Enhanced Human Intelligence Is Key to Defeating Terrorists

By Matt A. Mayer

June 2016

KEY POINTS

- *Encryption makes traditional counterterrorist intelligence collection methods more difficult, requiring renewed investment in human intelligence (HUMINT) collection.*
- *Local law enforcement, given its deep community ties and frontline role in thwarting terrorist planning, is ideally positioned to use HUMINT methods to detect terrorist activities.*
- *Terrorism grant funding from the US Department of Homeland Security should be used to develop and emphasize HUMINT capabilities in jurisdictions where we believe the risk of terrorist attack is highest.*

As the barbaric attacks in Paris, San Bernardino, Brussels, and Orlando have demonstrated, we need to enhance our capabilities to detect and thwart terrorists as they plan attacks. With the proliferation of off-the-shelf encryption technologies and other operational security measures, terrorists are becoming harder to find by traditional technical collection methods such as wiretaps and signals intelligence (SIGINT). Meeting this threat means investing in human intelligence (HUMINT) capabilities at home—not just at the federal level, but also at the state and local levels.

In an important speech nearly a decade ago, Gen. Michael Hayden, a retired four-star Air Force general and former director of both the Central Intelligence Agency and the National Security Agency, described the challenges the United States faced then and the critical importance of intelligence in winning the war on terrorism.

> We're now in an age in which our primary adversary is easy to kill, *he's just very hard to find*. So you can understand why so much emphasis in the last five years has been placed on intelligence. Moreover, the moment of an enemy's attack may be just that, a moment, a split second, the time it takes for an airliner to crash or a bomb to detonate. *There can be little or no time to defeat him on the battlefield he's chosen.*[1] (emphasis added)

This rings even truer today. In the age of ISIS-directed, -enabled, and -inspired attacks against our homeland, the enemy is harder to find than ever before. We have limited opportunities to detect and disrupt him.

Our future success depends on our ability to adapt. It is not enough to maintain the status quo and hope for better results. Terrorists have evolved since September 11; our domestic national security efforts must also evolve. One key is the expanded use of HUMINT, which will help local law enforcement agencies combat those who seek to harm Americans.

The Evolution from al Qaeda to ISIS

In the decade before the September 11 attack, our intelligence consisted mostly of federal entities directing their efforts at nation-states and, to a far lesser degree, at al Qaeda. After the attack, we focused far more attention on al Qaeda and its leader, Osama bin Laden.

Domestically, the FBI and large local law enforcement agencies began to expand their intelligence capabilities. Within a few years, the federal government added a new cabinet-level agency, the Department of Homeland Security (DHS). It received several billion dollars annually to distribute as grants to state and local entities to prevent, prepare for, respond to, and recover from terrorist attacks.

The FBI and DHS began investing in preventive resources for states and localities, expanding the Joint Terrorism Task Forces (JTTF) and creating state and local fusion centers.[2] The goals were better intelligence sharing among state, local, and federal law enforcement agencies, and more robust intelligence operations within larger, more sophisticated local agencies.

As we changed, the terrorists also changed. Our foreign operations disrupted al Qaeda and killed much of its leadership, including bin Laden. In its place, ISIS emerged, filling the vacuum left by the American withdrawal from Iraq. Experts estimate that ISIS has between 40,000 and 200,000 adherents in over 20 countries and assets in excess of $2 billion.[3] It has exploited the refugee crisis to slip terrorists into the West, who then execute ISIS-directed or -enabled terrorist attacks such as we saw in Paris and Brussels.

Part of the difficulty in fighting ISIS comes from its use of modern technology. It uses a sophisticated social media program to recruit and influence Western Muslims to engage in "lone wolf" attacks, as in San Bernardino. The program has been effective; over six thousand Europeans and several hundred Americans are believed to have gone to the Middle East to train with and fight for ISIS.[4] But use of encryption technology in ISIS-directed and -enabled attacks poses an even thornier problem, which was highlighted by the recent legal battle between the FBI and Apple over San Bernardino terrorist Syed Rizwan Farook's iPhone highlighted this challenge for several months.

Domestic Intelligence Operations Must Evolve to Meet Present and Future Threats

Mobile phones contain "a wealth of information of potential great value to law enforcement."[5] But much of that data is now encrypted. Terrorists increasingly conduct their activities using encryption technology. The first reported case of an authorized wiretap being stymied by encryption came in 2011,[6] and the intelligence community reports that the increasing use of encryption technology by terrorists is undercutting intelligence efforts.[7]

With court orders, law enforcement agencies can obtain metadata (e.g. phone numbers, call lengths, and location data) even for encrypted communications. But the substance of those communications remains hidden. As a result, SIGINT and wiretaps will likely show diminishing returns.

Congress must appoint a national commission to analyze this problem and recommend appropriate legislation.[8] But even this may have little effect. For example, Congress may pass legislation requiring US technology companies to provide law enforcement agencies with "back doors" to their encryption software. If this happens, terrorists will simply use encryption technologies developed by foreign companies.

Given that terrorists may work around such back doors with relative ease, and that the back doors come at the expense of privacy, the best answer for America may be to protect encryption and find other ways to empower law enforcement agencies to preempt and disrupt terrorist attacks.

Our focus on these threats must increase. As ISIS's hold on Syria and Iraq degrades, the threat to the West will increase. ISIS will attack Europe and America to prove its viability, reestablish its legitimacy, and strengthen its brand.

HUMINT Can Help Law Enforcement Stop Terrorist Attacks

We can overcome the increased use of encryption technology by terrorists and their increased presence in our cities by expanding our HUMINT capabilities. Human intelligence is the oldest form of intelligence collection. It is "the collection of information from human sources . . . done through clandestine or covert means."[9] HUMINT includes not only using CIA officers to recruit sources in foreign governments, but also using undercover police officers to penetrate criminal networks and build cases. Much of law enforcement investigative work, such as observing suspicious behavior, surveilling suspects, and undercover work, is collecting HUMINT.

Despite the encryption of communications, law enforcement agencies can use HUMINT to gain access to terrorist plans and organizations. The Major Cities Chiefs (MCC), an organization of police executives representing the 70 largest urban areas in the US and Canada, exists to answer this need. Its stated aim is to coordinate "the development and sharing of state and local intelligence collection plans and intelligence tradecraft so that each major locality can collect crime and terrorism information effectively and appropriately."[10] The MCC's Criminal Intelligence Enterprise Report concedes that it "cannot have quality analysis without quality collection."[11]

Local law enforcement is on the front lines in thwarting terrorist planning and attacks. The MCC notes:

> The task of rooting out violent extremism and disrupting terrorism in the homeland has . . . become as much of a local responsibility as it is a federal responsibility. . . . Upon an imminent terrorist threat, local law enforcement agencies are usually the first to identify the threat and the first to respond.[12]

In fact, roughly half of the foiled plots in America "required some preliminary [local] investigation (surveillance, undercover operations, searches, interviews, etc.) before a full-scale federal investigation could be initiated."[13]

It follows that relying primarily on federal resources will leave America less secure. Our domestic national security enterprise should readily acknowledge this.

We should expand HUMINT in three areas: monitoring, surveillance, and undercover investigations. The Los Angeles Police Department (LAPD) defines these as follows:

- **Monitoring:** the short-term or preliminary act of observing or watching the activities of an individual or organization . . . for the purpose of gathering information relevant to an investigation;
- **Surveillance:** the continuous or prolonged observation of a targeted individual or group by clandestine means for the purpose of collecting information material to an approved investigation; and
- **Undercover Investigation:** an approved investigation involving the use of an undercover officer who clandestinely obtains information about individuals or organizations through the development of ongoing in person relationships with such individuals or organizations.[14]

Note that, contrary to concerns raised by civil libertarians, these HUMINT activities do not include the use of agent provocateurs, who incite individuals or organizations to engage in illegal activities. In such sting operations, government agents penetrate organizations or make contact with individuals and incite and help them to commit illegal activities. The goal is to catch a suspect "pulling the proverbial trigger but on a dud weapon." However, civil liberties groups have raised concerns that these operations often constitute entrapment.[15]

As a practical matter, local law enforcement with limited resources cannot afford to expend HUMINT resources in sting operations aimed at catching individuals who may be interested in terrorist attacks. Instead, local HUMINT resources should work to embed themselves into suspected terrorist groups, which are already well along the path of radicalism, leaving sting operations to the FBI, which has the expertise and legal framework to avoid civil liberties violations.

Through wise use of monitoring, surveillance, and undercover investigations, local law enforcement can overcome the obstacles encrypted technology presents. HUMINT techniques also will allow law enforcement to determine more quickly the intentions of individuals and groups, thereby freeing resources for use in cases which warrant more intensive investigation.

We need to expand HUMINT activities in cyberspace. ISIS and other terrorist groups increasingly use the virtual world for recruitment and operations. Local law enforcement, therefore, should expand its capabilities to monitor and infiltrate terrorist activities in the virtual world. They should employ individuals whose native languages and backgrounds allow them to interact with suspected terrorists without compromising themselves by misusing phrases or missing cultural signals. These activities should be adapted to the time zones of the individuals being monitored, to avoid being discovered by terrorist groups who check to see if an online contact is active outside of normal US business hours.

Protecting Civil Liberties Remains Paramount in Any HUMINT Activities

Clear and consistent standards are critical to ensure that all HUMINT operations properly to preserve evidence and protect anticipated legal proceedings. For guidance in ensuring that a robust HUMINT program abides by current law, we can look at intelligence operations in the LAPD and the New York Police Department (NYPD). Both are large, sophisticated organizations operating under detailed guidelines.

In the LAPD all intelligence operations must be conducted in accordance with the "Intelligence Guidelines for Major Crimes Division Anti-Terrorism Intelligence Section" (LAPD Guidelines) as approved by the LAPD Board of Police Commissioners on September 25, 2012.[16] These guidelines require multiple approvals for initial lead investigations and full terrorism intelligence investigations.[17] LAPD must undergo a comprehensive annual audit by two board members, to ensure that its activities are fully in compliance with LAPD Guidelines and all applicable laws. This includes reviewing highly classified material in a Sensitive Compartmented Information Facility (SCIF).[18]

Similarly, the NYPD operates in accordance with the Handschu Guidelines, as modified this year by a proposed settlement agreement.[19] The Handschu Guidelines came from a 1985 federal court order governing the NYPD's investigations of political activities. After the September 11 terrorist attack, the court granted a requested modification of the guidelines to deal with potential terrorist activities. As with LAPD, NYPD's intelligence activities must receive multiple approvals and be conducted in accordance with established laws. These activities are overseen by a Handschu Committee, which includes a civilian representative whose job is to ensure full compliance with the Handschu Guidelines.[20]

Section VI of the LAPD Guidelines sets forth the basic framework for surveillance and undercover investigations, including:

- Safeguards,
- Authorizations,
- Specific information required for each application for undercover investigations,
- Requirements to approve applications,
- Additional requirements to penetrate a non-target organization,
- Terms and conditions of any undercover investigation,
- Requirements to extend undercover investigations,
- Restrictions on attending certain events, and
- Standards and responsibilities for undercover officers.

These elements should become the foundation of any local law enforcement agency's terrorism investigation program. The FBI, in partnership with the MCC, should evaluate all programs and certify compliance with established standards.

The MCC expressly acknowledges that law enforcement "must reinforce privacy protections as we continue to evolve. . . . The protection of the privacy, civil rights, and civil liberties of our stakeholders remains imperative."[21] The Criminal Intelligence Enterprise "will allow for better evaluation and standardization of state and local intelligence and counterterrorism operations."[22]

There is one caveat to this recommendation. We must adhere to our Constitution as we allow law enforcement to evolve its practices. This is difficult in a liberal democracy with a strong tradition of protecting innocent citizens from intrusive government. We can meet this challenge, but we should acknowledge that the Internet has altered our sense of privacy.

For example, their respective guidelines prohibit both LAPD and NYPD from maintaining files on individuals who are not the subjects of investigations. This makes sense, given the violations that occurred during the Civil Rights and Vietnam eras, when local law enforcement and the FBI kept files on political protestors and individuals engaged in the struggle for civil rights. However, it should be adapted for the Internet age.

Law enforcement agencies should be allowed to keep open source information on individuals without a criminal predicate, when that information is publicly available on the Internet and there is a nexus to suspected terrorist activities, such as travel to countries with strong ties to terrorism or making social media posts indicating sympathy for terrorist groups. It makes little sense to require redundant Internet searches for information that is permanently and publicly available.

Homeland Security Grants Should Fund and Emphasize HUMINT

After the September 11 terrorist attack, it was clear that America needed to develop domestic capabilities to prevent, prepare for, respond to, and recover from terrorist attacks. Given the national scope of this requirement, the federal government became the primary source allowing states and localities to acquire counterterrorism capabilities. After more than a decade of providing such funds to states and localities, the federal government has more than met its obligation to fund response and recovery capabilities, such as urban search and rescue squads, and turnout gear for firefighters.

In the future, federal counterterrorism funding should focus on prevention. With Homeland Security grant funding declining from a high of $3.6 billion in 2005 to $1.6 billion in 2016,[23] we must focus on prevention, which offers the greatest return on our investment. DHS should focus on building HUMINT capabilities in jurisdictions where we believe the risk of terrorist attack is highest.

In 2016, DHS identified 29 urban areas as "high-risk" jurisdictions for its Urban Areas Security Initiative (UASI) grant program. Those jurisdictions are listed in Table 1.

DHS should give a large portion of UASI grant funds directly to local law enforcement agencies in

Table 1. High-Risk Jurisdictions

Phoenix, AZ
Los Angeles/Long Beach, CA
San Diego, CA
Miami/Fort Lauderdale, FL
Chicago, IL
Detroit, MI
Las Vegas, NV
Charlotte, NC
Philadelphia, PA
Houston, TX
Anaheim/Santa Ana, CA
Riverside, CA
Denver, CO
Tampa, FL
Baltimore, MD
Twin Cities, MN
Jersey City/Newark, NJ
Cleveland, OH
Pittsburgh, PA
Seattle, WA
Bay Area, CA
Sacramento, CA
National Capital Region
Atlanta, GA
Boston, MA
St. Louis, MO
New York City, NY
Portland, OR
Dallas/Fort Worth/Arlington, TX

Source: US Department of Homeland Security, "Notice of Funding Opportunity (NOFO), Fiscal Year 2016 Homeland Security Grant Program (HSGP), 32, http://www.fema.gov/media-library-data/1455569937218-3daa3552913b8affe0c6b5bc3b448635/FY_2016_HSGP_NOFO_FINAL.pdf.

most or all of these areas, to fund expanded HUMINT capabilities. (Cleveland may be an exception.[24]) These grants should fund equipment, training, and personnel costs, including overtime incurred when an investigation requires it. DHS should commit to fund approved HUMINT programs for at least three years, to ensure continuity and personnel development. Absent a multiyear federal commitment, local law enforcement will be reluctant to invest in new HUMINT capabilities, for fear of being left to fund inherently labor-intensive, and therefore expensive, capabilities alone.

For a UASI jurisdiction to receive funds, it must already have an intelligence unit that houses a SCIF or participates with a JTTF that possesses a SCIF. FBI/MCC certification that a law enforcement intelligence program complies with established standards must be required for eligibility for UASI funding. Given the MCC's expertise, DHS should provide additional grant funding to the MCC to work with the FBI in developing standards and in advising and assisting other UASI law enforcement entities in developing HUMINT capabilities.

It is increasingly important that future domestic counterterrorism activities and policy formation be done jointly by federal and local law enforcement. This will also ensure that we continue the vital work of changing federal law enforcement cultures which historically opposed sharing information and intelligence with local law enforcement.

A New Threat Requires That We Adapt

With 15 years of growth and learning behind us, it is time to leverage the intelligence collection power of the million-strong state and local law enforcement community. These men and women are America's best chance to stop terrorists before they do more harm to our country and way of life. With the threat shifting from al Qaeda's large attacks to smaller attacks directed, enabled, or inspired by ISIS, and in view of terrorists' increased use of technology, our national security enterprise must adapt.

A key component of that adaptation is substantially increasing local law enforcement's HUMINT capabilities. This evolution will give us the best chance to preempt and thwart terrorist attacks. Adopting strong standards and oversight will ensure that our liberties are protected even as our lives are secured.

About the Authors

Matt A. Mayer is a visiting fellow in homeland security studies at AEI. He is a former senior official at the US Department of Homeland Security and author of *Homeland Security and Federalism: Protecting America from Outside the Beltway* (Praeger, 2009).

Notes

1. Gen. Michael V. Hayden, "Transcript of Remarks by Central Intelligence Agency Director," Council on Foreign Relations, September 7, 2007, https://www.cia.gov/news-information/speeches-testimony/2007/general-haydens-remarks-at-the-council-on-foreign-relations.html.

2. For a detailed discussion of these entities, see Matt A. Mayer, "Consolidate Domestic Intelligence Entities Under the FBI," American Enterprise Institute, March 2016, http://www.aei.org/ publication/consolidate-domestic-intelligence-entities-under-the-fbi/.

3. Priyanka Boghani, "What an Estimate of 10,000 ISIS Fighters Killed Doesn't Tell Us," *PBS Frontline* June 4, 2015, http://www.pbs.org/wgbh/frontline/article/what-an-estimate-of-10000-isis-fighters-killed-doesnt-tell-us/.

4. Ashley Kirk, "Iraq and Syria: How Many Foreign Fighters Are Fighting for Isil?" *Telegraph*, March 24, 2016, http://www.telegraph.co.uk/news/2016/03/29/iraq-and-syria-how-many-foreign-fighters-are-fighting-for-isil/.

5. Chan et al., "Mobile Devices: Challenges and Opportunities for Law Enforcement," *NAAGazette*, vol. 8, no. 2, http://www.naag.org/publications/naagazette/volume-8-number-2/mobile-devices-challenges-and-opportunities-for-law-enforcement.php.

6. Kristin Finklea, "Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations," Congressional Research Service, February 18, 2016, http://www.fas.org/sgp/crs/misc/R44187.pdf.

[7] Office of the Director of National Intelligence, "Remarks as Delivered by The Honorable James R. Clapper, Director of National Intelligence," U.S. Senate, Select Committee on Intelligence, February 9, 2016, at https://www.dni.gov/files/documents/2016-02-09SSCI_open_threat_hearing_transcript.pdf.

[8] Matt A. Mayer, "National Commission on Terrorists' Use of Technology Is Needed," American Enterprise Institute, January 2016, http://www.aei.org/publication/national-commission-on-terrorists-use-of-technology-is-needed/.

[9] Federal Bureau of Investigation, Intelligence Branch, "Intelligence Collection Disciplines (INTs)," https://www.fbi.gov/about-us/intelligence/disciplines.

[10] Major Cities Chiefs, "Criminal Intelligence Enterprise," March 29, 2012, https://majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

[11] Ibid.

[12] Ibid., 2.

[13] Ibid., 3.

[14] Los Angeles Police Department Board of Police Commissioners, "Intelligence Guidelines for Major Crimes Division Anti-Terrorism Intelligence Section," Los Angeles Police Department, September 22, 2012, 6–8.

[15] Jerome P. Bjelopera, "The Federal Bureau of Investigation and Terrorism Investigations," Congressional Research Service, April 24, 2013, 21–22, https://www.fas.org/sgp/crs/terror/R41780.pdf.

[16] Ibid.

[17] Ibid., 15–19.

[18] Ibid., 37–40. A SCIF is a secured room in which highly classified information is reviewed and analyzed. Access to the SCIF is limited to individuals possessing security clearances at the highest level known as Sensitive Compartmented Information (SCI).

[19] *Raza, et al. v. City of New York*, 13 CV 3448-PKC-JO (pending), Exhibit A: Proposed Modifications to the Handschu Guidelines, http://www.nyclu.org/Handschu-Settlement.

[20] Ibid., 10–12.

[21] Major Cities Chiefs, 2.

[22] Ibid.

[23] US Department of Homeland Security, Press Office, "DHS Announces Funding Opportunity for Fiscal Year (FY) 2016 Preparedness Grants," press release, February 26, 2016, https://www.dhs.gov/news/2016/02/16/dhs-announces-funding-opportunity-fiscal-year-fy-2016-preparedness-grants.

[24] Cleveland likely only made the 2016 list due to the Republican National Convention being held there in July, and likely won't be on the 2017 list. It was not on the 2015 list, when DHS finally cut the list down to fewer than 30 cities.