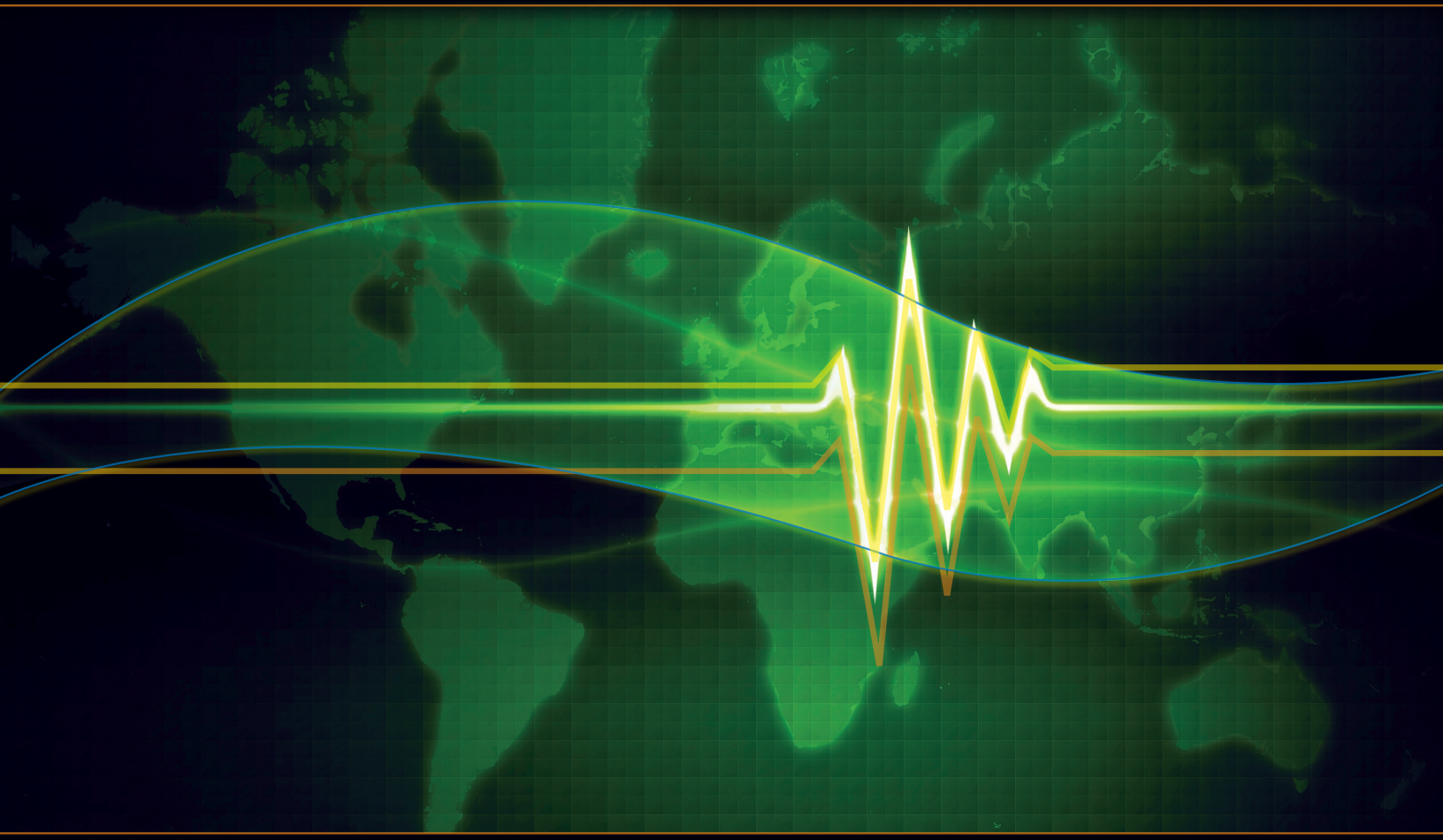
The Need to Share: The U.S. Intelligence Community and Law Enforcement



A White Paper prepared by the AFCEA Intelligence Committee

April 2007

AFCEA

Serving Intelligence Professionals and their Community

The Need to Share:

The U.S. Intelligence Community and Law Enforcement

Table of Contents

Executive Summary

Since September 11, 2001, the intelligence and law enforcement communities have struggled to adapt to new challenges and to refocus and reorder priorities. The media at times has been critical; Congress has demanded change; and the public has expected more. These communities have endured adjustments and upheaval while simultaneously confronting the war on terrorism—what many call *The Long War*.

Both law enforcement and intelligence organizations recognize the need to collaborate, share, and exchange information; however, the events leading up to 9/11 document how the legal and artificial boundaries between them created a serious impediment to protecting the country. Traditionally, participants in the intelligence arena use information to gauge *foreign* capabilities and intentions while members of law enforcement organizations collect information to support *domestic* prosecution. The Fourth Amendment to the Constitution limits surveillance of Americans, and regulations and directives limit distribution of foreign intelligence to domestic law enforcement. The seam between the federal, state, and local communities inhibits the United States' ability to fight terrorism.

In the pages that follow, the government and industry members of the AFCEA Intelligence Committee offer observations and recommendations that can help these communities move closer to the goal of sharing information and intelligence. It will require energy and emphasis to convince professionals in both communities that a new way of doing business is necessary and right, but it can be done.

Introduction

The Intelligence Committee of the Armed Forces Communications and Electronics Association (AFCEA) is pleased to present the seventh white paper in a series focused on the future of the Intelligence Community[1]. The committee's objective in producing these papers is to contribute

[1] See http://www.afcea.org/mission/intel/resource.asp#white to view the preceding white papers.

to the continuing discussion on how to strengthen the effectiveness of U.S. intelligence capabilities. This paper discusses the intersection of foreign intelligence with homeland defense, homeland security, and law enforcement.

Calls for Sharing Information

In the aftermath of the terrorist attacks of September 11, 2001, most observers concluded that the U.S. Intelligence Community and the law enforcement agencies need to share more information. Most also concluded that operational strategies and tactics—especially those focused on trans-national issues such as terrorism, drugs, counterintelligence, and weapons of mass destruction—needed to be better integrated. Understanding the need for change, Congress quickly passed the USA Patriot Act of 2001. It also enacted the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Congress wanted to strengthen the nation's ability to protect itself from future attacks and to provide more effective tools to fight the war on terrorism. These acts removed many of the barriers to cooperation between intelligence and law enforcement and mandated exchanging information related to international terrorist threats.

Although Congress included safeguards to protect the privacy and rights of U.S. persons[2], some critics argue the government has assumed too much authority and that some of the changes threaten important civil liberties. Others, however, contend that the legislation did not go far enough in providing the government with adequate tools to prevent future terrorist attacks. These views reflect the realities in establishing a different, more effective working relationship.

The goal of sharing information has a long, murky, and complex history. Part of the problem has been an inconsistent implementation of policies stemming from different interpretations of what is legally allowed. In the years leading up to the attacks of September 11, Congress and other groups in both the legislative and executive branches of government (for example, the National Commission on Terrorism and the U.S. Joint Task Force on Intelligence and Law Enforcement) had reviewed the legal and governing policies regarding sharing law enforcement and

[2] The legal definition of a "U.S. person" includes lawfully admitted permanent resident aliens, U.S. corporations, and U.S. citizens.

intelligence information. Generally, these reviews found that too frequently the barriers were excessively stringent. The groups recommended that the channels of communication among agencies be significantly improved to allow better and faster exchange of information; thereby fostering greater cooperation, particularly when focused on investigating terrorists' activities. In addition, the reviews almost universally concluded that many of the obstacles were bureaucratic or cultural (or both). Despite these recommendations, no significant improvement occurred because no compelling impetus to change existed before 9/11.

In addition, many of the barriers were responses to domestic spying abuses in the 1970s, which resulted in legislation ensuring the rights of U.S. persons. Over the next two decades the division between law enforcement and intelligence activities was reinforced by new policies that gradually extended the barriers to ensure legal compliance. In some instances the policies were treated as case law, and efforts to lawfully change them were discouraged.

During the 1990s, instances of international terrorism, narcotics trafficking, and other trans-national activities crossed the boundary between domestic and foreign intelligence. These activities raised awareness that terrorists did not care about the distinction the United States has made between foreign and domestic operations. Widespread Internet access and other modern communications technology provided enemies with tools to exploit the seam. However, many Americans continued to view closer cooperation of law enforcement and intelligence efforts as inappropriate and even dangerous to civil liberties.[3]

What Have We Done So Far?

The lack of information sharing between the law enforcement and intelligence communities was highlighted as a failure that might have made the 9/11 attacks possible. Objections against closer cooperation largely disappeared, and Congress enacted legislation to move these communities closer. *Inter alia*, the IRTPA mandated the creation of an Information Sharing Environment (ISE) that provides the technologies, procedures, policies, and standards for sharing terrorism related information among federal, state, and local jurisdictions. The IRTPA established the

[3] One important exception was the procedures established between the National Security Agency and law enforcement agencies to make use of actionable signals intelligence for counter narcotics purposes.

office of an ISE Program Manager to manage these efforts, measure progress, and ensure policy compliance. In addition to contractor support, the Program Manager's office currently has about 15 federal employees and is situated within the Office of the Director of National Intelligence. After lengthy coordination, the ISE Program Manager released a detailed Implementation Plan for the ISE in November 2006. ITRPA also created a Public and a Civil Liberties Oversight Board to watch over privacy and civil liberties issues that could arise with increased information sharing.

Other activities, such as the National Counterterrorism Center (NCTC), were created to help assure the flow of information. The NCTC has been challenged, however, in developing comprehensive effective mechanisms. The focus of the NCTC is on sharing information across federal intelligence and law enforcement agencies but not with state and local organizations. Some still believe that the NCTC's lines of authority are confusing and that certain important tasks are not well defined, making progress difficult. Nevertheless, the NCTC is staffed, functioning, and promises to be an important component of the fight against terrorists.

Despite many examples of federal, state, and local communities of interest that recognize the importance of sharing information to their performance, implementation is lagging.

What Are The Impediments?

Understanding the cultural differences between the intelligence and law enforcement communities is key to understanding the lack of progress.

The Law Enforcement Community

Pure law enforcement focuses on building a legal case related to a crime that already has been committed—an historical perspective with a forensic cast. A case is carefully constructed based on admissible evidence. The evidence is handled in a prescribed manner. The rules associated with chain-of-custody are designed to protect the integrity of information and reduce the pollution of evidence as much as possible. A set of procedures is followed precisely to ensure the case will be successfully prosecuted. In comparison, intelligence agencies often collect information in a way that is not admissible in a U.S. Court. Law enforcement agencies are

traditionally reluctant to use such information because of the potential of it being challenged and thereby jeopardizing a case.[4]

The pursuit of criminals requires secrecy—not information sharing. Premature release of data can destroy a criminal prosecution. Witnesses can change their testimony or even disappear. Important evidence may not become available if criminals learn that they are of interest to law enforcement. The law enforcement community lacks not only the desire but also an effective way of routinely providing information to the intelligence community.

The Intelligence Community

The intelligence community has its own deeply embedded culture and value systems. In contrast to law enforcement, the intelligence community focuses beyond the borders of the United States and on the future—assessing foreign trends and actions. Intelligence community analysts evaluate what they learn, interpret the importance of the information, and determine who should be informed. "Need to know" historically has been paramount.[5] Protecting "sources and methods" is regarded as crucial to keeping sources intact. Intelligence professionals are constantly reminded that they are responsible for *foreign* intelligence and must unerringly adhere to the laws and policies designed to protect the rights of U.S. persons.

Intelligence community policies have in the past erred by being too cautious. The intelligence community agencies created policies and guidelines to ensure personnel complied with legal boundaries for the gathering and use of national intelligence information. While these practices were designed to ensure full protection of the rights of U.S. persons, the policies were sometimes so restrictive that they effectively prohibited legal exchanges of information outside the community and at times even within. In many circumstances, no information was exchanged, and "connecting the dots" was nearly impossible.

[4] Notwithstanding these challenges, it is important to note that historically there have been counterintelligence, counterterrorism, and counter narcotics intelligence activities within the FBI that often cooperated or collaborated with the intelligence community. Many in the Bureau, however, considered these functions a "backwater," and generally not career enhancing.

[5] The practice of "need to know" presumes that when the intelligence and law enforcement communities interact, intelligence professionals understand what law enforcement officials "need to know," which is not always the case.

The Path Forward

September 11, 2001, demonstrated that there are threats that cross national and bureaucratic borders. As a result, Congress passed new laws to help the federal, state, and local communities overcome some of the "connect the dots" issues. One of the more obvious methods is to make more information quickly available to all who need it. Congress directed the establishment of an Information Sharing Environment (ISE) to bridge the gaps perceived by many as vulnerabilities exploited by the 9/11 terrorists. In addition, the intelligence and law enforcement communities have also created fusion centers and other such organizations to help address this problem. By most accounts, however, progress has been slow, and successes are measured in small steps.

The District of Columbia's new Acting Chief of Police Cathy L. Lanier published an editorial in the *Washington Post* (January 7, 2007)[6] that was a call to action. She advocated specific approaches to improve sharing national intelligence information with state and local law enforcement agencies. The AFCEA Intelligence Committee also recognizes this need, as do many others in the intelligence and law enforcement communities. However, the mutual desire has not yet resulted in agreement on mechanisms to share information that would enable an effective partnership among national, state, and local communities.

It appears easier for law enforcement organizations to share information with the intelligence community than for intelligence organizations to share compartmented intelligence information with the law enforcement community. Chief Lanier has proposed—and implemented in the District of Columbia—some innovative ways to share law enforcement and intelligence information. It stands to reason that having access to intelligence information will allow local law enforcement organizations to direct resources more effectively, reduce local vulnerabilities, and serve the public better. Cleared law enforcement officials can direct other resources effectively. If federal, state, and local law enforcement personnel are aware of emerging technology and tactics overseas, they can improve their ability to detect those capabilities here and develop countermeasures before the threat is imminent.

[6] http://www.washingtonpost.com/wp-dyn/content/article/2007/01/05/AR2007010501517.html.

How Can We Do Better?

The committee believes certain steps can help the intelligence and law enforcement communities move forward in their ability to share information and intelligence better.

Communicate and Reinforce the Need for Sharing:
People have a natural tendency to resist change. For this reason, leaders throughout the intelligence and law enforcement communities must consistently and repeatedly deliver the message of change and ensure that everyone understands the importance of sharing information. Analysts who have been told for years that releasing certain types of information violates the law must now be strongly encouraged to exchange the information with others. The new Director of National Intelligence, Mike McConnell, has made a strong statement to all intelligence professionals with his direction that it is not enough to share intelligence: There is a responsibility to provide it.

Earn Public Trust:
Abuses of the past have made the public skeptical about the government's role in personal lives. Yet, the public wants and deserves a collaborative intelligence and law enforcement community effectively working together to prevent another terrorist attack. A Markle Foundation task force[7] noted, "For information sharing to succeed, there must be trust.… Building trust requires strong leadership, clear laws and guidelines, and advanced technologies to ensure that information sharing serves important purposes and operates consistently with American values." The communities must ensure compliance with the law and make the commitment visible to the public.

Manage Risk:
The intelligence and law enforcement communities have been risk averse in the past regarding sharing information—often for good reasons. Today's environment calls for a different approach. The risk of sharing information must be balanced against the risk of not "connecting

[7] Mobilizing Information to Prevent Terrorism. Accelerating Development of a Trusted Information Sharing Environment. Third report of the Markle Foundation Task Force. July 2006.

the dots." What is the true value of having important information—even if it comes from a tenuous source in some cases—if the information is never shared with others who may need it and who may add value to the information? As a first step, local law enforcement should have a formal role and presence within the NCTC. This would give law enforcement officials early warning about terrorist tactics used overseas before the terrorists try to apply them in the United States, and it would help law enforcement plan and train better.

Create Clear, Understandable, and Consistent Guidelines:

Many current guidelines and policies are complex, confusing, inconsistent, and make sharing information difficult to achieve. This complexity causes delays in sharing data and undermines its utility. People are more apt to give up if the rules are too hard to follow.

Eliminate the Construct of "Data Ownership:"

The "owners" do not always appreciate why information they control could be significant to others. For sharing to be effective, those who have a broader picture may be the best advocates regarding what needs to be shared. For example, local and state law enforcement, fire, and public health organizations can make a critical contribution in terms of detection, prevention, and response. The federal intelligence or law enforcement communities may not be taking full advantage of these capabilities and skills because they do not have a clear understanding of what they can contribute. These individuals on the "front lines" may hold key pieces of the puzzle. The fact that some of their information comes from an unclassified source does not automatically mean it is not useful or important.

Use Technology in a Meaningful Way:

Most of the obstacles to meaningful change in this arena are cultural, but technology still can play an important role. Most, if not all, of the technological impediments to protecting sources and methods while enabling effective information sharing have been solved. Technology should be embraced as a key in easing the administrative burdens of sharing information.

Emphasize Training:

Effective and focused training can improve the confidence of community members and the public's perception that information is being handled appropriately. The right training, coupled with intelligence policies, will better enable sharing and ultimately will help change the cultures.

Share Good Ideas and Lessons Learned:

The District of Columbia, among others, has taken first and useful steps. It has initiated discussions in the law enforcement and intelligence communities to broaden understanding of what types of information are needed and why. Once state or local law enforcement organizations articulate and justify specific needs, and it becomes clear the contribution they can make to mission success, the willingness to share information will improve significantly. Other steps are possible. In the early 1980s the Drug Enforcement Agency (DEA) partnered with local law enforcement to educate U.S. police officers on the trends, tactics, and patterns of the South American drug cartels. As a result, local law enforcement officers knew what behavior, pre-cursor chemicals, and modes of transportation were associated with major trafficking and violent crimes of the international cartels. Such partnerships work. Leaders in both communities should look to the partnership model within the Joint Terrorism Task Force as an approach to enabling information sharing.

The Director of National Intelligence has recently created an Information Sharing Steering Committee (ISSC) and declared the ISSC will "move the Intelligence Community beyond the 'need to share' philosophy and more to a 'responsibility to provide.'"[8] This commitment can steer the federal, state, and local communities closer to the goal of a shared information environment.

Conclusion

Since September 11, 2001, the intelligence and law enforcement communities have struggled to adapt to new challenges and to refocus and reorder priorities. Nonetheless, the seam between federal, state, and local communities has inhibited the United States' ability to fight terrorism.

[8] PRNewswire-USNewswire: Creation of New Information Sharing Steering Committee for the Intelligence Community, Washington, March 6, 2007

Although Congress has removed many of the existing barriers to cooperation, and limited examples of progress exist, implementation is lagging. The key to change is strong leadership in both communities. Leaders must understand and nurture cultural change that emphasizes a responsibility for providing information—not just for sharing it. They must also communicate to their subordinates a willingness to accept risk in sharing data and must deemphasize data ownership. These steps, along with clear guidelines, inter-community training, the exchange of lessons learned, and the effective use of technology, can open doors of cooperation that have been closed for too long.

The AFCEA Intelligence Committee is a group of government and private sector volunteers which oversees AFCEA International's outreach to the Intelligence Community. By providing alternate means for the exchange of ideas of interest to intelligence professionals, the committee seeks to make a contribution to national security.