to interfere with, impair, or influence the loyalty, morale, or discipline of the military or naval forces of the United States, advising, counseling, urging, or in any manner causing or attempts to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the military or naval forces of the United States; or distributing or attempting to distribute any written or printed matter which advises, counsels, or urges insubordination, disloyalty, mutiny, or refusal of duty by any member of the military or naval forces of the United States. The offense is punishable by up to ten years in prison and

---

[35] Act of June 15, 1917, 40 Stat. 219, § 217, 3–8.
[36] Lockhart v. United States, 264 F. 14 (6th Cir. 1920).
[37] Wilmer v. United States, 264 U.S. F. 11 (6th Cir. 1920).
[38] 18 U.S.C. § 2385 (2012).

ineligibility for employment by the United States for the next five years. These penalties are less severe than those listed in § 2388, proscribing similar acts against the armed forces during a time of war, given the greater national security threat of such activities during active hostilities.

The last part of Chapter 115, 18 U.S.C. §§ 2389–90, is the most underutilized, with no real uses.[39] Both provisions were set into law by the same Civil War-era statute,[40] illuminating that every provision in Chapter 115 is a response to wartime—either the American Revolutionary War, the American Civil War, World War I, or World War II—and therefore not just wartime, but the most important wars and those that were most threatening to the continued existence of the United States. Title 18 U.S.C. § 2389, Recruiting for service against United States, penalizes recruiting "soldiers or sailors within the United States, or in any place subject to the jurisdiction thereof, to engage in armed hostility against the same"; or opening "within the United States, or in any place subject to the jurisdiction thereof, a recruiting station for the enlistment of such soldiers or sailors to serve in any manner in armed hostility against the United States." The penalty is up to five years. The next provision, and last of the chapter, is 18 U.S.C. § 2390: Enlistment to serve against United States. It provides that "[w]hoever enlists or is engaged within the United States or in any place subject to the jurisdiction thereof, with intent to serve in armed hostility against the United States, shall be fined under this title or imprisoned not more than three years, or both."[41]

While treason is an evocative and important criminal concept, it appears rarely in the United States history. The codification of the most important treason-related crimes appears to follow dramatic wars and conflicts in U.S. history. Possible topics for future study include why many of these treason-related crimes are so rarely used—because of the strong First Amendment protections for political thought in the United States, as I have suggested? Another reason? Another topic for study might be whether these crimes should be used more and whether criminal law can be helpful to advancing national security purposes in the areas Congress has chosen. Should new criminal offenses be invented, or should current offenses be modified to make them more useful? Are traitors being tried for lesser

---

[39] *See In re* Charge to Grand Jury, 30 F. Cas. 1036 (CCSD Ohio 1861).
[40] Act of August 6, 1861, 12 Stat. 317.
[41] 18 U.S.C. § 2390 (2012).

crimes to avoid the two-witness rule? Is there normative value to calling a person a traitor and achieving a hard won conviction on a treason-related crime?

C. Espionage

Perhaps one of the next most iconic types of national security crime is that of espionage. Espionage is generally considered the theft or exploitation of national defense information.[42] It is a relatively common way in which individual acts directed against the national security of the United States are committed, and therefore, espionage laws are some of the more utilized national security criminal laws. Espionage is forbidden in a few parts of the U.S. Code. From 18 U.S.C. § 793, entitled "Gathering, transmitting or losing defense information":

> (a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation [obtains information]; or
>
> (b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or
>
> (c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives

---

[42] The British Security Service defines espionage as "a process which involves human sources (agents) or technical means to obtain information which is not normally publically available. It may also involve seeking to influence decision makers and opinion-formers to benefit the interests of a foreign power." *What is Espionage?*, SECURITY SERVICE: MI5, https://www.mi5.gov.uk/output/what-is-espionage.html (last visited June 9, 2012).

or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense,

> (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or
> (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—
>
> Shall be fined under this title or imprisoned not more than ten years, or both.

A more serious provision, in which the person actually transmits defense information to a foreign government, is located in 18 U.S.C. § 794, entitled "Gathering or delivering defense information to aid foreign government":

> (a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or, if there is no jury, the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning

> systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.
>
> (b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

And finally, in 18 U.S.C. § 798, "Disclosure of classified information":

> (a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—
>
> (1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or
> (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
> (3) concerning the communication intelligence activities of the United States or any foreign government; or

> (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—
>
> Shall be fined under this title or imprisoned not more than ten years, or both.

Other, more specific acts of espionage, such as photographing or sketching defense installations,[43] are also criminalized in the remaining portions of Title 18, Chapter 37.

1. Disclosure of Classified Information

Chapter 37 addresses espionage for the purposes of aiding an enemy or levying war against the United States (i.e. the movement of classified information against a state's interest in the context of interstate relations). Yet there are other movements of classified information that can undermine national security without creating a conflict between states. While the statutes above mostly contemplate interstate war and security of information from state enemies, there are other threats in the disclosure of classified information. This could include the mass disclosure of protected government information in the Pentagon Papers and WikiLeaks episodes.

The Pentagon Papers involved the disclosure of classified reporting about the "real" war in Vietnam, including a number of things the U.S. Government had misrepresented to the public. The leaker of the Pentagon Papers was not successfully prosecuted (charges against the leaker being dismissed for gross governmental misconduct in the course of the prosecution), and the New York Times, which published the story, was not prosecuted but instead seen as shielded by the journalistic protections of the First Amendment.[44] There was, and is still, a great deal of public support for the disclosure.

More recently, WikiLeaks, a journalistic website that had previously been praised for revealing various counts of government misconduct,[45]

---

[43] 18 U.S.C. § 795 (2012).

[44] *See generally* INSIDE THE PENTAGON PAPERS (John Prados & Margaret Pratt Porter, eds. 2005).

[45] *Winners of Index on Censorship Freedom of Expression Awards Announced*, INDEX ON CENSORSHIP (Apr. 22, 2008), http://www.indexoncensorship.org/2008/04/winners-of-index-on-

published thousands of diplomatic cables that merely embarrassed the United States and undermined cooperative diplomatic relations abroad.[46] Though intended to reveal governmental misconduct in the Iraq War, the disclosed materials instead showed that there were no real secret aspects to the war in Iraq, and that the U.S. Government had been largely forthcoming, or already exposed by the normal operation of the press, regarding the events of the war.[47] Public support for the perpetrators of the WikiLeaks classified information dump has been much weaker, as many believe that those who published the information had unnecessarily put the United States in danger by revealing the information.[48]

2. The Other Espionage Crimes

The espionage prosecutions in the United States are coordinated by the Counterespionage Section (CES) within the National Security Division of the Department of Justice, cooperating with the local U.S. Attorney's Office for the federal district that has jurisdiction over the crime. The Counterespionage Section's work includes not only prosecuting the offenses listed above, but also additional and related duties more tangential to traditional espionage. The typical view of espionage is that of a foreign agent clandestinely working to steal defense technologies and secrets. Other crimes that CES prosecutes include those targeting those agents and their presence in the United States, preserving good diplomatic relations with friendly countries, protection of weapons, and preservation of U.S. pioneering technologies. Some of the most important duties of the Counterespionage Section are ensuring the registration of foreign agents operating in the United States, which is intended to make it more difficult for foreign agents to engage in espionage, and the protection of U.S.

---

censorship-freedom-of-expression-award-announced; *The Cry of Blood. Report on Extra-Judicial Killings and Disappearances*, KENYA NATIONAL COMMISSION ON HUMAN RIGHTS (Sept. 2008), http://www.ediec.org/library/item/id/402/; Press Release: Amnesty announces Media Awards 2009 Winners, AMNESTY INTERNATIONAL UK (June 2, 2009), http://amnesty.org.uk/news_details.asp?NewsID=18227.

[46] Praveen Swami, *Wikileaks: Cables Will Embarrass, but Won't Cause Diplomatic Meltdown*, TELEGRAPH, (Nov. 29, 2010), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8169019/Wikileaks-cables-will-embarrass-but-wont-cause-diplomatic-meltdown.html.

[47] *See Wikileaks's Leaks Mostly Confirm Earlier Iraq Reporting*, WASH. POST (Oct. 26, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/10/25/AR2010102504643.html.

[48] *Pew Survey: Public Views WikiLeaks Document Release as Harmful*, CBS NEWS (Dec. 8, 2010), http://www.cbsnews.com/8301-503544_162-20025074-503544.html.

national defense technologies, particularly if related to atomic energy. These different responsibilities of CES, all related to protecting the national security of the United States in terms of relationships with other states, are explored below.

a. Foreign Agents and Diplomatic Relations

The relevant prohibitory provision of the Foreign Agents Registration Act (FARA),[49] 22 U.S.C. § 612, the "Registration statement," reads, in part:

> (a) Filing; contents
> No person shall act as an agent of a foreign principal unless he has filed with the Attorney General a true and complete registration statement and supplements thereto as required […].

While the FARA was not intended to be used against U.S. nationals (those in the best position to steal national defense technologies) and is more often used against diplomatic personnel and representatives to the United States from foreign governments, it is an interesting anti-spying statute. This law does not address spying directly, but tries to criminalize the factual situations that create the opportunity for a person to function as a spy, so that a would-be spy, if he or she is discovered, can be arrested and stopped before any damage is done. The FARA has enjoyed some recent attention due to the "Russian Spy" cases in the summer of 2010.[50] A number of deep-cover agents of the Russian government were living in the United States for extended periods of time, purportedly to gain information about U.S. culture and political attitudes, and not trying to access classified information directly.[51] They were indicted under FARA-like provision 18 U.S.C. § 951.

---

[49] For more information on the FARA, *see* THE REGISTRATION OF FOREIGN AGENTS IN THE UNITED STATES: A PRACTICAL AND LEGAL GUIDE (Joseph E. Pattison & John L. Taylor, eds. 1981).

[50] *See, e.g.*, Jason Ryan & Megan Chuchmach, *Russian Spy Ring Suspects Busted! 10 Alleged Secret Agents Arrested in U.S.*, ABC NEWS (June 28, 2010), http://abcnews.go.com/Blotter/russian-spy-ring-10-accused-russian-spies-arrested/story?id=11037360#.T7QOFZ9YvIY.

[51] *See Ten Alleged Secret Agents Arrested in the United States*, U.S. DEP'T OF JUSTICE, (June 28, 2010); http://www.justice.gov/opa/pr/2010/June/10-nsd-753.html. *See also* Complaints 1 & 2, attached to the Press Release (detailing the discovery and activities of the Russian agents). In particular, the complaints show the use of new computer technologies to transfer information between the Russian government and its agents. The traditional method of

The maximum penalty for a violation of FARA is five years in prison.[52] This relatively low sentence may reflect two things about the statute: (1) that it is primarily prophylactic and aimed at preventing more serious crime—once a foreign agent is discovered, it is generally about as helpful to jail him or her as it is to simply deport him or her, and (2) the offender is generally not a traitor. FARA violations rarely involve betrayal of trust by a U.S. Government employee, soldier, or other citizen. Foreign agents have been ordered to undertake a mission in the United States. The offense is more diplomatic in nature, an offense by the government that sent the unregistered agent. The more appropriate solution may thus reasonably be for the unregistered agents to be returned to their country as *persona non grata* [53] in the United States, which is what is done when diplomats commit serious crimes, and for the offending nation to make amends with the United States.

More diplomacy, foreign affairs, and pseudo-espionage related offenses can be found in Chapter 45 of Title 18: "Foreign Relations." These offenses may target espionage from another angle, or just try to keep good relations with other states. They might also seek to protect neutrality in a time of war—while espionage protects defense capabilities in times of conflict, these peace-related provisions may protect the safe position of neutrality. Prohibitions include:

- § 951. Agents of foreign governments (the actual charge of the Russian Spy cases, requiring registration, carrying up to ten years incarceration)

- § 952. Diplomatic codes and correspondence (prohibiting a U.S. employee's interference with diplomatic communication, carrying up to ten years incarceration—a potential charge in future WikiLeaks-esque crimes?)

---

passing information, shown in the Hanssen case, was by "dead-drops"—leaving physical copies of the information in a mutually agreed place. The "Russian spy" cases may show that espionage is becoming more technological, but it may also show that low-tech methods are still the hardest to detect.

[52] 22 U.S.C. § 618(a)(2) (2012).

[53] *Persona non grata* is Latin for "an unwelcome person." It most often refers to the right of a country to expel and ban a diplomat from reentering the country after he or she has committed a serious offense, which, because of diplomatic immunity, cannot be prosecuted.

- § 953. Private correspondence with foreign governments (U.S. citizen communication with a foreign government to the detriment of the United States, carrying up to three years incarceration)

- § 954. False statements influencing foreign government (similar to the previous section, except the substance of the communications is false, carrying up to ten years incarceration)

- § 955. Financial transactions with foreign governments (doing business with a government who is in default on financial obligations to the United States, carrying up to five years incarceration)

- § 956. Conspiracy to kill, kidnap, maim, or injure persons or damage property in a foreign country (carrying varying levels of punishment depending on the object of the crime)

- § 957. Possession of property in aid of foreign government ("knowingly and willfully possess[ing] or control[ing] any property or papers used or designed or intended for use in violating any penal statute, or any of the rights or obligations of the United States under any treaty or the law of nations"—carrying up to ten years incarceration)

- § 958. Commission to serve against friendly nation (exactly as it sounds, a provision criminalizing "accept[ing] and exercise[ing] a commission to serve a foreign prince, state, colony, district, or people, in war, against any prince, state, colony, district, or people, with whom the United States is at peace"—carrying up to three years incarceration)

- § 959. Enlistment in foreign service (if doing so from the territorial United States; it is not a crime to travel to another country to enlist once there—carrying up to three years incarceration)

- § 960. Expedition against friendly nation (carrying up to three years incarceration)

- § 961. Strengthening armed vessel of foreign nation (augmenting forces of foreign armed force at war with a country that the United States is at peace with—carrying one year of incarceration)

- § 962. Arming vessel against friendly nation (augmenting forces to commit hostilities against friendly nation of the United States—punishable by three years incarceration)

- § 963. Detention of armed vessel (authorizing the President to, in times of U.S. neutrality, detain vessels capable of participating in a war effort until satisfied they will remain neutral, and criminalizing anyone who attempts to take them out of port in such a case by up to three years incarceration)

- § 964. Delivering armed vessel to belligerent nation (ten years)

- § 965. Verified statements as prerequisite to vessel's departure (ten years)

- § 966. Departure of vessel forbidden for false statements (ten years)

- § 967. Departure of vessel forbidden in aid of neutrality (ten years)

- § 970. Protection of property occupied by foreign governments:

> (a) Whoever willfully injures, damages, or destroys, or attempts to injure, damage, or destroy, any property, real or personal, located within the United States and belonging to or utilized or occupied by any foreign government or international organization, by a foreign official or official guest, shall be fined under this title, or imprisoned not more than five years, or both.
>
> (b) Whoever, willfully with intent to intimidate, coerce, threaten, or harass—
> (1) forcibly thrusts any part of himself or any object within or upon that portion of any building or premises located within the United States, which portion is used or occupied for official business or for diplomatic, consular, or residential purposes by—

> (A) a foreign government, including such use as a mission to an international organization;
> (B) an international organization;
> (C) a foreign official; or
> (D) an official guest; or
> (2) refuses to depart from such portion of such building or premises after a request—
> (A) by an employee of a foreign government or of an international organization, if such employee is authorized to make such request by the senior official of the unit of such government or organization which occupies such portion of such building or premises;
> (B) by a foreign official or any member of the foreign official's staff who is authorized by the foreign official to make such request;
> (C) by an official guest or any member of the official guest's staff who is authorized by the official guest to make such request; or
> (D) by any person present having law enforcement powers;
> shall be fined under this title or imprisoned not more than six months, or both.

Other diplomatic crimes outside of Chapter 45 might include 18 U.S.C. § 112: Protection of foreign officials, official guests, and internationally protected persons; 18 U.S.C. § 878: Threats and extortion against foreign officials, official guests, or internationally protected persons; 18 U.S.C. § 1116; Murder or manslaughter of foreign officials, official guests, or internationally protected persons, and 18 U.S.C. § 1201(a)(4): Kidnapping, when the person is a foreign official, an internationally protected person, or an official guest as those terms are defined in § 1116.

b. Weapons

If the criminalization of espionage is aimed at protecting national defense information, then sensitive weapons technologies, some of the most critical portions of national defense information, must be protected from disclosure. The other side of the Counterespionage Section's work, away from foreign relations issues, is export controls on sensitive and potential weapon-use technologies. It is in export controls that CES does most of its work. The most dangerous technology protected is nuclear technology. The

relevant prohibition of the Atomic Energy Act appears in 42 U.S.C. § 2122, "Prohibitions governing atomic weapons":

> (a) It shall be unlawful, except as provided in section 2121 of this title, for any person, inside or outside of the United States, to knowingly participate in the development of, manufacture, produce, transfer, acquire, receive, possess, import, export, or use, or possess and threaten to use, any atomic weapon. [...]

There are also some prohibitions in other sections of the United States Code, 42 U.S.C. §§2274–77, that ban the communication, receipt, tampering, and disclosure of restricted data about atomic energy.

Other export control crimes include those listed under the Arms Export Control Act of 1976, 22 U.S.C. ch. 39 (AECA), which provides comprehensive regulation, including criminal penalties, for protecting defense technologies from export. The AECA confers authority on the President to control the import and export of defense goods and services. The AECA puts the onus on American arms manufacturers and dealers to comply with certain best practices that will prevent weapons materials from falling into the wrong hands, including verification of buyers and documentation of sales. Other parts of Title 22 also proscribe movement of defense technologies, including 22 U.S.C. § 401: "Illegal exportation of war materials"; but the AECA is the most commonly used statute for weapons trading prosecutions, and probably CES's most commonly used basis for prosecution overall.[54]

Other common provisions for CES prosecutions include those of the International Emergency Economic Powers Act of 1977 (IEEPA), 50 U.S.C. §§ 1701–07, which is a flexible set of statutes allowing the President to regulate commerce after declaring a national emergency in response to any unusual and extraordinary threat to the United States which has a foreign source. The President can designate a country or organization and thus block trade with that country or organization, as well as freeze assets of the

---

[54] *See generally* U.S. Dep't. of Justice, Interim Response to FOIA/PA #09-037 (July 27, 2009), *available at* http://www.judicialwatch.org/files/documents/2009/480_DOJ_NSD_chinaexports_interim_7_2009.pdf (describing prosecutions for export control violations between 2003 and 2009).

country or organization. The trade need not be weapons-related (though as a practical matter, it often is). Thus this statute is one of the most important, and complex, statutes used to suppress international weapons dealings.

The Export Administration Act of 1979 (EAA) and its attendant regulations are also common CES prosecutions.[55] The EAA allows the President some control over exports in cases of national emergency or foreign policy, including short supply of essential materials. AECA, IEEPA, and EAA are the most commonly prosecuted cases of the Counterespionage Section, unlike the other charges reviewed in this section of this paper.

Also important, there are criminal prohibitions on trade or use or development of highly destructive weapons like weapons of mass destruction, including "CBRN"—chemical, biological, radiological, and nuclear weapons. There are chapters of the U.S. Code that proscribe chemical (Chapter 11B of Title 18) and biological (Chapter 10 of Title 18) weapons specifically.

c. Technology

Recently, "economic espionage"—the spying of foreign agents on American businesses for trade secrets, has become more of a national security priority.[56] This subject is not treated extensively here, and is not handled by the Counterespionage Section, but by the Department of Justice's Computer Crime and Intellectual Property Section.[57] The statute, 18 U.S.C. § 1831, "Economic espionage," reads:

> (a) In General.— Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

---

[55] *Id.*

[56] *The FBI's National Strategy for Counterintelligence: A Primer*, FEDERAL BUREAU OF INVESTIGATION (May 31, 2005), http://www.fbi.gov/page2/may05/ciprimer053105.htm.

[57] *See, e.g., Chinese National Charged with Economic Espionage Involving Theft of Trade Secrets from Leading Agricultural Company Based in Indianapolis*, U.S. DEP'T OF JUSTICE, (Aug. 31, 2010), http://www.justice.gov/opa/pr/2010/August/10-crm-983.html.

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.
>
> (b) Organizations.— Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

D. Sabotage

Treason, espionage, disclosure of classified information, spying, and trading in weapons technology may be some of the crimes that come most readily to mind when one thinks of national security crimes (of course along with terrorism). Yet there is another category of offenses which I believe constitute an entirely distinct class: destructions of things or people who contribute to the U.S. Government's proper functioning or continued existence. This subsumes assassinations and all other attacks on government personnel, facilities, instrumentalities, and vital infrastructure. These crimes belong to a single genus, even though they have yet to perhaps be considered a group of related crimes, and do not come under a common heading, not in the U.S. Code nor in supervision of prosecution at the Department of Justice. They should be considered a part of our typology of "Sabotage" since they all attempt to strike at national security by

undermining its vital instrumentalities. Most of these statutes appear in Chapters 18 and 84 (attacks on government personnel) and Chapter 105 (Sabotage), but others are scattered throughout the U.S. Code (such as crimes relating to attacks on government facilities).

Assassination and kidnapping crimes that strike at the country's leadership are some of the foremost Sabotage crimes. Chapter 18 contains a single statute, 18 U.S.C. § 351, which prohibits "Congressional, Cabinet, and Supreme Court assassination, kidnapping, and assault." Chapter 84 has two criminal statutes: 18 U.S.C. § 1751, which prohibits "Presidential and Presidential staff assassination, kidnapping, and assault," and 18 U.S.C. § 1752, which prohibits interfering with or flouting security protocols at "Restricted buildings and grounds" when restricted for the security of the President.

Together these statutes protect the leadership of the country in order to preserve continuity of government and ensure that the nation is not suddenly decapitated and unable to function in its security interest. Assassinations and attempted assassinations are common throughout history, either motivated by politics (such as one orchestrated by an enemy country or terrorist organization), or the general insanity or nihilism of the offender. Around the turn of the 20th century, anarchists often succeeded in accomplishing semi-political, semi-nihilistic attacks on heads of state, called "propaganda by deed." Successful hits include the French president in 1894, the empress of Austria in 1897, the Spanish prime minister in 1897, the king of Italy in 1900, and U.S. President McKinley in 1901. One need only examine the immediate cause of World War I to discover how vital preventing assassination may be to the national interest.

Title 18 U.S.C. § 1114, Protection of officers and employees of the United States, provides jurisdiction for protection of other government employees, including rank and file.

> Whoever kills or attempts to kill any officer or employee of the United States or of any agency in any branch of the United States Government (including any member of the uniformed services) while such officer or employee is engaged in or on account of the performance of official duties, or any person assisting such an officer or employee in the

> performance of such duties or on account of that assistance, shall be punished—
> (1) in the case of murder, as provided under section 1111 [maximum punishment being death];
> (2) in the case of manslaughter, as provided under section 1112 [maximum punishment being 15 years]; or
> (3) in the case of attempted murder or manslaughter, as provided in section 1113 [maximum punishment being 20 years for murder or 7 for manslaughter].

While perhaps not as dangerous to national security as the sudden loss of state leadership, the government's effectiveness relies on the protection of its workforce from being targeted for sabotage.

Chapter 105, "Sabotage" contains five criminal prohibitions, mostly relating to interfering with defenses during a time of war: including interfering with Fortifications, harbor defenses, or defensive sea areas (18 U.S.C. § 2152), Destruction of war material, war premises, or war utilities (18 U.S.C. § 2153), Production of defective war material, war premises, or war utilities (18 U.S.C. § 2154), Destruction of national-defense materials, national-defense premises, or national-defense utilities (18 U.S.C. § 2155), and Production of defective national-defense material, national-defense premises, or national-defense utilities (18 U.S.C. § 2156). The idea of the crime of sabotage comes from wartime conduct directed against the national war effort. Such conduct has been proscribed not only by domestic law but also the international law of armed conflict, which does not grant spies or saboteurs prisoner of war status if captured. Rather, they are referred to military criminal prosecution.[58]

Other statutes that should be placed under the heading of sabotage might include some of the Chapter 65 "Malicious Mischief" crimes: 18 U.S.C. § 1362: Communication lines, stations or systems (attacks on); § 1363: Buildings or property within special maritime and territorial jurisdiction (attacks on); § 1365: Tampering with consumer products; § 1366: Destruction of an energy facility; § 1367: Interference with the operation of a satellite; or even § 1368: Harming animals used in law enforcement. Other candidates include crimes like 18 U.S.C. § 1992: Wrecking trains, or § 2101: Riots, or 42 U.S.C. § 2284: Sabotage of nuclear

---

[58] *See* Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 5, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

facilities or fuel. The genus of sabotage crimes might also include 18 U.S.C. § 2332f, Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities—a crime that actually appears in the Terrorism chapter of Title 18. Together these crimes cover activities generally directed to undermining the infrastructure of the United States.

There are also many other kinds of crimes that could be considered national security crimes in the sense that they affect the security of the state, its people, and its facilities, including counterfeiting, passport or immigration fraud, or fraud in other government documents. These crimes may form a periphery of what we consider to be national security crime of the kind in this section, sabotage crimes like assassination or the bombing of government property. They undermine the proper functioning of the U.S. Government and its instrumentalities, but in more of a nuisance manner than a destructive one, and often with purposes not related to national security.

Perhaps even the disclosure of classified information a la WikiLeaks is more appropriately classified as "Sabotage" than it is "Espionage," if indeed those actors intended to disclose protected information, but not really information pertaining to the national defense. Perhaps they were simply trying to "take down" the reputation of the United States—more of a sabotage-style goal. Such an example might show the conceptual difficulty of putting clear lines around the typology of crimes that this paper suggests: treason, espionage, sabotage, and terrorism. Of course such concepts can and necessarily do somewhat overlap, but may still provide a helpful typology for studying the creation, use, and application of like criminal statutes.

E. Terrorism

Terrorism is generally thought of as the use of violence against civilian targets when committed with a political motive.[59] Texts, articles, and even law school courses are dedicated to the legal regime surrounding terrorism. Unlike some of the crimes discussed above, information about

---

[59] For more on the longstanding debate surrounding the definition of terrorism, *see* BEN SAUL, DEFINING TERRORISM IN INTERNATIONAL LAW (2008), and Nicholas J. Perry, *The Numerous Federal Legal Definitions of Terrorism: The Problem of Too Many Grails*, 30 J. LEGIS. 249 (2004).

terrorism crimes is abundant—so this section is brief. Terrorism is a roving concept that is not confined solely to criminal law, but also touches on military law, the law of armed conflict, intelligence law, and other areas. Perhaps because of its discursive nature, terrorism does not neatly fit into any division of crimes relating to international system—it could be classified under International Criminal Law, Transnational Criminal Law, or, as I argue, National Security Criminal Law.

A good starting point for any course or text on National Security Criminal Law is the American laws that criminalize terrorist acts. Many of these laws are contained in Chapter 113B of the U.S. Code under the heading "Terrorism." This chapter contains two different approaches to terrorism: the pre-9/11 or pre-Patriot Act approach, and the post-9/11 or post-Patriot Act approach. The distinction has less to do with *when* the laws were passed—all of the crimes in the terrorism subchapter were enacted between 1988 and 2004—than it does with *how* these laws are used by prosecutors.

Sections 2332–39 represent the pre-9/11 approach, criminalizing the Use of weapons of mass destruction (18 U.S.C. § 2332a), Acts of terrorism transcending national boundaries (18 U.S.C. § 2332b), certain Financial transactions (18 U.S.C. § 2332d), Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities (18 U.S.C. § 2332f), use of Missile systems designed to destroy aircraft (18 U.S.C. § 2332g), Radiological dispersal devices (18 U.S.C. § 2332h), and Harboring or concealing terrorists (18 U.S.C. § 2339). These offenses target a method or tactic that is commonly used by terrorists, not "terrorism" itself.

By contrast, the post-Patriot Act statutes deliberately target terrorists as terrorists, not merely the use of terrorist tactics. Indeed, they to interdict would-be terrorists before they employ their dangerous tactics. These statutes, 18 U.S.C. §§ 2339A, 2339B, 2339C, and 2339D prohibit: the provision or material support to terrorists or designated terrorist organizations, the financing of terrorism, and the receipt of military-type training from a foreign terrorist organization. These charges—§ 2339A and § 2339B particularly—have become far and away the most commonly used by the Department of Justice to fight terrorist crime—comprising 71% of all

terrorism cases.[60] It may be hard to say which approach works best in the long run, and it may be that a combination works best for the United States. However, the relative success of law enforcement in preventing any major terrorist plot from coming to fruition since 9/11 tends to show the importance of utilizing criminal statutes designed for interdiction.

The Counterterrorism Section (CTS) of the Department of Justice is responsible for coordinating the federal effort to interdict, incapacitate, prosecute, and punish terrorists through the use of domestic criminal law.[61] To this end, the Counterterrorism Section typically relies on the following statues (some of which were discussed above, while others, though not technically "terrorism statutes," are still used to combat terrorism):

- aircraft piracy and related offenses (49 U.S.C. §§ 46501-07)
- aircraft sabotage (18 U.S.C. § 32)
- crimes against immediate family members of all federal officials (18 U.S.C. § 115) and against internationally protected persons (18 U.S.C. §§ 112, 878, 1116, 1201(a)(4))
- sea piracy (18 U.S.C. § 1651)
- hostage taking (18 U.S.C. § 1203)
- terrorist acts abroad against United States Nationals (18 U.S.C. § 2332)
- acts of terrorism transcending national boundaries (18 U.S.C. § 2332b)
- conspiracy within the United States to murder, kidnap, or maim persons or to damage property overseas (18 U.S.C. § 956)
- provision of material support to terrorists and terrorist organizations (18 U.S.C. §§ 2339A, 2339B, 2339C, 2339D)
- use of biological, nuclear, chemical or other weapons of mass destruction (18 U.S.C. §§ 175, 831, 2332c, 2332a)

---

[60] CENTER ON LAW AND SECURITY, NEW YORK UNIVERSITY SCHOOL OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2008 6 (Sept. 11, 2008), *available at* http://www.lawandsecurity.org/publications/Sept08TTRCFinal.pdf ("Overall, the two material support charges account for 71% of all convictions under the core terrorism statutes, while terrorist acts or conspiracy to commit terrorist acts (18 U.S.C. [§] 2332) account for only 10% of those convictions.").

[61] U.S. DEPARTMENT OF JUSTICE, COUNTERTERRORISM SECTION, http://www.justice.gov/nsd/counter_terrorism.htm (last visited June 9, 2012).

- genocide (18 U.S.C. § 1091), war crimes (18 U.S.C. § 2441), torture (18 U.S.C. § 2340A)[62]

Some of these offenses clearly include the assorted national security offenses mentioned in the last section that can be a tactic to commit a national security crime but are not necessarily national security related in nature (such as hostage-taking, which can also be similar to simple domestic kidnapping, or attacks on internationally protected persons, i.e., diplomats, which is not necessarily a terrorism-related attack). The offense also include crimes related to terrorism which have no other home for enforcement within another section of the Department of Justice (such as proscriptions on piracy). However, the pre- and post-9/11 crimes are also clearly represented.

Treason, espionage, sabotage, and terrorism are overlapping concepts, but form four basic categories of national security crime. With our main typology formed (but not overly committed to), we are ready to consider a criminology and pragmatic law enforcement approach to national security crime.

II. Causes

What causes a person to engage in espionage or treason, or to sell weapons to a rogue nation? Or to be a rogue saboteur or assassin, or to join a terrorist organization? After studying our typology above, it is possible to detect a dichotomy between the types of criminals likely to commit such offenses. First, there are the professional, or what we might loosely term the "white collar" national security criminals, namely, trained spies, weapons dealers, financial and administrative sponsors of terrorism. Second, there are the "violent" criminals, those who wage war on the United States by bombing government facilities, assassinating officials, or taking hostages. This may be a crude division, but separating professionalized criminals from radical users of violence will help strengthen our understanding of national security crime. By evaluating these two types of crime, we can divine related causes and potentially strengthen our ability to interdict and deter national security crime. This area of study in particular is an excellent one for criminological insights to bolster our study of national security crime.

---

[62] *Id.*

Espionage and terrorism are not only the most studied types of national security crime, but they also the only types of national security crime to which the Justice Department dedicates separate prosecutorial sections within the National Security Division. Therefore they are the easiest to explore. Espionage and terrorism are both studied below for examples of professionalized or white collar crime and violent or radicalized crime.

A. Organized, Professional, or "White Collar" National Security Crime

Despite the significance and long history of the crime of espionage, the legal and criminological profile of how espionage crimes are committed and tried is not well-publicized. There may well be great research by counterintelligence officials that is simply not available for public consumption.[63] Many of the details regarding how these crimes are actually perpetrated and how they may be detected are understandably not public information. This paper looks to the publicly available details of past cases, and other public information to paint a non-classified picture of these crimes.

Espionage cases are extremely infrequent, which makes general trends hard to discern and prosecutions hard to predict. For example, while many people will have financial problems, most will not turn to selling state secrets, so the fact that many spies are paid is not easily reverse engineered to come up with a list of persons who are "susceptible" to taking a bribe for committing espionage. And it is also hard to place screening mechanisms in place that will not have massively disproportionate costs, such as monitoring all documents that employees copy at work and what documents they take home in the evening. Yet attention must nevertheless be paid to what the causes of espionage are so that potential forms of preventing and detecting these crimes can be put in place.

Though the causes of national security crime are rarely studied, there is some scholarship and some conjecture about what drives a person to spy. During the Cold War, intelligence and counterintelligence operations

---

[63] For example, *see* Lynn F. Fischer & John E. Leather, ESPIONAGE INDICATORS 1985-2005: A REVIEW OF CLASSIFIED DATA SOURCES (2007) (classified Secret). *See also* KATHERINE L. HERBIG, CHANGES IN ESPIONAGE BY AMERICANS: 1947–2007 v (Mar. 2008), *available at* http://www.fas.org/sgp/library/changes.pdf (an unclassified report explaining some work done on the classified side).

on both the Soviet and American sides encouraged both CIA and KGB members to seek out traitors and spies from the other side. Their post-war memoirs give some insight into what may motivate espionage and espionage-related treason crimes, as well as how these crimes are instigated and ultimately detected.[64] Espionage was particularly common over the long duration of the powerful but low-violence confrontation between the United States and the U.S.S.R., and it provides the most examples of modern espionage.

Former KGB Major Stanislav Levchenko described the motives of those who commit espionage as conforming to four major causes: motivation (payment), ideology (e.g., empathy for communist, democratic, fundamentalist Islamic causes, etc.), compromise (to avoid embarrassment), and ego (a desire to be important, a feeling of under-fulfillment or under-appreciation as a government official)—leading to the use of the acronym MICE.[65] It has been suggested that the acronym is more complete as SMICE, adding sexual gratification as a separate cause.[66]

Criminology author Frank E. Hagan has suggested another typology to explain espionage: mercenary spies, ideological spies, alienated/egocentric spies, buccaneer or sports spy, professional spies (non-traitors), compromised spies, and deceived spies.[67]

Mercenary spies, in Hagan's typology, are those who spy for payment from a foreign government.[68] Hagan claims that the majority of espionage cases since 1980 have been mercenary spies,[69] though there may be some reason to doubt this claim.

---

[64] In addition to the memoirs of Cherkashin and Modin, mentioned below, *see* CLARENCE ASHLEY, CIA SPYMASTER: GEORGE KISEVALTER: THE AGENCY'S TOP CASE OFFICER WHO HANDLED PENKOVSKY AND POPOV (2004); MILTON BEARDEN & JAMES RISEN, THE MAIN ENEMY: THE INSIDE STORY OF THE CIA'S FINAL SHOWDOWN WITH THE KGB (2004); OLEG KALUGIN, SPYMASTER: MY THIRTY-TWO YEARS IN INTELLIGENCE AND ESPIONAGE AGAINST THE WEST (2009); ROBERT WALLACE, H. KEITH MELTON & HENRY R. SCHLESINGER, SPYCRAFT: THE SECRET HISTORY OF THE CIA'S SPYTECHS, FROM COMMUNISM TO AL-QAEDA (2009).

[65] FRANK E. HAGAN, INTRODUCTION TO CRIMINOLOGY 361 (7th ed. 2010).

[66] *Id.*

[67] *Id.* at 362.

[68] *Id.*

[69] *Id.*

Ideological spies are those who spy against their home nation because of a political or other ideological affiliation with another.[70] Many spies do claim to have an ideological affinity with the country that they spy for. However, Victor Cherkashin, legendary Soviet spy-handler for two of the most famous American turncoats,[71] posits that ideological rationalizations for behavior are actually post hoc,[72] and perhaps adopted so that the spy can feel like a good person, or demonstrate loyalty to the country he or she is now serving. This will be discussed further below. There are, however, some spy cases in which the accused traitors do appear to have strong ideological motivations, including Julius and Ethel Rosenberg[73] and the Cambridge Five[74] in Britain, who deeply supported the early communist movement in the Soviet Union.[75] Hagan theorizes that ideological spies were most common before the 1980s and 1990s, when he believes the motivation then switched to financial remuneration.[76] A reasonable conclusion to take from examining the known cases is that ideological considerations were more common during the revolutionary period of the early Soviet Union (when many people, including some inside the United States were supportive and hopeful about the newly-emerged state of communism), and explained by other causes as the Cold War went on.

Hagan says that there are some niche forms of spies: including a buccaneer or sports spy, who simply enjoys the thrill. Potential sports spies include Christopher Boyce and John Walker, who both cited the rush of spying.[77] Hagan also mentions "professional spies," persons who are actually intelligence officers operating under cover—usually by posing as a diplomatic agent and working out of his or her country's embassy, though never really posing as a native or penetrating a U.S. Government

---

[70] *Id.*
[71] Robert Hanssen and Aldrich Ames. *See infra* note 72.
[72] *See* VICTOR CHERKASHIN & GREGORY FEIFER, SPY HANDLER: MEMOIR OF A KGB OFFICER: THE TRUE STORY OF THE MAN WHO RECRUITED ROBERT HANSSEN AND ALDRICH AMES 115–16 (2005).
[73] For more information on the famous Rosenberg case, *see* RONALD RADOSH & JOYCE MILTON, THE ROSENBERG FILE (2d ed. 1997).
[74] For more information on the Cambridge Five, *see* YURI MODIN, JEAN-CHARLES DENIAU & AGUIESZKA ZIAREK, MY CAMBRIDGE FIVE FRIENDS: BURGESS, MACLEAN, PHILBY, BLUNT, AND CAIRNCROSS BY THEIR KGB CONTROLLER (1995).
[75] HAGAN, *supra* note 65, at 362.
[76] *Id.* at 361.
[77] *Id.* at 362.

installation;[78] and a "deceived spy" who is convinced by an agent of a foreign government that he or she is spying to benefit their own government—essentially, someone who consents to be a professional spy for their own country, using Hagan's definition of the term, but is tricked into treason.[79] Professional spies are what a person may envision when they think of espionage, a "James Bond" or "Mission Impossible" sort of figure breaking into a secure facility and stealing highly guarded information. Spies of this kind are, unfortunately for fiction writers, exceedingly rare.

Another category in Hagan's typology, the alienated or egocentric spy, is much more common than the previous types. Alienated spies are those who betray their country for personal reasons. The most common reasons seem to be: a perception of unfair treatment in their government jobs, a sense of personal importance and frustration when others fail to acknowledge these delusions of grandeur, a need to be important (regardless of whether that importance comes from doing good or bad acts), and a desire for revenge. There are many examples of persons motivated by such considerations, though they may have also received money for their services or professed ideological reasons for their crimes at some point in their espionage careers. Volunteer spies—those who seek out the opportunity to betray their country rather than being somehow recruited or pressured into it, are very often motivated by these personal reasons. For example, after the CIA fired Edward Lee Howard, he vindicated a personal vendetta against the agency, by defecting to the Soviet Union.[80] Aldrich Ames, an American spy for the Soviet Union who may have caused the most deaths of American agents in Russia (estimates are between ten and twenty-five), was motivated by his inability to progress in his career, as well as by what he viewed as a number of missteps by the CIA: including lying to the American public about the Soviet threat to gain more money.[81] Robert Hanssen was similarly frustrated by his isolation and inability to influence his peers at the FBI, as well extremely egotistical about his intelligence.[82] Earl Edwin Pitts also cited numerous problems he had had with his superiors at the FBI, and

---

[78] *Id.*
[79] *Id.*
[80] *Id.*; *see also* CHERKASHIN & FEIFER, *supra* note 72, at 147.
[81] CHERKASHIN & FEIFER, *supra* note 72, at 28.
[82] *See id.* at 238–39.

that he wanted to pay them back by frustrating their efforts by providing the Soviets with information to thwart the FBI's national security efforts.[83]

The Cold War record is also replete with many examples of Soviet spies who decided to work for the United States because of grievances or difficulty achieving promotion within the Soviet intelligence services. Cherkashin notes that Oleg Penkovsky, a member of the Soviet Scientific Research Commission, volunteered his services for the British and Americans (a few times before they accepted) after suffering numerous setbacks in his career. He is also said to have suffered from delusions of grandeur and sought to play a definitive role in determining the path of the Cold War.[84] He ultimately played such a role by giving the United States the intelligence that precipitated the Cuban Missile crisis.[85] Valery Martynov was a KGB officer who actually worked in the handling of spies and chose to spy for the United States out of frustration with his inability to rise in his career.[86] The FBI offered to supply Martynov with a fake FBI spy that Martynov could use to funnel false, but convincing, intelligence back to his bosses at the KGB, while instead being a spy for the U.S.[87] The opportunity to seek professional validation and become an important asset for the Americans was too much influence for Martynov to resist.[88] Cherkashin refers to another, still classified Soviet turncoat for the Americans, who spied because of professional mistreatment by his KGB superiors.[89] Ronald Kessler claims that it was this agent, fittingly codenamed AVENGER, whose intelligence eventually outed Ames and Hanssen.[90]

As truly surprising as it seems that a person charged with protecting their country could turn around and participate in espionage because of frustration at work, this mindset is well-documented. And, with some thought, it does make some sense. Espionage and treason are both low-frequency phenomena. It is not difficult to imagine that a few narcissistic

---

[83] *See* U.S. DEPARTMENT OF ENERGY OFFICE OF COUNTERINTELLIGENCE, *Counterintelligence Briefing Center—Earl Edwin Pitts*, http://www.hanford.gov/c.cfm/oci/ci_spy.cfm?dossier=48 (last visited June 9, 2012).
[84] CHERKASHIN & FEIFER, *supra* note 72, at 63–64.
[85] *Id.* at 56.
[86] *See id.* at 215–16.
[87] *Id.* at 216.
[88] *See id.*
[89] *Id.* at 253.
[90] *Id.* at 251.

personality types can slip by the interview and clearance process without detection. Narcissistic personality types are truly selfish: they do not join the intelligence services because of deep patriotism or concern for the safety of their countrymen, but because they perceive this career path to be one that will glorify them and make them extremely important. When that expectation is frustrated, the need for self-importance finds an alternate means for expression: the narcissist becomes an extremely valuable "hero" to an opposing country, rather than a mediocre and unappreciated civil servant in his or her own home country. Accepting exorbitant pay for his or her services and professing true belief in the opposing country's ideology both contribute to the traitor's perception that he or she is important—because the services are worth so much money, and heroic—because professing the new country's ideology will elevate the spy from viewing his or herself as a mercenary-narcissist, to viewing him or herself as a patriot for his or her newly-adopted country.

The harm that these spies are doing may not be perceptible to them. The entire betrayal occurs in secret, with no one knowing and no harm done to any known person, isolating the spy from the consequences and any empathy he or she might feel for victims. The betrayal of one's employer becomes an abstract goal of defeating an objective that the spy professionally disagreed with and now sees a way to affect from the other side, rather than a treasonous betrayal that may cost American lives. Perhaps viewing the mindsets of "self-recruiting spies" in this way can inform future efforts to combat espionage.

However, self-recruiting spies who reach out to opposing countries, offering their services, are not the only ones to commit espionage. Hagan discusses another category in his typology: the compromised spy.[91] A compromised spy is one who is not independently motivated to commit espionage, and only agrees to do so because of blackmail and coercion.[92] Victor Cherkashin, a forty-year, high-ranking veteran of the KGB, describes in his memoirs how such persons were recruited. Intelligence forces for both sides would often follow and track government officials of other governments, including "studying their activities to find weaknesses—prostitutes, say, or gambling—and the best ways of taking advantage of them. If a target seemed recruitable, we'd usually try to goad him into

---

[91] HAGAN, *supra* note 65, at 362.
[92] *Id.*

working for us by means of money and sex."[93] Cherkashin also states that KGB members would frame government agents by setting them up for illegal activities and causing the police to arrest them, offering to help make the charges go away if the target would supply information to the KGB.[94] The KGB would also target opposing government agents with large gambling or other debts. Cherkashin observes:

> The most successful cases involved 'swallows,' male or female agents sent to seduce targets . . . [The targets could then be] confronted with secret photographs or recordings. … [Or] a swallow could claim pregnancy and demand an abortion, or fictitious outraged family members would surface and threaten action. Then a marginally involved benevolent figure—I or another intelligence officer—would offer to intervene and provide rescue, only to ask for certain favors later in return.[95]

Yet Cherkashin notes that most set-ups such as these ended in the target refusing to collaborate, reporting the attempted recruitment to their government, and returning to their home country if they were at-that-time posted abroad.[96] "Even the worst bastard, wife beater and cheat doesn't necessarily betray his country."[97]

The fact that many or most attempts failed is not surprising, considering that many people who choose government service, despite their flaws, are able to appreciate the wrongfulness of exchanging national security secrets for self-preservation. Many government officers were probably confident that reporting these set-ups immediately would preserve their careers—their home government might very well have been impressed that they resisted the set-up. Yet some succumbed out of fear. The criminal profiles of such persons are harder to construct, as motivations varied. Two well-known cases of compromised spies involve two U.S. Marine Corps guards responsible for protecting embassy staff in Moscow: Arnold Bracey and Clayton Lonetree. Their Russian "swallow" girlfriends convinced them

---

[93] CHERKASHIN & FEIFER, *supra* note 72, at 49.
[94] *See id.*
[95] *Id.*
[96] *Id.* at 49–50.
[97] *Id.* at 30.

to turn over information they otherwise might have had no inclination to become involved with.[98]

A March 2008 study by the Defense Personnel Security Research Center examined changes in the motivation of spies in the post-Cold War era.[99] It reported 173 cases of espionage between 1947 and 2007, the majority of which occurred during the Cold War.[100] The study analyzed not only historical patterns but also isolated recent trends in the changing nature of spying, trends that may be moving away from some of Hagan's findings. The study isolated a trend to more of the spies being naturalized citizens, with an existing allegiance to another country.[101] Two-thirds of citizen spies since 1990 volunteered, 80% overall receiving no compensation.[102] Between 2000 and the time of the study, no known citizen spies were compensated.[103] Six of the eleven cases between 2000 and the time of the study involved terrorist organizations.[104] Fewer of the new spies had clearances: more than a third had none, compared to about a quarter during the Cold War.[105] As time progresses, more and more volunteer spies reach out using the internet.[106] This report claims that most spies since 1990 have spied out of loyalty to another country, with money as a motivation coming second and disgruntlement, noted above, a third-place motivator.[107]

Money does not appear to be much of a motivator in these cases. This may not be surprising. For example, Islamic fundamentalist terrorists have previously been radicalized by the xenophobia, exclusion, and discrimination they face when they emigrate to or visit European countries.[108] The rise is espionage by foreign-affiliated persons in the United

---

[98] *See* HAGAN, *supra* note 65, at 362.
[99] KATHERINE L. HERBIG, CHANGES IN ESPIONAGE BY AMERICANS: 1947–2008, (Mar. 2008), *available at* http://www.fas.org/sgp/library/changes.pdf.
[100] *Id.* at. vii.
[101] *Id.* at i.
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.* at viii.
[106] *Id.*
[107] *Id.* at 32.
[108] *See* Robert S. Leiken, Europe's Angry Muslims, FOREIGN AFFAIRS (July–Aug. 2005), http://www.foreignaffairs.com/articles/60829/robert-s-leiken/europes-angry-muslims. *See also* NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT (July 22, 2004), http://www.9-11commission.gov/report/911Report.pdf (noting that some of the 9/11 hijackers became

States could be attributable a similar sense of disaffection and lack of belonging in the United States, although the United States generally fares better than Europe at integrating minorities. Money may play only a secondary role in convincing those who already have divided loyalties, or who have already become resentful of American society or government.

B. Radical, Violent National Security Crime

Explaining the causes of terrorism has generated no small amount of scholarship over the years. Academics have looked to three main causes: structural factors, psychological factors, and rational-choice analysis.[109] One of the most pervasive questions has been: Are terrorists those who have to choose whether to give up "worthy ends" or to resort to "unworthy means," or are they simply deviant personalities who would have eventually committed other crimes had they not become terrorists?[110]

A structural analysis evaluates whether "the causes of terrorism can be found in the environment and the political, cultural, social, and economic fabric of societies."[111] Structural factors to consider might involve the geographical location of the terrorist or terrorist organization, the type of political system they are living under, the amount of modernization in their location, whether any social or cultural or historical factors might facilitate or inhibit turning to or using terrorist tactics, organizational dynamics with the terrorist organizations themselves—including their formation and split, the presence of other forms of unrest in the terrorist's locality—like riots or labor strikes or even war, whether there is public support in some form for terrorism or even financial and logistical support from a well-positioned well wisher like a neighboring state, the nature of any counterterrorist authority or operations, the availability of weapons, and the existence of individual or group grievances.[112] Following a structuralist analysis, we might be able to make some conclusions like, for example:

---

radicalized while studying in Europe) [hereinafter 9/11 REPORT]; LORENZO VIDINO, RADICALIZATION, LINKAGE, AND DIVERSITY (July 2011) (finding more instances of Islamic fundamentalist radicalization in Europe).

[109] JEFFREY IAN ROSS, POLITICAL TERRORISM: AN INTERDISCIPLINARY APPROACH, 77 (2006).

[110] NEIL C. LIVINGSTONE, THE WAR AGAINST TERRORISM 31 (1982) (quoting William A. Hannay, International Terrorism: The Need for a Fresh Perspective, THE INTERNATIONAL LAWYER 283 (April 1974)).

[111] ROSS, *supra* note 109, at 79.

[112] *Id.* at 82 (synthesizing Crenshaw, *The Causes of Terrorism*, 13 COMP. POL. 379 (1981)).

terrorism might flourish better in urban and more anonymous locations.[113] Terrorism might be facilitated if an oppressed ethnic or cultural group has a proud warrior tradition,[114] but might be inhibited if the group ascribes to a pacifist religion.

The existence of a grievance has been thought to be the most important structural factor.[115] And of course this makes sense—the amount of urbanization or the existence of a warrior culture matters little without a rallying cry. Examples of grievances might include the desire for independence—many terrorist organizations like the Irish Republican Army in Ireland or the National Liberation Front in Algeria were formed by ethnic groups that conceived of themselves as oppressed and used terrorist tactics to agitate for political independence from a colonizer. Other intra-state examples of terrorism might include a grievance like rejection of the ruling government's ideology—such as a number of extreme left- and right-wing revolutionary and counterrevolutionary groups operating in Colombia.

Psychological theories, on the other hand, "try to specify and explain the mental processes of individuals and groups"[116] and might technically include rational choice evaluations,[117] since rational choice might be considered part psychology, part economics. This Article looks at rational choice separately due to its emphasis on situation-based logical thinking as opposed to individual characteristics. Psychological theories[118] might include a psychoanalytical view,[119] questioning as to whether those who turn to terrorism have common psychological traits or a "profile;"[120] whether terrorists are made, not born, and can be explained by "developmental" theories;[121] whether terrorism can in some cases be attributed to learning,[122] frustration-aggression theories—suggesting that an inability to resolve a

---

[113] *Id.* at 82.
[114] *Id.* at 83.
[115] *Id.* at 85.
[116] *Id.* at 79.
[117] *Id.*
[118] *Id.* at 87.
[119] *See generally* GUSTAVE MORF, TERROR IN QUEBEC: CASE STUDIES OF THE FLQ (1970).
[120] *See* Charles A. Russell & Bowman H. Miller, *Profile of a Terrorist*, *in* PERSPECTIVES ON TERRORISM 45–60 (Lawrence Zelic Freedman & Yonah Alexander eds., 1983).
[121] *See* SABRI SAYARI, GENERATIONAL CHANGE IN TERRORIST MOVEMENTS: THE TURKISH CASE 10 (July 1985).
[122] Brian L. Pitcher & Robert L. Hamblin, *Collective Learning in Ongoing Political Conflicts*, 3 INT'L POL. SCI. REV. 71, 73–74, 82 (1982).

grievance—a structural factor noted above—might cause some persons to adopt violence;[123] or narcissism-aggression theories—noting that many terrorists share a history of receiving a significant blow to their ego that they try to correct through violence—a factor not unfamiliar to us from our evaluation of what might cause spying activity.[124]

Even if psychological factors are not the sole cause of an individual deciding to become a terrorist, this does not mean that they are not helpful for profiling terrorists and therefore not only pursuing policies which can decrease the behavior, but also for tracking potential terrorists before their most destructive crimes occur, or finding offenders after the fact. While many terrorists are believed not to be functionally insane, they do appear to share certain traits. For example, many have "paranoic symptoms" such as an overwhelming belief that they have been selected for an important purpose and must complete a critical mission.[125] They also display dissociative behavior, demonstrating kindness and sentimentality in ordinary life and detachment during episodes of violence.[126] It has been posited that terrorists tend to have above average intelligence.[127] This would not be so surprising given that sometimes persons with above average intelligence are more susceptible to ideological pitches—something used in cult recruiting. However, the intelligence of terrorists is disputed.[128] Numerous high profile bungles by terrorists might suggest that less intelligent persons are attracted to be lone wolves.[129]

A few terrorists may even have the thrill-seeking impulse, similar to the rare buccaneer spy, discussed above.[130] It is noted that "[t]errorism is a youthful profession," and the great majority of terrorists are under 30 years of age.[131] It may be that buccaneers are more common among the young,

---

[123] *See generally* TED ROBERT GURR, WHY MEN REBEL (1970).
[124] RICHARD MERRILL PERLSTEIN, THE MIND OF A POLITICAL TERRORIST 25–27 (1991).
[125] Conrad V. Hassel, *Terror: The Crime of the Privileged—An Examination and Prognosis*, 1 TERRORISM 1, 1, 5–6 (Nov. 1977).
[126] *Id.* at 32–33.
[127] *Id.* at 32.
[128] Daniel Byman & Christine Fair, *The Case for Calling Them Nitwits*, THE ATLANTIC (July–Aug. 2010) http://www.theatlantic.com/magazine/archive/2010/05/the-case-for-calling-them-nitwits/8130/.
[129] *See, e.g.*, *id.*
[130] *See* Hassel, *supra* note 125, at 33 (thrill-seeking behavior would be a more plausible explanation if there were more terroristic episodes that were not linked to a serious underlying grievance).
[131] LIVINGSTONE, *supra* note 110, at 43.

and that either youth or a thrill-seeking personality leads to recklessness and a feeling of immortality.[132]

Perhaps this thrill-seeking desire can be attributed to some of the younger lone wolves appearing in Western culture today. Mobsters like Henry Hill noted that their attraction to a criminal lifestyle began with seeing local gangsters, feared by many and committing crimes with impunity.[133] Somehow this cements in the mind as being a "cool" thing. Something seems to have happened in Western culture now that young men, perhaps too young to be traumatized by September 11th when it happened, are growing up in its aftermath and seeing that terrorism is the biggest, baddest thing they can do. Lone wolves are most common in the West, where they have negative experiences in their formative years and education,[134] such as cultural intolerance and isolation.[135] This situation could lead them to act out through terrorism where no sustained terrorist organization exists, or can be contacted, or is interested in having them as members.

Another psychological trait common to many terrorists is a tendency to blame society broadly for frustrating them in their desire to be important or achieve great things.[136] The notoriety of terrorism thus becomes an end run to fame and prominence. Such egotists sound not dissimilar from the egotists within the U.S. Government who ultimately become spies when their professional ambitions within the United States are frustrated. In both cases, the criminal behaviors and their purported motivations seem paradoxical: terrorists are claiming to help vindicate the grievances of oppressed groups, but kill innocents; public servants sign up to vindicate their country's interests, but end up betraying the nation in the most

---

[132] *Id.*

[133] NICHOLAS PILEGGI, WISEGUY 5–6 (25th anniv. ed., 2011).

[134] LIVINGSTONE, *supra* note 110, at 37.

[135] *See* 9/11 REPORT, *supra* note 108, at 160–63 (describing the Hamburg cell). Many of the hijackers were not radicalized until they left their home countries, the conditions of which they claimed as their grievances. Isolation and cultural intolerance in Europe appears to have helped radical them, and may explain why there are more successful Islamic fundamentalist terrorist attacks in Europe, where xenophobia is more pervasive than in the United States. *See also* Isaac Kfir, *Islamic Radicalism: The UK Case*, 47 LEGAL ASPECTS OF COMBATING TERRORISM 42, at 46–47 (2008) (discussing the persistent racial discrimination against non-Caucasian Muslims in the UK which may have contributed to the July 7, 2005 terrorist attacks in London).

[136] LIVINGSTONE, *supra* note 110, at 37.

damaging possible ways. A strong sense of egoism and the need to be important may be the primary motivator in such narcissistic cases.[137]

A relative of narcissistic behavior can also manifest in a number of terrorism cases: primary process thinking.[138] These persons project their needs and wants and concerns onto a larger community and often think they "speak for the people"—without being asked.[139] Such persons, when they encounter situations they find unacceptable in the world, try to modify the world and not their expectations.[140]

An additional psychological consideration, terrorists may employ necessary coping mechanisms to filter their understanding of what they are doing and view it as something other than what it is without being actually psychologically affected. Often these beliefs center around viewing themselves as legitimate warriors despite their non-adherence to the most basic rule of armed conflict—the requirement that civilians not be targeted.[141] They may view the violence they cause clinically and cultivate desensitization to it.[142] In order to view their activities as acceptable or even laudable, they will convince themselves that the enemy is not human, or view the target as "evil" and the world as a simplified place of black and while.[143] They will also cultivate beliefs that reinforce that good-versus-evil worldview, including beliefs that utopia can be achieved through their actions, belief in the absolute morality of the underlying cause, and reverence for self-sacrifice.[144]

Rational choice analysis, the last of our three perspectives, assumes that actors are rational and seeks to evaluate the incentives and disincentives that cause their behavior. Rational choice analysis can be particularly helpful in criminology since it can not only indicate a cause of crime, but also a means of preventing the crime: altering incentive structures. Under some evaluations, the adoption of terrorist techniques might be a logical

---

[137] *Id.* at 50.
[138] *Id.* at 37.
[139] *Id.*
[140] *Id.*
[141] *Id.* at 74.
[142] *Id.*
[143] *Id.* at 82.
[144] *Id.*

option.[145] Although repugnant, this can scarcely be surprising: terrorism has often worked.[146] National liberation groups seeking independence have been able to fight a war of attrition using terrorism tactics that may eventually cause a militarily superior force to withdraw. Terrorist tactics bring publicity to political causes—often the end in itself. The use of terrorist tactics to attack government objectives can undermine popular support for those objectives.

One thing that is often wondered is how terrorists can possibly cope with or accept doing something that is considered highly morally condemnable by the rest of the global community. Isn't it necessarily so that terrorists are crazy if they chose to be terrorists? Yet rational choice decision-making can play a large role in making terrorism appear to be a viable option, especially given the existence of structural factors like serious grievances. Lack of opportunity to participate in politics, dissatisfaction with leadership and elites, and other situations that frustrate nonviolent vindication of grievances can all have the effect of increasing incidences of terrorism.[147] Groups that produce terrorists may also feel "relative deprivation" compared with the group they seek to adapt.[148] Relative deprivation is an irrational concept in economics modeling, but a common one to human sociological thinking. The theory goes that in a situation in which everyone in society is better off, if inequalities are more severe, the poorest members of society will "feel" poorer than they did when they actually had less. Under this model, the success of the West, financial inequalities in developing countries, and other social situations can create a sense of irrational "relative deprivation" that sets the stage for intergroup conflict to even out inequalities.

Looking to these three main models, we can speculate as to different methods to combat terrorism: from reducing grievances to profiling possible offenders to altering incentives. But our modeling of the causes of terrorism cannot simply look to these three main strains of thought to understand the complex nature of the changing threat of terrorist crime. For example, one

---

[145] Martha Crenshaw, *The Logic of Terrorism*, *in* ORIGINS OF TERRORISM: PSYCHOLOGIES, IDEOLOGIES, THEOLOGIES STATES OF MIND 7–24 (Walter Reich ed., 1990).

[146] For example, the Irish Republican Army in Ireland or the National Liberation Front in Algeria. *See generally* ALISTAIR HORNE, A SAVAGE WAR OF PEACE: ALGERIA 1954–1962 (2006); ALAN J. WARD, THE EASTER RISING: REVOLUTION AND IRISH NATIONALISM (2d ed. 2003).

[147] GUS MARTIN, UNDERSTANDING TERRORISM 64 (3rd ed. 2010).

[148] *Id.* at 67.

important issue to understand in our models is trends in terrorist behavior. Much of the modeling of terrorism that this paper draws on is from the pre-9/11 era when terrorist groups were often large, hierarchical, secular, national liberation groups. Now there are more decentralized groups seeking greater lethality with less of a discrete agenda.[149] How does one explain the shift? What are the new structural factors, new psychological profiles, and new incentives of the "new" terrorists?[150] Rather than being a community of freedom fighters using shocking tactics, there are more lone wolves who are not themselves personally affected by the grievances they profess—instead they are elites who somehow turn to religiosity and violence after appearing to grow up with relative normalcy.[151] How will this be explained?

While this section provides a synopsis of some theories as to the causes of terrorism generally, a complex and unique combination of these factors is most likely at work in any particular terrorist criminal act.[152]

III. Detection

Extending the use of the examples of espionage and terrorism for our two polar kinds of national security crime, the next issue to consider in the crimes' profiles is a law enforcement perspective on the issue of detection.

Espionage committed by citizens is an extremely low-occurring crime, with less than 200 cases in the 20th and 21st centuries[153] out of the millions of past and present government employees. Many detection methods that might seem like good ideas at first glance—such as monitoring of government employee communications or developments in their personal

---

[149] Walter Laqueur, *The Age of Terrorism*, *in* THE NEW TERRORISM: ANATOMY, TRENDS AND COUNTER-STRATEGIES (Andrew Tan & Kumar Ramakrishna eds. 2002) (charactering the "new" terrorism has four key characteristics: lethality, religiosity, networked rather than hierarchical, and more striking power).

[150] *See* JAMES J.F. FOREST (ED.), THE MAKING OF A TERRORIST: RECRUITMENT, TRAINING, AND ROOT CAUSES (2006) (2 vols.).

[151] Sam Peleg, *Comtemporary Modern Terrorism: Actors, Motivations, Countermeasures*, *in* FIGHTING TERRORISM IN THE LIBERAL STATE: AN INTEGRATED MODEL OF RESEARCH, INTELLIGENCE, AND INTERNATIONAL LAW 1, 3 (Samuel Peleg & Wilhelm Kempf eds., 2006).

[152] *See* ROOT CAUSES OF TERRORISM (Tore Bjorgo ed., 2005) (evaluating diverse case studies of causes).

[153] HERBIG, *supra* note 99, at vii.

lives—are simply economically out of reach. Trying to find a spy by tracing the information he or she sent to the opposing country is also nearly impossible: if the Russians or Cubans or Al Qaeda appears to have accessed two different pieces of classified information, the U.S. Government cannot simply find one person who has recently accessed both. The same information could be from multiple leaks, and dozens of persons at a minimum access any particular piece of classified information.

During the Cold War, the most common method of discovering espionage was by obtaining a spy from the opposing side with knowledge about espionage operations in their country. This reality is one that completely belongs in the history and mentality of the Cold War: spies spying on spies. However, Cherkashin verifies that spies ferreting out other spies was truly the best detection method[154]: "almost all exposed spies are betrayed by other agents." There would normally be over a dozen intelligence officers who knew about a number of active spies, and intelligence officers from one country are often known to be intelligence officers by other countries. Thus, an FBI or CIA agent from the United States would approach some low-paid Soviet intelligence officer with money troubles—perhaps a gambling debt or a sick relative—and offer $1 million dollars and a comfortable life in the United States for him or her and his or her family in exchange for information identifying security leaks. Sometimes, such "pitches," as they are called in the counterintelligence community, would work, often they would not, and many times they would be met with a "counterpitch." Perhaps the Soviet would agree, but only to feed misinformation and disrupt American intelligence work. This normal back-and-forth of the Cold War era is a part of history now, but direct intelligence on state-affiliated spies in the United States is probably still easiest to gather through turning intelligence officers from the opposing side.

In the post-Cold War era, so far as we know, incidents of traditional espionage appear to have declined. However, there is an increasing amount of economic espionage directly against U.S. businesses, and there is a rise in the use of spycraft by more amateur, non-cleared, nongovernmental, and even terrorist-affiliated spies. There are more volunteer spies finding their handlers over the internet. Nontraditional methods and objectives of spycraft change the method of detection from spy versus spy to reliance on other law enforcement techniques. For example, spies affiliated with terrorist organizations may be found as part of general observation of a

---

[154] CHERKASHIN & FEIFER, *supra* note 72, at 252–54.

terrorist group, use of undercover agents pretending to represent a foreign country trying to contact people through the internet or people, or through a wiretap or other physical searches of known spies or other criminals.

Terrorism poses its own detection issues. While terrorist organizations coordinating attacks between multiple members might be easier for law enforcement to gain information on or infiltrate, there are also lone actors who self-radicalize and are extremely hard to predict. Organizations themselves are secretive, dangerous, and in the era of global telecommunications and the Internet, may be globally far-flung. Without the hierarchy of a state controlling the actions of operatives, they can be unpredictable, or splinter into uncontrollable factions. Actual violent attacks are of course easy to detect, but the objective of counterterrorism operations, more emphasized by the post-Patriot Act approach, is to prevent attacks before they occur. To do that, there is a need to detect operatives and unearth terrorist plans, networks, and financing schemes.

Detection of terrorism may involve a combination of traditional law enforcement approaches and a more intelligence centric approach following 9/11.[155] Human intelligence is compiled from countries and terrorist organizations around the world. Additionally, ordinary American citizens provide human intelligence in the form of tips to law enforcement. Using either bought or civically volunteered intelligence, the next step is to monitor the organization, networks, or individuals suspected and learn their plans and associates. The main method of monitoring communications is a version of a wiretap or microphoning of the residence, vehicles, etc. Title III and the Foreign Intelligence Surveillance Act are the two main legal mechanisms to monitor these communications.

There are two ways to obtain a wiretap in the United States. The first is through what is known as "Title III." Title III is Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act.[156] This law lays down the acceptable uses and methods of wiretapping for use as evidence in a crime. Title III provides that:

---

[155] *See generally* MATHIEU DEFLEM, THE POLICING OF TERRORISM: ORGANIZATIONAL AND GLOBAL PERSPECTIVES (2010).

[156] 18 U.S.C. §§ 2510–22 (1968), *amended by* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), the Communications Assistance to Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994), the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, 120 Stat. 278 (2006), and

> The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of— [list of crimes.][157]

Title 18 U.S.C. § 2518 provides the procedure for requesting a wiretap. The U.S. Government must submit a full and complete accounting of all relevant facts to a federal judge, explaining what evidence the government intends to obtain and how long the wiretapping will endure.[158] The judge evaluates whether the government has shown probable cause that a crime will be detected. A final order granting the requested wiretap must state the person being targeted and the nature and location of the tapped line, amongst other things.[159] The period of the wiretap cannot be longer than 30 days, though a judge can extend another 30 days.[160]

A FISA (short for "Foreign Intelligence Surveillance Act")[161] wiretap, or even a FISA physical search, is given in quite another circumstance: not when the government can show that it will gather evidence to support a criminal case, but instead when the government can

---

by the Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[157] 18 U.S.C. § 2516(1) (2012).

[158] 18 U.S.C. § 2518(1) (2012).

[159] 18 U.S.C. § 2518(4) (2012).

[160] 18 U.S.C. § 2518(5) (2012).

[161] The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (originally codified at 50 U.S.C. § 1566 et seq.) is an Act of Congress which prescribes procedures for physical and electronic surveillance and the collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers." FISA has been amended by the USA PATRIOT Act of 2001 to include terrorist groups.

show probable cause to believe it will obtain evidence that a targeted person is the "agent of a foreign power." Applications for wiretaps are not requested in the normal federal courts of the United States, but from the Foreign Intelligence Surveillance Court (with appeals heard by the Foreign Intelligence Surveillance Court of Review), the proceedings of which are ex parte and generally classified. The court can authorize wiretapping for periods of 90 days or longer, with extensions.[162] A FISA wiretap can also occur without a court order for a period of over a year, if for intelligence purposes, on the authority of the U.S. Attorney General, and no U.S. person is targeted.[163]

In 2004, FISA was amended to include a "lone wolf" provision: 50 U.S.C. § 1801(b)(1)(C). A "lone wolf" is a non-U.S. person who engages in or prepares for international terrorism alone—they are, in effect, themselves the foreign power. The lone wolf provision amended the definition of "foreign power" to permit the FISA courts to issue surveillance and physical search orders without having to find a connection between the "lone wolf" and a larger foreign government or terrorist group. Broadening the scope of FISA, preventative surveillance of lone wolves has become increasingly important to prevent terrorist attacks when foreign groups are unable to operate efficiently in the U.S. and instead focus their efforts on recruiting such lone actors.

IV. Prevention

Given that detection of espionage and terrorism is so difficult, it is not surprising that the U.S. and other governments invest so much time in prevention of national security crime. The main methods of preventing crime are deterrence through punishment (which seems as though it would have questionable success with regard to national security crime), incapacitation of offenders (generally only useful once the offender is identifiable—probably by having already done a serious crime), addressing the underlying societal causes (often costly), and hardening the target of attack. For most national security crimes, whose scale is so dangerous and frightening, hardening is the most commonly pursued strategy.

The main means of preventing espionage is requiring persons who handle classified information to get "security clearances" and handle

---

[162] 50 U.S.C. § 1805(d) (2012).
[163] 50 U.S.C. § 1801(a)(1)–(3) (2012).

classified material in carefully constructed and controlled government buildings. While fortified buildings protect information from direct thievery, the clearance process seeks to identify individuals who may betray national security information. There are three main forms of clearances: Confidential, Secret, and Top Secret.[164] The lowest level is that possessed by military personnel, a Top Secret clearance is required for nearly all national security posts.[165] Confidential clearances must be reinvestigated every 15 years, Secret clearances every 10 years, and Top Secret clearances every 5 years.[166] Confidential information is the least likely to affect national security if accidentally disclosed, Top Secret is the most likely.[167]

The SF-86, the questionnaire used for the clearance process, is publicly available and shows the main areas about which investigators are concerned.[168] Besides collecting past jobs and addresses and family and friends' names to go and fish around and see if anything turns up, the form looks for evidence of past foreign contacts, drug and alcohol use, mental health, criminal records, and any potential financial vulnerability. Criminal records, mental instability, and substance abuse could all suggest general unreliability that would preclude the U.S. Government from placing trust over classified information with the individual. More interestingly for espionage purposes, the extensive questioning about any and all foreign contacts in the SF-86, and about any and all financial vulnerabilities, appears to seek out persons who might be susceptible as compromisable or mercenary spies: persons with gambling or other debts, or persons who are even just known to foreign agents, and therefore can be watched until a blackmail opportunity presents itself.

For some positions, a polygraph examination is needed to verify the answers given in the application for a clearance. For even fewer positions,

---

[164] CLEARANCEJOBS.COM, SECURITY CLEARANCE FREQUENTLY ASKED QUESTIONS 1 (n.d.), *available at* http://www.clearancejobs.com/security_clearance_faq.pdf.
[165] JOBMONKEY, UNDERSTANDING GOVERNMENT SECURITY CLEARANCE, http://www.jobmonkey.com/governmentjobs/gov-security-clearance.html (last visited June 10, 2012).
[166] CLEARANCEJOBS.COM, *supra* note 164, at 2.
[167] Derrick Dortch, *Hush-Hush: Obtaining a Government Security Clearance*, WASH. POST (June 23, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/06/22/AR2006062201458.html.
[168] OFFICE OF PERSONNEL MANAGEMENT, STANDARD FORM 86: QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS (Dec. 2010), *available at* http://www.opm.gov/forms/pdf_fill/SF86.pdf.

the polygraph expands beyond personal history, signs of instability, financial information, and foreign contacts, into what is called the "lifestyle polygraph."[169] This polygraph is used to dig out any skeletons in one's personal life, often secrets pertaining to the person's sexual life, to determine the amount of blackmailable information that could be used against the person, either now or in the future.[170] Typical topics include drug and alcohol use, gambling, homosexuality, solicitation of prostitutes, extramarital affairs, and so on.[171] It is conventional wisdom that honest answers and full disclosure will assist in obtaining a clearance[172] (for example, drug use experimentation at a young age may be considered relatively common), however, there are obviously some cases in which the information disclosed will suggest that the person is not stable, or is highly blackmailable.

Acts of sabotage are also prevented using hardening tactics. Important government personnel have the protection of bodyguards, including the famous Secret Service detail that guards the U.S. President. Government facilities, particularly the working facilities of government employees, that contain not only the government's people but its information and instrumentalities, are guarded by a number of protective services, including forces like the Pentagon Police or the Federal Protective Service. The U.S. Marshals protect the courthouses and judges of the United States—including the justices of the Supreme Court, though a special force of Supreme Court Police guard the Supreme Court's courthouse. The Marine Corps Embassy Security Group, a part of the U.S. Marine Corps within the U.S. Navy, guards U.S. embassies around the world. Many of these buildings are designed securely, with metal detectors, identification badges that scan in for secure access, and so on.

Preventing acts of terrorism relies not only on the hardening of government personnel and facilities, but also some cultural symbols, like national monuments, which may also benefit from guards, metal detectors, and other hardeners. Additionally, items that might become the tools of a terrorist attack must be guarded. Due to a period of frequent terrorist hijacking of airplanes in the 1970s and 1980s particularly, and through September 11th, airport facilities have been increasingly well guarded, with

---

[169] CLEARANCEJOBS.COM, *supra* note 164, at 11.
[170] *Id.*
[171] *See id.*
[172] *Id.* at 8.

metal detectors, luggage scanning, strict rules on what may be carried on an airplane, and the use of Air Marshals, who fly secretly on planes at random to discourage and interrupt any terrorist attacks.

Other methods of preventing terrorism exist, including the already mentioned option of mollifying the underlying causes. The United States might mollify Islamic extremism, for example, by supporting the Israeli-Palestinian Peace Process, or appealing to political and religious moderates in the Middle East. "Underlying cause" forms of prevention are often expensive and impractical, but they may be well-suited in principle to the idea of alleviating the all important structural factor of the grievance, and in the case of terrorism it may be especially desirable as advancing these processes has the double goal of furthering U.S. foreign relations abroad and promoting international peace and security generally.

In cases of international terrorism particularly, a prevention option exists that rarely is available for other national security crimes; the option to reduce the enemy through the use of military force. This option is scarcely desirable in espionage since it would involve starting hostilities with another state, and with homegrown terrorists or saboteurs or assassins, the potential criminals are hard to find and fight in this way. Persons inside the United States cannot ordinarily be fought with military force as an alternative to criminal prosecution. Though approaches to terrorism are more diversified, hardening remains the most utilized method of preventing national security crime.

V. Trial and Punishment

During times of war, many spies, saboteurs, and traitors were tried and sentenced, often to death, by military commissions.[173] Because such persons were usually not entitled to prisoner of war status under the Hague Regulations for the conduct of war, this was a common practice in other countries as well.[174] There were spy-trials during the American Civil War,[175]

---

[173] DEPARTMENT OF THE ARMY, FIELD MANUAL 27-10: THE LAW OF LAND WARFARE, ¶¶ 75–77 (July 15, 1976), *available at* http://www.afsc.army.mil/gc/files/fm27-10.pdf.

[174] Regulations Respecting the Laws and Customs of War on Land, arts. 29–31, annexed to Convention Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631. The Hague Regulations are important and enduring treaties for the conduct of warfare.

[175] *See* LOUIS FISHER, CONG. RESEARCH SERVICE, RL 32458, MILITARY TRIBUNALS: HISTORICAL PATTERNS AND LESSONS 16–32, particularly 20 (July 9, 2004).

and during World War II.[176] There is a famous case from World War II in which Nazi saboteurs secretly entered the United States were caught and tried by military commissions, and most were executed.[177] Some of those Nazi saboteurs were even American citizens.[178]

Most national security crime cases are tried before federal judges in the local district of federal court by the local United States Attorney's Office. U.S. Attorneys are federal prosecutors responsible for prosecuting all federal crimes in their one of the 94 districts in the United States and its territories. U.S. Attorneys are assisted in espionage and espionage-related cases by specialized prosecutors from the Counterespionage Section (CES)[179] and in terrorism cases by the Counterterrorism Section (CTS). Other national security crimes, depending on whether affiliated with state-on-state activities or non-state actors, are divided between CES and CTS, with most state-on-state issues of sabotage or weapons trading going to CES and non-state actors going to CTS. Both United States Attorneys and members of the Counterespionage Section work for the Department of Justice, the lawyers for the federal government. The Department of Justice has two main components: the United States Attorney's Offices, located all around the country and handling whatever kinds of cases occur in their territory; and the lawyers at "Main Justice" in Washington, D.C., who are often specialized in a particular kind of law and can give expert assistance to the local United States Attorneys' Offices.

While a national security crime trial might proceed like any other in many respects, there are special laws for the protection of classified evidence. The American criminal law tradition puts heavy emphasis on public disclosure of all evidence at trial. The Sixth Amendment itself guarantees a right to public trials. This used to create a problem with espionage cases in particular, because the defendant demanded that the classified information he or she was accused of disclosing be presented at trial. This tactic was known as "graymail": defendants could force the

---

[176] *Id.* at 32–59, and particularly 5, 37, & 46.

[177] FEDERAL BUREAU OF INVESTIGATION, FAMOUS CASES: GEORGE JOHN DASCH AND THE NAZI SABOTEURS, http://www.fbi.gov/libref/historic/famcases/nazi/nazi.htm (last visited June 12, 2012). *See also* FISHER, *supra* note 175, at 37–47.

[178] *See Ex parte* Quirin, 317 U.S. 1 (1942) (citizens may be tried by military commission if they are enemies of the United States in war).

[179] U.S. DEP'T OF JUSTICE, NATIONAL SECURITY DIVISION, SECTIONS AND OFFICES, COUNTERESPIONAGE SECTION, http://www.justice.gov/nsd/sections-offices.html (last visited June 12, 2012).

government not to bring prosecutions when the information at issue was too important to be disclosed at trial. Congress reacted to this problem by passing the Classified Information Procedures Act (CIPA)[180] in 1980. CIPA allows for classified information to be kept secret, and even redacted or changed for court proceedings, to protect it from public disclosure. CIPA has been found constitutional,[181] despite the fact is does take some issues of proof of guilt out of public view.

One of the most distinct elements of a trial for treason or espionage or sabotage or terrorism is the sentencing element. Federal sentences for such offenses are very ungenerous to the offender. For example, a terrorism crime resulting in death can be punished by the federal death penalty.[182] Even terrorism crimes that are financial or unconsummated carry very heavy penalties. Terrorism crimes are also subject to a very serious "terrorism enhancement" under the U.S. Sentencing Guidelines.[183]

Providing defense information to a foreign government can result in a sentence of life in prison.[184] Not only can a spy receive an extremely lengthy prison term, the dangerousness of the inmate may make it necessary to have extremely restrictive methods of incarceration applied. For example, extremely damaging spy Robert Hanssen is in solitary confinement at "AdMax" in Florence, Colorado, underground, where it is nearly impossible to communicate with anyone by any means, in order to ensure that he does not disclose any more national security information, of which he still knows volumes.[185]

Under the U.S. code, treason can also be punished by life in prison, perhaps even a death sentence as well. Treason remains one of the few crimes for which it is unclear whether the death penalty could be

---

[180] Pub. L. No. 96-456, 94 Stat. 2025 (18 U.S.C. App. III §§ 1-16), *amended by* Pub L. No. 100-690, 102 Stat. 4396, Title VII, Sect. 7020(g) (1988); Pub. L. No. 106-567, 114 Stat. 2855, Title VI, § 607 (2000); Pub. L. No. 107-306, 116 Stat. 2423, Title VIII, § 811(b)(3) (2002); Pub. L. No. 108-458, 118 Stat. 3691, Title I, § 1071(f) (2004); Pub. L. No. 109-177, 120 Stat. 248, Title V, § 506(a)(8) (2006).

[181] *See, e.g.*, LARRY M. EIG, CONG. RESEARCH SERVICE, CLASSIFIED INFORMATION PROCEDURES ACT (CIPA): AN OVERVIEW, iii (March 2, 1989).

[182] *See*, *e.g.*, 18 U.S.C. § 2332b(c)(1)(A) (2012).

[183] U.S. SENTENCING GUIDELINES MANUAL § 3A1.4 (2012).

[184] 18 U.S.C. § 794 (2012).

[185] *See* BUREAU OF PRISONS, INMATE LOCATOR, ROBERT PHILIP HANSSEN, http://www.bop.gov/iloc2/LocateInmate.jsp (last visited June 12, 2012).

constitutionally applied. The Supreme Court has previously implied that the imposition of the death penalty outside of cases of murder is unlikely to be constitutional, because it would violate the proscription on "cruel and unusual punishment" of the Eighth Amendment.[186] Because no treason case has gone to trial in over fifty years, it is not clear how the Supreme Court or any court would rule on this issue. While treason may not always cost human lives, it is the ultimate betrayal of one's country and an extraordinarily serious crime.

Conclusion

This paper makes two opposite arguments. First, it argues for the creation of a new, more specialized legal subject, National Security Criminal Law. Second, it argues criminal law courses could benefit from a more interdisciplinary focus, one that looks not only to the crimes and cases themselves, but also criminological insights on the causes and nature of the crimes, and pragmatic law enforcement realities about detection, prevention, trial, and punishment. Both suggestions need not be followed in a single instance, but it is the endeavor of this paper to give a quick sketch of what "National Security Crime" is and what it can be. This concept is a discrete one, and by splitting it between different disciplines, or failing to study it altogether, full understanding of it is undermined. The importance of the criminal law as a means not only to punish but also help stem national security threats will ultimately be vindicated by improvement of this field. A fuller understanding of the crimes falling under the headings of treason, espionage, sabotage, and terrorism will help us understand them better individually and fight them collectively.

---

[186] *See* Coker v. Georgia, 433 U.S. 584, 598 (1977) (plurality) (noting in passing that the death penalty may not be appropriate for any crime in which a human life is not taken).