

Provide Resources and Capabilities to Exploit Fully Information on Terrorists

U.S. intelligence and law enforcement communities lack the ability to prioritize, translate, and understand in a timely fashion all of the information to which they have access.

Terrorists are using the same modern computer and communications technology as the rest of us, resulting in more information being collected. For example, a raid on a terrorist hideout is increasingly likely to result in the seizure of their computers. Instead of just finding a few handwritten notebooks and address books, counterterrorism authorities are faced with dozens of CD-Roms and hard drives. While there may well be information stored away in an encrypted file that could prevent the next terrorist attack, it is far more difficult to find that one file quickly out of the hundreds that may be stored on the terrorists' computers. To determine what is relevant, counterterrorism agencies must be able to process volumes of information—this can mean decrypting it, translating it, and perhaps making sense of conversations using code words. Until the information is in plain English, it is almost impossible to determine whether it is relevant to a terrorism operation.

The ability to exploit information collected—process it into understandable information and prioritize it—is essential to an effective global counterterrorist program. Intelligence derived from modern communications sources can provide indispensable warning and supports all aspects of the government's counterterrorism program, including military and law enforcement operations. Such intelligence is a necessary complement to that derived from human sources.



***We prevented
this attack—can
we prevent the
next?***

Unfortunately, this is an area where the United States, like other nations, is having trouble keeping pace with the information revolution. The National Security Agency (NSA) is America's most important asset for technical collection of terrorism information, yet it is losing its capability to target and exploit the modern communications systems used by terrorists, seriously weakening the NSA's ability to warn of possible attacks. The Senate Select Committee on Intelligence established a Technical Advisory Group whose recent report on NSA cites significant and expanding technology gaps.

Similarly, the FBI's ability to exploit the increasing volume of terrorism information has been hampered by aging technology. To address these deficiencies, the FBI has identified specific technology needs including improved technical means for using legal wiretap authorities; enhanced data storage and retrieval systems; and counterencryption equipment.

The Counterterrorist Center (CTC) in CIA is also suffering from inadequate resources. As a result, the Center has had to cut back or eliminate plans for an increased operational tempo to meet the globalization of terrorism and for development and acquisition of technology designed to assist in combating terrorists.

All U.S. Government agencies face a drastic shortage of linguists to translate raw data into useful information. This shortage has a direct impact on counterterrorism efforts. The process is further complicated by initially affording all data collected under FISA or pursuant to ongoing terrorist investigations the highest level of classification, thereby restricting access to personnel possessing the necessary security clearance. In many instances involving unique dialects, this requirement leaves material unprocessed while a worldwide search is conducted to identify the single appropriately cleared linguist.

The difficulty faced by the U.S. Government in coordinating linguistic capabilities with operational requirements highlights the need for a centralized coordinating and policy oversight body to mobilize linguists to prepare for an emergency surge requirement. The Foreign Language Executive Committee (FLEXCOM), located within the Community Management Staff of the Director of Central Intelligence (DCI), possesses the capability but lacks the designated authority to carry out these functions.

Recommendations:

- The President should direct the Director of Central Intelligence, the Secretary of Defense, and the Director of the Federal Bureau of Investigation to work with Congress to ensure that adequate resources are devoted to meet essential technology requirements of the National Security Agency and the Federal Bureau of Investigation and to expand and accelerate the DCI's Counterterrorist Center's activities.
- The Director of Central Intelligence should authorize the Foreign Language Executive Committee to develop a larger pool of linguists and an interagency strategy for employing them, including flexible approaches to reduce problems related to handling of classified material.

Promote the Flow of Terrorism Information From Law Enforcement to Policymakers and Analysts

The law enforcement community is neither fully exploiting the growing amount of information it collects during the course of terrorism investigations nor distributing that information effectively to analysts and policymakers.

As the federal law enforcement community becomes more involved in the response to international terrorism, it is collecting information that is important to policymakers and to intelligence community analysts. For a variety of reasons, the information is not always shared.

Law enforcement agencies are traditionally reluctant to share information outside of their circles so as not to jeopardize any potential prosecution. The FBI does promptly share information warning about specific terrorist threats with the CIA and other agencies. But the FBI is far less likely to disseminate terrorist information that may not relate to an immediate threat even though this could be of immense long-term or