Undercover Operations
in the U.S. to Counter Terrorism and National Security Threats

by Tyne Truong

To effectively thwart various national security threats, such as transnational criminal organizations and terrorism, the U.S. must adopt a robust, cohesive, and coordinated national Undercover Operations (OPS) strategy at the Federal, state, and local levels. This paper asserts that the establishment of Undercover OPS by all Law Enforcement Agencies (LEA) of said jurisdictional levels ensures that the most effective prosecution can be formulated for any given criminal or terrorist group, regardless of jurisdiction. A national undercover OPS strategy adopted by Federal, state, and local LEAs would also allow substantive law enforcement information to be transparently and timely accessible to all LEAs at all jurisdictions, so that actionable intelligence information can be operationalized to support the mutually inclusive goals of intelligence-gathering and successful prosecutions. Thus, a U.S. national strategy of coordinated and targeted Undercover OPS, to include all LEAs of all jurisdictions being able to fully access all Undercover OPS databases that provide valuable Undercover OPS-gleaned "probable cause" fact patterns of criminal activities would support that particular LEA's affidavits for arrest, search, seizure, and electronic surveillance warrants. Such a cohesive Undercover OPS infrastructure ensures that U.S. national power is fully realized and efficiently resourced amongst all jurisdictional LEAs, effectively thwarting national security threats and terrorism.

Background

In 1983, Senator Charles McCurdy Mathias, Jr. sponsored and introduced Senate Bill 804 (S. 804), also known as the Undercover Operations Act, to the U.S. Senate to allow the U.S.

Mr. Tyne Truong is a retired Assistant Special Agent in Charge for the U.S. Department of Homeland Security, Homeland Security Investigations Directorate where he led national security, counterterrorism, and export control missions at the enterprise and regional levels. He is one of Security Magazine's 2020 "Most Influential People in Security," holds a Master's degree in Leadership from the McDonough School of Business, Georgetown University, and is a Homeland Defense Fellow Distinguished Scholar at the National Defense University, College of International Security Affairs.

Attorney General to give Department of Justice LEAs, such as the U.S. Federal Bureau of Investigation (FBI), the authority to carry out Undercover OPS.[1] This bill subsequently set guidelines and established considerations for undercover operations for various U.S. federal law enforcement agencies to follow, such as a) starting, continuing, and ending Undercover OPS, b) Undercover OPS standards; and (c) the role, authorities, and make-up of the Undercover OPS Undercover Review Committee.[2] S. 804 also set forth limitations on Undercover OPS, established standards for how subjects of investigation were targeted, and transferred the tort liability from government agents to the Federal government for negligence committed by said agents during Undercover OPS.[3]

...a properly vetted and registered confidential informant may also be deemed as a Undercover employee and/ or a government agent...

What are Undercover OPS? Before we go further, the following key Undercover OPS terms and their meaning shall be defined as per the Attorney General's guidelines for FBI Undercover OPS[4] and for purposes of the following analyses, will also apply to other Federal, state, and local LEAs employing Undercover OPS. Undercover activities are any investigative activity in which an LEA employee or another Federal, state, or local LEA working with the lead LEA (i.e., a task force officer[5] - a state/local LEA officer granted limited Federal arrest, search, seizure authorities), uses an assumed name or cover identity. Undercover OPS are an investigation involving a series of related Undercover activities by an Undercover employee over a period of time, usually the timeframe of a given investigation. A Undercover employee is any LEA employee or employee of another Federal, state, or local law enforcement agency working under the direction and control of the lead LEA in a particular investigation, whose relationship with that lead LEA is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity.[6] Based on the experience of the author of this paper as a criminal investigator and which has been defined by prosecuting U.S. Attorneys and state/local District Attorneys, a properly vetted and registered confidential informant may also be deemed as a Undercover employee and/or a government agent within this definition. A confidential informant can be a transnational criminal organization or terrorist organization member who is providing information to the U.S. government unbeknownst to the subjects of investigation of that organization.[7] "Proprietary" means a sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the lead LEA, and whose relationship with that lead LEA is concealed from third parties.

With these definitions established and to reiterate the thesis of this paper, if all U.S. LEAs, regardless of jurisdiction, created certified Undercover OPS programs to gather evidence and intelligence on identified transnational criminal organizations, terrorist organizations, and their top-tier leadership, the U.S. government would effectively be exercising its national power by leveraging Undercover OPS as a powerful intelligence and evidence gathering tool of that national power. Intelligence information is the window into the criminal/terrorist organization's illicit activities that once gleaned from Undercover OPS methodology, allows the U.S. government and specifically, LEAs, to puppeteer targeted covert (i.e., undercover meetings) or overt (i.e., search warrants) operational events to obtain prosecutable evidence. Undercover OPS is just one investigative technique that LEAs could

use to gather prosecutable evidence, but unlike obtaining information from individuals subject to arrest by say, responding to a criminal incident that has already occurred (i.e., interviewing occupants of a narcotics-laden vehicle that has been detained entering the U.S. from Mexico at a land border), LEAs would not have to rely on being reactive to a given event to obtain prosecutable evidence, but would now have a powerful proactive tool to obtain said evidence and choose the timing of either overt or covert investigative activity.

To obtain prosecutable evidence from subjects of investigation, an LEA could now use Undercover employees to conduct Undercover activities and perform Undercover OPS by, for example, running a proprietary business to establish the Undercover operation's bona fides with said subjects. The power of Undercover OPS is further magnified when one takes into account the sheer interconnectedness of persons, places, things, and other evidence employed by a criminal/terrorist group to advance their objectives that Undercover OPS methodology would reveal, particularly when Undercover employees are ferreting out this information from subjects of the targeted transnational criminal organization. When said evidence is developed, shared, and analyzed from the local level all the way up to the state and Federal levels in a national Undercover OPS framework, a local LEA's Undercover OPS purchase of street-level quantities of drugs (distribution-side) could be, for example, tied to the larger supply-side, international source country's command and control elements, which is the purview of federal LEAs. However, the sheer numbers of Undercover OPS being run by various U.S. LEAs at the various jurisdictions at this time, often without timely deconfliction or coordination, can make Undercover OPS not only ineffective as an overarching instrument of U.S. national power, but at the operational and prosecutorial level, extremely dangerous when LEAs targeting a criminal group draw weapons against subjects of investigation who may be Undercover employees of another LEA.[8]

When discussing the prosecution of investigative subjects via evidence obtained from Undercover OPS, one has to discuss the concept of "entrapment."

Analysis

Prosecuting Undercover OPS Cases and Entrapment

When discussing the prosecution of investigative subjects via evidence obtained from Undercover OPS, one has to discuss the concept of "entrapment." This is particularly important when trying to prove the validity of Undercover OPS as an instrument of U.S. national power to counter criminal and terrorist threats. One must first conceptualize LEA Undercover OPS as being one part of a two-part team, the other part being the prosecuting entity, i.e., the U.S. Attorney's Office, who prosecutes the Undercover OPS-obtained evidence in a particular investigation. Although the following example refers to the U.S. Attorney's Office, the analysis extends to all prosecutorial entities, such as a local jurisdiction's District Attorney's Office or State Attorney General's Office.

A U.S. Attorney's Office is headed by a U.S. Attorney and staffed by a number of Assistant U.S. Attorneys who serve as the U.S. federal government's principal litigators under the direction of the United States Attorney General.[9] Since there are 93 United States Attorneys and their respective Assistant U.S. Attorneys stationed throughout the United States, Puerto Rico, the Virgin Islands, Guam, and the Northern Mariana Islands,[10] these prosecutorial resources further enhance LEA Undercover OPS from a national perspective, via the direction and

counsel they provide LEAs to ensure a solid prosecution. For purposes of this discussion, U.S. Attorneys conduct trial work in which the United States is a party, as authorized under Title 28, Section 547 of the United States Code and as such: 1) prosecute criminal cases brought by the Federal Government and 2) prosecute and defend civil cases in which the United States is a party.[11] Throughout the life of any given Undercover OPS investigation, regardless of jurisdiction, LEAs must work with their prosecuting attorney in a robust, transparent, collaborative manner to thwart a criminal defense's arguments to have the government's case against their client dismissed. Without this collaboration, a given Undercover OPS investigation and the budgetary and time allocations invested in it may be wasted by a successful defense of entrapment, for example.

LEAs must work with their prosecuting attorney in a robust, transparent, collaborative manner to thwart a criminal defense's arguments to have the government's case against their client dismissed.

As defined by the U.S. Attorney's Office's criminal resource manual 645: entrapment is a defense to a criminal charge, on the theory that "Government agents may not originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act, and then induce commission of the crime so that the Government may prosecute." [12] *Jacobson v. United States*, 503 U.S. 540, 548 (1992). A valid entrapment defense has two related elements: (1) government inducement of the crime, and (2) the defendant's lack of predisposition to engage in the criminal conduct. *Mathews v. United States*, 485 U.S. 58, 63 (1988). Of the two elements, predisposition is by far the more important.[13] Even if inducement has been shown, a finding of predisposition is fatal to an entrapment defense. The predisposition inquiry focuses upon whether the defendant "was an unwary innocent or, instead, an unwary criminal who readily availed himself of the opportunity to perpetrate the crime." *Mathews*, 485 U.S. at 63. Thus, predisposition should not be confused with intent or mens rea: a person may have the requisite intent to commit the crime yet be entrapped. Also, predisposition may exist even in the absence of prior criminal involvement: "the ready commission of the criminal act," such as where a defendant promptly accepts an undercover agent's offer of an opportunity to buy or sell drugs, may itself establish predisposition. *Jacobson*, 503 U.S. at 550.[14]

Based on the aforementioned entrapment analysis, the U.S. Attorney's Office can thwart the defense's ability to assert entrapment of an indicted subject of investigation since the LEA's Undercover OP can show, often multiple times via multiple recorded undercover meetings, that the subject was predisposed to committing the criminal act, whether that act was provided by the government or not. Herein again illustrates the power of Undercover OPS as an instrument of national power: if the government always proves in a court of law that a criminal/terrorist subject was predisposed to committing the crimes with which he's charged and those crimes were revealed because of the LEA's deployment of the Undercover OPS upon the subject, then the pervasive use of Undercover OPS at all jurisdictional levels would enhance the prolificity of successful prosecutions against those criminals/terrorists subjected to said Undercover OPS. That the entrapment defense rarely succeeds in court is a testament to an Undercover OPS' ability to determine, over time, the predisposition of a subject of investigation via a number of recorded undercover meetings discussing, planning, and strategizing illicit activities. FBI Director Robert S. Mueller III said at an appearance in 2014, "I challenge you to find one of those cases in which the defendant

has been acquitted asserting that (entrapment) defense," when referring to prosecutors having a perfect record in defeating entrapment claims by defense attorneys in terrorism cases, the area in which the FBI has used Undercover OPS most aggressively.[15]

Intelligence Information, Discovery and Parallel Construction

As part of the National Strategy for Combating Terrorism that defines the elements of U.S. national power via diplomatic, information, military, economic, financial, intelligence and law enforcement (DIMEFIL),[16] how can DIMEFIL's Information, Military, Intelligence and law enforcement elements be effectively realized to specifically support various LEA operations, such as Undercover OPS? How do domestic LEAs obtain and use information from the intelligence community to thwart a given national security/terrorist threat, without jeopardizing the methods/tradecraft employed by that intelligence agency via the U.S. judicial system's "discovery" process? Can the "Intelligence" piece of DIMEFIL coexist effectively with the "Legal" aspect of DIMEFIL, specifically when we are talking about the LEA's use of intelligence information to obtain evidence for prosecutions at the state, local or Federal level?

In the U.S. justice system relating to prosecutions of criminals/terrorists, defendants of a charged crime are entitled to "discovery" information, to include exculpatory information that may exonerate the defendant. Discovery is a formal process of exchanging information between the prosecutor and the defense attorney about such things as witnesses and the evidence that will be presented at trial. Discovery lets the prosecutor and defense know before a trial starts as to what evidence will be presented and is designed to prevent "trial by ambush," where one side doesn't learn of the other side's evidence or witnesses until the trial itself, when there's no time to obtain counter-evidence.[17] Basically, think of discovery as the defense and the prosecution knowing everything about the evidence that will be presented by the opposing side, to include what type of evidence is being presented, how that evidence was obtained and whether that evidence was obtained legally. All LEA tools to obtain evidence, such as Undercover OPS, will be subject to discovery.

All LEA tools to obtain evidence, such as Undercover OPS, will be subject to discovery.

Since discovery is a mandatory process for all prosecutorial entities in the U.S. judicial system, regardless of whether it's a Federal, state, or local jurisdiction, what are the implications of discovery to LEAs obtaining information from the intelligence community and operationalizing that information in a Undercover OPS capacity to obtain prosecutable evidence in the U.S.? If LEAs use intelligence community-derived information to effect arrests, indictments, seizures, and other law enforcement actions against a criminal/terrorist organization, will discovery jeopardize the sources (i.e., Undercover agents, confidential informants) and methods employed by the intelligence agency that provided the originating information? This last question is particularly important, since the intelligence community may invariably be using Undercover OPS methodologies of its own that are not subject to the Federal Rules of Criminal Procedure, like U.S. LEAs are bound to. Federal Rules of Criminal Procedure governs how U.S. district and trial courts conduct federal criminal prosecutions in the U.S.

In the aftermath of 9/11 and according to a Congressional Research Service Report for Congress titled, "Sharing Law Enforcement and Intelligence Information: The Congressional Role," U.S. intelligence and law enforcement agencies' failure to share information with one

another subsequently led to Congress enacting legislation that removed barriers to information sharing between said agencies and mandated exchanges of information relating to terrorist threats.[18] Congress wanted to change the way the law enforcement and intelligence agencies were communicating information to one another and it wanted to address the pre-9/11 statutory barriers that had prevented such information sharing based on ensuring that the U.S. government was prevented from spying on U.S. citizens. These pre-9/11 statutes created a "wall" between intelligence and law enforcement that prevented transparent, timely, and robust information exchange. It is asserted herein that for a national Undercover OPS program to be most effective and for LEAs to have the most complete picture possible of a given criminal/terrorist organization, that LEA must be able to use intelligence community-derived information, with caveats. As needed during the discovery process, LEAs in concert with their prosecutors must exercise discretion as to whether prosecuting a particular subject is in the best interests of an investigation, or to the government in general, especially if ongoing international, intelligence community Undercover OPS are being conducted outside of the Federal Rules of Criminal Procedure and which may be jeopardized upon discovery.

Does LEAs' use of "parallel construction" solve the discovery problem when it comes to using intelligence information to advance a domestic Undercover OPS investigation? According to an open source Reuters article, parallel construction is a law enforcement process of building a parallel, or separate, evidentiary basis for a criminal investigation in order to conceal how an investigation actually began.[19] As such, it can be inferred that parallel construction was created to address discovery issues of intelligence community-derived information that was used by law enforcement to initiate an investigation that led to an arrest, indictment, and prosecution of a criminal/terrorist. According to the same Reuters article, some defense lawyers and former prosecutors said that using "parallel construction" may be legal to establish probable cause for an arrest. But they said employing the practice as a means of disguising how an investigation began may violate pretrial discovery rules by burying evidence that could prove useful to criminal defendants.[20]

Conclusions

A cohesive Undercover OPS infrastructure that local, state, and Federal LEAs create and maintain ensures that U.S. national power is fully realized and efficiently resourced amongst these LEAs, thus minimizing national security threats and terrorism. Although issues of entrapment, discovery, and translating intelligence community-sourced information into prosecutable evidence in U.S. court all challenge Undercover OPS, these challenges are outweighed by its benefits. These benefits include allowing LEAs to (1) proactively control the timing of overt and covert law enforcement activities to obtain evidence, (2) creatively construct the undercover operational circumstances, businesses, assets, etc. to establish bona fides with a hard-to-infiltrate criminal/terrorist organization, and (3) leverage these undercover operational circumstances and infrastructure at-will with intelligence community-derived information to exploit transnational criminal organizations and terrorists anywhere in the world, for the ultimate goal of successful prosecutions. Positing that electronic surveillance, such as Title III wiretaps or PRISM (Planning Tool for Resource Integration, Synchronization, and Management)[21] programs, represents a more effective tool than Undercover OPS to minimize national security threats and terrorism is untenable because information obtained from electronic surveillance and operationalized by LEAs requires the officer to be reactive to the electronic surveillance information, whereas Undercover OPS is premised completely on proactive

methodology; electronic surveillance is "wait and see" whereas Undercover OPS is "see and do." Additionally, because every eavesdropping warrant is required to have a statement as to other investigative techniques (i.e., Undercover OPS) used prior to the submission of the wiretap according to 18 USC § 2518(1)(c),[22] because the statement must include why these investigative techniques (Undercover OPS) tried have failed, or why they reasonably appear to be unlikely to succeed if tried, or are too dangerous,[23] and because defense litigation involving electronic surveillance wiretaps may originate from LEAs not having exhausted these investigative techniques, these reasons effectively make Undercover OPS a prong that must be fulfilled anyway prior to an electronic surveillance eavesdropping warrant being authorized by a court. However, employing electronic surveillance and intelligence information with Undercover OPS methodology and conventional investigative techniques forms a comprehensive strategy to fully realizing U.S. national power to thwart national security and terrorist threats to the Homeland. ***IAJ***

Notes

1 S.804 - Undercover Operations Act of 1983, 98th Congress (1983-1984)

2 Ibid.

3 Ibid.

4 Undercover and Sensitive Operations Unit, Attorney General's Guidelines on FBI Undercover Operations, Revised 11/13/92.

5 "DEA / DEA Programs, State & Local Task Forces". 2017. Dea.Gov. <https://www.dea.gov/ops/taskforces.shtml>.

6 Undercover and Sensitive Operations Unit, Attorney General's Guidelines on FBI Undercover Operations, Revised 11/13/92.

7 "Special Report". 2017. Oig.Justice.Gov. <https://oig.justice.gov/special/0509/chapter3.htm>.

8 Lichtblau, E. and Arkin, W.M. (2014, November 16). More Federal Agencies Are Using Undercover Operations. New York Times. p. A1.

9 "Mission | USAO | Department of Justice". 2017. Justice.Gov. <https://www.justice.gov/usao/mission>.

10 Ibid.

11 Ibid.

12 "645. Entrapment—Elements | USAM | Department of Justice". 2017. Justice.Gov. <https://www.justice.gov/usam/criminal-resource-manual-645-entrapment-elements>.

13 Ibid.

14 Ibid.

15 Lichtblau, E. and Arkin, W.M. (2014, November 16). More Federal Agencies Are Using Undercover Operations. New York Times. p. A1.

16 McDonnell, John P. National Strategic Planning: Linking DIMEFIL/PMESII to a Theory of Victory. No. JFSC-25789. National Defense University Norfolk VA Joint Advanced Warfighting School, 2009, p. 11.

17 "How Courts Work | Public Education". 2017. Americanbar.Org. <https://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/discovery.html>.

18 Best Jr, Richard A. "Sharing law enforcement and intelligence information: The congressional role." (2007).

19 "Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans". 2017. U.S. <https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805>.

20 Ibid.

21 PRISM is a system the National Security Agency uses to gain access to the private communications of users of nine popular Internet services, such as Microsoft, Yahoo, Google, Facebook and others. It is governed by Section 702 of the Foreign Intelligence Surveillance Act, which was enacted in 2008 ("Here's Everything We Know About PRISM to Date". 2017. Washington Post. <https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?utm_term=.c3f9a96ffc24>).

22 See 18 USC § 2518(1)(c).

23 Ibid.