CHAPTER TWELVE

The Intelligence Agenda

Transnational Issues

As noted in chapter 11, the division between nation-state issues and transnational issues is artificial if for no other reason than that the transnational issues all have major centers of activity in nation-states. Nonetheless, these transnational issues tend to be addressed in somewhat different ways and raise additional issues for intelligence services.

U.S. National Security Policy and Intelligence After the Cold War

For the first forty-five years of the existence of the intelligence community, one issue dominated its work—the Soviet Union. Director of Central Intelligence (DCI) Robert Gates (1991–1993) estimated that 50 percent of the intelligence budget went to the Soviet target—meaning the Soviet Union itself; its Warsaw Pact satellites; other states closely aligned to the Soviet Union, such as Cuba;

and Soviet activities worldwide. Other issues or regional crises arose from time to time, but the Soviet issue, as defined in chapter 11, remained the primary focus of U.S. intelligence. Also, given the global nature of the cold war, many of the other crises also had salience largely because they played a role in the bipolar rivalry.

With the dissolution of the Soviet Union on December 25, 1991, U.S. national security policy entered into a period of uncertainty in terms of focus and priorities. Several circumstances were important. First, there was a yearning within the United States for a "peace dividend," meaning a re-allocation of resources with less going to national security and more to domestic needs. (Cold war spending on defense as a percentage of gross domestic product [GDP] actually peaked in 1953 at 14.2 percent. During the so-called Ronald Reagan buildup, defense spending never went higher than 6.2 percent of GDP. For 1991, the last year of the Soviet Union's existence, U.S. defense spending was at 4.6 percent of GDP. The Soviet Union had allocated roughly 40 percent of an admittedly smaller GDP to defense on a fairly consistent basis, showing the overemphasis they put on this issue.) Second, there was a widely held belief that the remaining issues that might challenge U.S. national security were of a much lower order than the nuclear-armed Soviet Union had been. Third, there were a few ultimately futile attempts to create a grand theme (much like containment) under which U.S. national security could be organized. The George H. W. Bush administration tried "New World Order." The Bill Clinton administration briefly tried "Preventive Diplomacy" and later the concepts of engagement and enlargement. These concepts failed because they were too vague, they did not seem to be tied to any specific national security issues, and the United States was content not to be faced with major foreign policy challenges after half a century of world war and then cold war, which included several smaller "hot wars." There was also an interesting intellectual discussion, prompted primarily by the work of political scientist Francis Fukuyama in *The End of History and the Last Man* (1992), who argued that the end of the cold war marked the end of ideological conflict and the triumph of Western democratic liberalism. At the same time, some assumed that there would be a new "ism" to confront the United States and other nations with shared values, but no one could define what it might be. No one predicted the return of extremist religious views as the next "ism."

An oft-repeated but misguided question about intelligence was whether the role of intelligence had changed. The question betrayed a certain lack of understanding about intelligence, implying that its role was somehow bound up directly with the fact of the cold war. However, the role of intelligence—to collect and analyze information that policy makers need and to carry out covert actions as lawful authorities direct—did not and does not change. This mission

is—or should be—independent of any particular target, relationship, or crisis. It is the reason for having an intelligence community and should not be subject to the vagaries of international politics. U.S. intelligence targets and priorities have changed, but the community's mission has not.

This interregnum lasted for a decade, ending decisively with the terrorist attacks of September 11, 2001. (As discussed later, there had already been a series of terrorist attacks, beginning with the first attack on the World Trade Center in New York in February 1993. These did not have the same galvanizing or emotional effect as the 2001 attacks.) During this intervening decade, the intelligence community's responsibilities neither changed nor receded, but the leadership of the community found it more difficult to focus or to prioritize. They also received little help from the Clinton administration, which did not get actively involved in setting intelligence priorities other than one time in the middle of its eight years in office. The priority tier system introduced in the mid-1990s showed some initial promise but broke down as the priorities were never updated and revised and as policy makers and intelligence officers figured out how to manipulate the system to claim higher priorities for their favored issues.

The post–cold war interregnum created several strains for the intelligence community. The main one was budgetary. On a percentage basis, the intelligence community, rather than the much larger defense budget, bore the brunt of calls for a peace dividend. This had costs not only in real terms but also as an impediment to making a transition away from a cold war–based workforce, workforce skills, and the unexpected advent of the computer revolution. For example, some agencies found themselves with too many Soviet experts or Russian speakers, many of whom were rather senior. Was it worthwhile to invest in retraining them, knowing that their ongoing service would be short? It might seem wiser to let them go and invest in younger people with new skills and longer career prospects. But the more senior staff could not be fired, and many did not want to retire, thus creating a situation in which there was insufficient funding for new slots to bring on new people. DCI George Tenet has stated that during the 1990s the intelligence community lost the equivalent of 23,000 positions—meaning either people never hired or positions actually lost.

The cost of this was twofold. First, there was a draining away of veteran talent and a resultant smaller workforce to handle a more complex and diverse set of policy issues. Second, as the intelligence workforce began to increase dramatically after 2001, it meant that the number of experienced analysts dropped steadily as a percentage of the workforce, until, by 2015, roughly half of the analysts had no more than six or seven years of experience. This was, arguably, the least experienced analytic workforce since the inception of the intelligence community in 1947.

Therefore, in the second decade of the twenty-first century we find an intelligence community that was in the midst of a period of rebuilding, with a workforce that was perhaps less experienced than at any time in its history since its inception, and facing a series of issues that are much more difficult, more interconnected, and among which there is no clear priority. The budget impasse between President Obama and the Congress appears to have brought the more overt rebuilding process to an end. Budgetary constraints mean that new hires will be much fewer in number and, for the Defense intelligence analytic workforce, contractors serving as analysts—many of whom have more experience than their government counterparts—will be departing as their funding disappears. It will still be possible to rebalance the workforce, presumably de-emphasizing terrorism and counterinsurgency to some degree, but the era of growth is likely over.

Intelligence and the New Priorities

An examination of several issues that have risen in priority in the post–cold war period reveals some of the difficulties that the intelligence community faces. A major problem is the fact that many of these issues are closely related to one another. Terrorism, for example, has a direct connection to weapons of mass destruction (WMD) as it is widely assumed that terrorist groups would like to have access to these weapons. Terrorism is also related to narcotics, which serves to fund many terrorist activities, as do some other international criminal transactions. For example, the Taliban, which suppressed narcotics traffic when it ruled Afghanistan, now uses that same traffic to finance its operations against the Afghan government and the North Atlantic Treaty Organization (NATO). Director of National Intelligence (DNI) James Clapper noted this problem in his Worldwide Threat Assessments for 2011 and 2012, when he said, "It is virtually impossible to rank—in terms of long-term importance—the numerous, potential threats to US national security. . . . Rather, it is the multiplicity and interconnectedness of potential threats—and the actors behind them—that constitute our biggest challenge."

Many of these issues are related to the problem of failed states, which provide safe havens for such activities. Thus, just as it is somewhat artificial to separate nation-states and transnational issues, it is also somewhat artificial to discuss each of those transnational issues in isolation when that is not how they occur. However, there is no coherent way to discuss them as a single entity. Therefore, they will be discussed individually and, where appropriate, their relationship to other issues will be acknowledged.

This difficulty is reflected in the question of intelligence priorities. How does one make resource allocations among issues that have interdependencies but may not have the same priority individually? It is important to make some distinctions or one is left in the situation where there are, in effect, no priorities. When everything is important, nothing is important. For example, terrorism is a very high-priority issue. Should narcotics be given an equally high priority because of its relationship to terrorism, or can it be dealt with at a lower level and not lose the importance of the connection? This problem recurs across the spectrum of transnational issues.

Cyberspace

Like most other transnational issues, conflict in cyberspace is not entirely new, although it has undergone several transformations in the past twenty years. Indeed, even the name has gone through a series of changes—**information operations**, information warfare, net-centric warfare, and now cyber war—underscoring the still developing intellectual underpinnings of the issue.

It is somewhat difficult to give a precise starting point for cyberspace issues. Moore's Law about computing power and cost was first posited in 1965. Personal computers began to proliferate in the mid-1970s; the publicly accessible World Wide Web dates from 1989. Since then, computer-based technology has become pervasive in public and private activities. Jason Healey, a historian of cyberspace conflict, dates it from 1986, when German hackers searched through U.S. computers and sold the results to the Soviet KGB.

One of the most difficult aspects of the cyberspace issue is the great deal of hype, if not hysteria, that surrounds it—such as fears about a "cyber Pearl Harbor" (see below). DNI Clapper gave cyber a very high priority in his 2015 and 2016 Worldwide Threat Assessment. In 2015, DNI Clapper noted that the cyber threat was expanding but also said, "Rather than a 'Cyber Armageddon' scenario that debilitates the entire U.S. infrastructure . . . we foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security." DNI Clapper also said, "The cyber threat cannot be eliminated; rather, cyber risk must be managed." In 2016, the DNI added the Internet of things (a host of devices all connected to the Internet) and artificial intelligence to the list of cyber concerns.

The issue is not cyberspace per se but the uses to which it may be put. Broadly speaking, there are four major areas of concern beyond the use of cyberspace to support military operations:

- Infrastructure attacks
- Cyber espionage (government and commercial targets)
- Denial-of-service attacks
- Cyber-based terrorism

The main U.S. national security concern with cyberspace is the vulnerability of the cyber world to intrusion, corruption, or disruption, with potentially catastrophic effects for government or commerce. In his 2010 annual threat assessment, DNI Dennis Blair (2009–2010) noted that "acting independently, neither the U.S. government nor the private sector can fully control or protect the country's information infrastructure." Cyberspace is also an important arena for intelligence activities and war fighting. That is, nations need both to defend their government and private sector from intrusion but also use cyberspace to conduct military or intelligence operations against potential or current adversaries.

A major problem in cyberspace is its relative newness and the still inchoate nature of policy and doctrine related to cyber conflict. One of the truisms for all weapons is that doctrine—the ways in which the capability can be used to maximum effect—always comes *after* the technology's invention and initial use in the field. The development of air warfare offers a useful analogy. The first powered flight was in 1903; the first use of airplanes in warfare came in the Italo–Turkish War (1911–1912), fought over control of what is now Libya. Italy pioneered the use of airplanes first for reconnaissance and then to drop explosives on Turkish positions. The use of airplanes evolved further in World War I (1914–1918) and saw the evolution of plane-to-plane combat (dogfights) and strategic bombing against enemy civilian populations. However, the first comprehensive examination of air power doctrine did not come until Giulio Douhet's *Command of the Air,* published in 1921. A similar course can be traced for armored warfare as well. Thus, it should not be surprising to find that the doctrine for the use of cyberspace is still very much unformed.

The stated premise of this book is that properly conceived and conducted intelligence is derived from and serves policy. This helps explain a great deal of the problem in cyberspace, where there is much confusion about our policy goals—beyond the simplistic one of trying to prevent intrusions and attacks. To be fair, it is very difficult to craft policy for technology that serves simultaneously as a means of communication, of industrial control, of intelligence collection, and, possibly, of warfare, among other roles, and that exists in the international public sector. For the United States, the problem is further complicated by the fact that most of the infrastructure, broadly defined, belongs to the private sector. Among the concepts with which the

U.S. government is grappling, each of which has intelligence implications, are the following:

- *Information sharing about cybersecurity*. In February 2015, President Obama signed Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing." The goal is to encourage the private sector to share cyber threat information. Such sharing is seen as necessary to get a better sense of the cyber threat and to create better responses. However, as the E.O. recognizes, this is a voluntary concept. Private-sector firms may be unwilling to admit they have had serious cyber attacks and may be wary about sharing information about their infrastructure and operations for reasons of security and competitiveness.

- *Commercial encryption*. In large part as a reaction to the Snowden leaks, several companies—including Apple and Google, among others—decided to go to an encryption standard that does not have a key that can be shared with the U.S. government and that would be extremely difficult to break. Previous government access was sometimes referred to as **backdoor encryption**. Obama administration officials considered but then dropped, in October 2015, the idea of pursuing legislation to mandate such access. FBI director James Comey was especially vocal about the problems raised by the new encryption and the advantage that it gives to terrorists and criminals. Computer security specialists note that there are several other ways to get the data, other than directly through a device. They also note that any backdoor could also possibly be exploited by others as well. As noted earlier, Comey and DCIA John Brennan raised what they saw as grave national security implications of this new commercial practice in the aftermath of the November 2015 Paris attacks. Interestingly, European Union (EU) officials have also made the same request of various technology companies—again reacting to the Paris attacks. This represents a major shift, as many EU officials have been extremely critical of U.S. SIGINT activities in the aftermath of the Snowden leaks and had been very zealous about the need to safeguard privacy.

- *Hack back*. To date, the United States has opposed entities that have been hacked taking retaliatory action on their own, citing the difficulties of accurate attribution and the possible evolution into a "wild west" scenario of hacks and counterhacks without end, some of which would actually be misdirected. At the same time, firms in the private sector have bridled at what they see as a lack of action on the part of the government. Several questions arise. If propriety data are stolen, what is the appropriate response? No hack back will retrieve the data, so is the goal revenge?

There are also concerns about collateral damage from a hack back and the possibility of escalatory attacks. Finally, for U.S. firms, there are legal issues. The Computer Fraud and Abuse Act makes it illegal to access a computer network without permission. There is no exception if you have been attacked.

- *Deterrence*. There have been more and more calls for some sort of deterrence policy in cyberspace. The essential dynamics of deterrence are well known: holding something of value at risk as a means of preventing certain actions. Deterrence was one of the underlying concepts of the U.S.–Soviet relationship during the cold war: maintaining large nuclear forces on both sides that could not be wholly eliminated in a first strike, leaving open the likelihood of devastating retaliation. Deterrence is based in part on the reality of the deterrent force and in part on perception, the belief that you will use the force if necessary. However, there is also the problem that a deterrent may become a target if the other power decides not to be deterred any longer. This was the case for the U.S. fleet at Pearl Harbor. Indeed, one of the underlying problems in deterrence is the uncertainty that the deterrent is having the desired effect. Did the Soviets not attack because they were deterred, or did they never plan to attack anyway? All of these uncertainties are compounded in cyberspace. First, the fact of deterrence has to be declared, either overtly or by the creation and deployment of a deterrent force. In cyberspace, how would one distinguish current capabilities from a deterrent force? Second, what would be held at risk: opposing cyber forces or physical assets? This appears to run the risk of immediate escalation. Third, the use of a cyber deterrent would still be dependent on successful attribution. This might be an issue if it was decided to go to the UN to justify a defensive strike. Would there be sufficient intelligence to garner international support? Fourth, what threshold would differentiate current activities in cyberspace from an action that would require a counterstrike? Finally, deterrence relies on the assumed shared rationality of the parties involved. Assuming this works among most nation-states, does it extend to terrorists, hacktivists, and criminals? Likely not. Moreover, how would you hold these more ephemeral groups at risk to create deterrence?

- *Export control*. Initial international efforts to control the sale of software that could be used maliciously have run into difficulties. Much of the software in question—encryption, surveillance, security—may have legitimate uses, depending on who is using it and for what reason. There is also the very strong possibility that groups will use fronts or cutouts to get access to the needed software and tools.

Another problem that relates to cyberspace for the United States has been organizational: deciding where responsibility for cyber activities would be located. To an observer, it would appear that there are too many players, none of whom has much authority in cyberspace. Much of the cyber infrastructure in the United States belongs to the private sector. The Department of Homeland Security (DHS) is responsible for the nation's cyber defense and protecting critical infrastructures, but as DNI Blair noted, this must be done in cooperation with the private sector. There is also a cyber security coordinator in the National Security Council (NSC).

For the military, after much debate, the Barack Obama administration set up Cyber Command (USCYBERCOM), with overall responsibility for all aspects of defending Department of Defense (DOD) cyber networks and for coordinating, planning, and conducting military cyber operations. CYBERCOM is headed by a four-star officer who is also the director of the National Security Agency (NSA). This led some to conclude that CYBERCOM is part of NSA, but it is not. They are two separate organizations, and the only overlap is in the position of their leader. To confuse matters further, CYBERCOM is subordinated to Strategic Command (STRATCOM), which evolved from the Strategic Air Command (SAC) in 1992, and now has intelligence, surveillance, and reconnaissance responsibilities for global strikes worldwide, whether with kinetic (that is, projectiles) or cyber weapons. Moreover, each of the military services has retained its own organic cyber capabilities. In 2013, the Defense Science Board, an advisory group, criticized Defense's "fragmented" approach to cyberspace.

In the aftermath of the Snowden leaks, some suggested that the positions of NSA director and cyber commander be split, especially given the impending retirement of Gen. Alexander in 2014. Ultimately, the Obama administration decided to keep the current structure, with Admiral Mike Rogers succeeding to both positions. In 2016, Secretary of Defense Ash Carter hinted at the possibility of making CYBERCOM a full combatant command, which would probably also necessitate ending the dual role of the cyber commander and director, NSA. Some critics had also suggested that the next NSA director be a civilian, apparently believing that this would have precluded the NSA programs that had become controversial and ignoring the fact that these programs began after the PATRIOT Act became law and that the programs were briefed to the congressional oversight committees and had nothing to do with the background of the NSA director.

The existence of CYBERCOM does not preclude the possibility of some cyber activities being carried out by intelligence agencies. This is not just a bureaucratic issue. There are distinct legal implications on the use of cyber capabilities as a weapon or an intelligence tool in terms of who controls

the activity, the legal framework within which it operates, and the ways in which Congress should be informed, just as there is for special operations and intelligence, as discussed earlier. As noted earlier, there was not much support in the intelligence community for the creation of CTIIC (Cyber Threat Intelligence Integration Center) on the grounds that it was largely duplicative, but the NSC staff insisted on it.

As part of his reorganization of CIA, DCIA John Brennan created a Digital Innovation Directorate, which has three areas of emphasis: (1) improving CIA's ability to gather cyber-based intelligence; (2) improving CIA data management; and (3) making better use of the large amounts of data that the CIA collects, for both operations and analysis.

Finally, there has been a general recognition that the United States—both government and industry—does not have the trained workforce that it needs to be successful in cyberspace. Although there is frequent reference to a generation of "digital natives," there is a very great difference between being conversant or familiar with computer technology and being able to be effective in cyberspace. Again, part of this stems from the lack of firm doctrine.

For the sake of discussion, cyber operations can be broadly divided into offensive and defensive activities. A third important activity is forensics, which in cyberspace means investigating what has happened either in an activity that you are conducting or in one that you are defending against. Thus, forensics is tied to both cyber offense and cyber defense and can be thought of as a major intelligence activity. The offensive activities include the use of cyber capabilities either as a military weapon or as an intelligence tool, either for collection or for operations. One of the key issues here is **computer network exploitation (CNE)** versus **computer network attack (CNA)**. Once one has achieved access to a target's computers, one can exploit that access, determining capabilities, collecting available data retrieved, and possibly taking control of all or part of the network for one's own ends. All of that is CNE. There may also be reasons to bring down the network, to disrupt command and control or vital services within the target nation. That is CNA. One can obviously carry out CNE and, at some point, move to CNA. Much will depend on goals and surrounding circumstances. But these can become stark choices, not unlike the counterintelligence choice of allowing a known spy to operate as a means of determining how he or she works and for whom, as well as feeding false intelligence to him or her, versus arresting the spy. An interesting case was reported in the press in which NSA and the Central Intelligence Agency (CIA) disagreed about using cyber capabilities against an online jihadist magazine, *Inspire*. NSA saw the magazine as a legitimate counterterrorism target to be blocked and thus help protect U.S. troops deployed overseas. CIA argued that this would expose sources and methods and deprive them of an important

intelligence source. The CIA reportedly won the debate, but the magazine was then attacked by British cyber activity.

CNE has traditionally been considered an intelligence activity to be conducted by intelligence agencies, rather than a military operation. Because of the bureaucratic implications of such a division, DOD has recently been advocating the concept of the **cyber operational preparation of the environment (cyber OPE)** to cover military activities that intrude into adversary systems in advance of offensive operations.

An interesting intelligence issue for CNA is determining the degree to which an attack has been successful, again, forensics. In military operations, this is called **battle damage assessment (BDA)** and can usually be determined by geospatial intelligence (GEOINT) or signals intelligence (SIGINT). The cyber "battlefield" is more difficult to assess. How could it be determined that an enemy's computer system has been successfully disrupted or that the enemy has just shut it down when it recognized that an attack was under way? How could it be discovered if the enemy has backup systems? If a successful cyber attack is a precondition for some type of overt military operation, how can it be determined that the precondition has been satisfied? How much disruption should be caused? Disrupting enemy communications is useful, but should such action preclude, for example, the ability of an enemy headquarters to signal its troops authoritatively that hostilities are to cease? Or, having disrupted the enemy's ability to communicate, how can an enemy's offer to cease hostilities, to negotiate, and so on, be verified?

The interconnectedness of various systems worldwide also may serve to limit offensive activities as there can be unexpected and undesired consequences. For example, according to press accounts, in 2003 the United States considered crippling the Iraqi financial system via cyberspace before the actual invasion so that Saddam Hussein could not purchase war supplies. However, there was also concern that such an attack would affect the Middle Eastern and, then, potentially the global banking system, so the attack was not undertaken. Websites can also serve multiple purposes, creating conflicting opportunities and risks. Again, press accounts state that in 2008 the United States launched a cyber attack on a site that officials believed was being used by extremists planning attacks on U.S. forces in Iraq. The site had been sponsored by Saudi Arabia to lure extremists and would-be terrorists as a means of identifying them and tracking them. Even though the Saudis were told about U.S. plans, they were frustrated by the loss of an intelligence source. This is a classic case of competing and conflicting goals: the operational safety of U.S. forces versus luring in more terrorists. Finally, during the NATO air war against Muammar Qaddafi in 2011, the United States reportedly considered launching cyber attacks on Libya's air defense systems, which is always one of the first targets in

an air campaign. However, these cyber attacks were not made, apparently out of concern for setting a precedent about the use of cyber in warfare. Decisions like those in Iraq in 2003 and Libya in 2011 underscore the relative novelty of cyber and uncertainties about how and when to use it. These uncertainties do not preclude the use of cyber by several states and by non-state actors for various types of intelligence operations, from collection to sabotage. Nor is U.S. restraint likely to be sufficient to preclude actions by others.

Much of the concern about cyberspace focuses on the problems of defense and the chance of an "electronic Pearl Harbor." Again, this is analogous to early concerns in air warfare about a devastating strategic bombing surprise attack and the mistaken belief, prevalent in Britain in the 1930s, that "the bomber will always get through." As DNI Clapper and some cyber analysts point out, however, the chance of a surprise cyber attack carried out by a nation-state would most likely come only after a serious deterioration of relations, thus providing a period to prepare to whatever extent was possible. This would not be the case for non-state actors (terrorists, narco-traffickers, criminals, hackers), but they are also likely to have less well-developed cyber capabilities. Thus, the issue of cyber indications and warning depends, to some degree, on the nature of the attacker. Two of the most prominent cyber attacks followed varying periods of tension. In April 2007, Estonia was the target of widespread denial-of-service attacks, following a period of nationalist tension with Russia. Although independent Russian groups claimed responsibility for the attacks, many believed that these had to have been orchestrated by the Russian government. Before Russia's military attack on Georgia in August 2008, there was a series of cyber attacks on Georgian sites. There has also been Russian activity, apparently related to its campaign against Ukraine, against Ukrainian and NATO targets. This has included the use of "trolls," either robots or human commentators, to sway social media. There has also been an overall increase in Russian cyber activity, which may be part of the more aggressive posture assumed by President Vladimir Putin. According to press reports, there has been increased Russian surface ship and submarine activity near the undersea cables that are the backbone of the international Internet, raising concerns about possible Russian efforts to tap the cables or to cut them during a crisis.

A key intelligence issue in cyberspace is that of **attribution**. Again, for a large-scale nation-state attack, this presumably would be relatively easy as the cyber attack would not likely come in isolation from a deterioration in relations or other actions. The problem becomes more difficult for non-state actors and for CNE. Any response to a CNA or CNE depends on the ability to determine with some certainty who is behind the hostile action. This is made more difficult by the nature of cyber, where the origin of attacks can

be masked in terms of location or actor by having the attack travel through several points from origin to target or by attacking, either entirely or in part, by commandeering otherwise innocent computers. This becomes both an intelligence task and a policy decision: What level of certainty will policy makers need about attribution before ordering a response? This cannot be determined in advance and will depend, in part, on the nature of the intrusion or attack and the damage it has caused, which will lead to increased pressure for a response; the ramifications of a response, depending on who is believed to be the intruder; and the personality of the policy maker. In his 2015 assessment, DNI Clapper said attribution was improving and that most intruders will be detected and identified. Analysts note that the United States was able to identify the source of the November 2014 North Korean cyber attack against Sony Pictures. North Korea is seen as being less capable than China or Russia. (Some cyber analysts question this attribution.)

The barrier to entry for a cyberspace capability is clearly much lower than for WMD, although there are still varying degrees of capability. Cyber analysts view the United States as being the most capable and the most active nation in cyberspace. Britain, China, and Russia likely have cyber capabilities roughly comparable to those of the United States; followed, at a slightly lower level, by Israel; and then France and India. Most of these nations, including the United States, have been cited as cyberspace attackers in the last several years. The capabilities of non-state groups are likely lower than those of the most sophisticated nation-state cyber programs.

A great deal of attention in the United States has focused on the cyberspace activities of China. Chinese cyber activities can be divided into four major groups: (1) economic espionage against U.S. high-technology firms, (2) military espionage against new U.S. weapons systems, (3) reconnaissance in control systems for U.S. critical infrastructure, and (4) retaliation against groups publishing adverse information about China. Given the nature of the Chinese state, it is widely assumed that the vast majority of this activity is directed by the Chinese government, although some smaller fraction of it likely comes from Chinese nationalists or hackers. Mandiant, a U.S. computer security firm, identified People's Liberation Army Unit 61398, based in Shanghai, as a major source of cyber activity against the United States.

It is interesting to look at each of these motives in turn. DNI Clapper said in his 2013 Worldwide Threat Assessment that it is difficult to quantify the economic losses of cyber espionage. That same year, the Federal Bureau of Investigation (FBI) put total U.S. losses at $13 billion, without breaking down what portion is due to China. However, some analysts point out that although there are gains to be made in economic espionage, true economic success comes from innovation and marketing, not copying. Economic espionage

and espionage against weapons systems is hardly new; cyberspace simply provides another means of accomplishing this. Reconnaissance against critical infrastructure can be either economic espionage or preparation for a possible attack should this eventually become desirable or necessary. Some examples of retaliatory Chinese cyber attacks include those against Mandiant after its report was published and against *The New York Times* after it published detailed articles alleging official corruption in the family of then-Premier Wen Jiabo. Therefore, it can be argued that Chinese cyber activity represents traditional ends through new means.

Interestingly, DNI Clapper refused to characterize the OPM data loss as a cyber attack, saying that it was "passive intelligence collection," similar to what the U.S. does. In December 2015, China stated that the OPM intrusion was the work of criminal hackers and not the government, which some doubted for obvious reasons. Three months earlier, Admiral Michael Rogers, director of NSA, had said that there were no signs that the OPM data was being used for fraud or financial crimes, which is typical of criminals, which again calls into question the Chinese assertion.

There are other China-based cyber threats as well. Many, if not most of the computers purchased worldwide are assembled in China, presenting opportunities for both CNE and CNA. In 2013, U.S., British, and Australian intelligence agencies banned the use of highly classified networks of computers manufactured by Lenovo, a Chinese firm that acquired IBM's personal computer business in 2005. "Backdoors," that is, means for allowing remote unauthorized access, were found on Lenovo products.

Early press accounts indicated a decrease in cyber intrusions by China's People's Liberation Army (PLA) after five PLA officers were indicted by the United States in May 2014, although observers questioned whether this was a tactical or more meaningful change. In September 2015, President Obama and Chinese president Xi Jinping agreed to a "common understanding" that neither nation would engage in cyber intrusions to steal intellectual property. It is not clear how this agreement will be enforced. Notably, DNI Clapper questioned whether Chinese behavior would change. In November 2015, William Evanina, head of the National Counterintelligence and Security Center (NCSC), said he had not seen any indication of a decrease in Chinese economic espionage. U.S. concerns about China's and other nations' cyberspace activities were severely undercut by the exposure of NSA programs by Edward Snowden in 2013. Although these were intelligence collection programs rather than efforts to manipulate cyber systems, the extent of the alleged activity has made it difficult for the United States to appear as an injured party. The reality, of course, is that cyber activities—like espionage—are practiced by virtually every nation that can do so.

The Stuxnet virus that received a great deal of press attention and speculation in 2010 is a useful example of many of the issues noted above. Stuxnet was malware (malicious software) designed to attack a specific target, control systems for nuclear plants, especially those systems produced by Siemens, the German engineering firm. Although Stuxnet has reportedly affected systems in ten countries, the greatest interest was in Iran, where the largest number of systems was affected. Many press reports state that the virus caused damage among the centrifuges needed to create enriched uranium by altering their operating speeds. Iran, although admitting to some problems, downplayed any setbacks. Less attention was paid to the Flame virus, apparently created by the same people as Stuxnet. Flame, instead of sabotaging computers, apparently turns them into captive information retrieval devices.

Several germane points stand out. First, Stuxnet was apparently introduced via a thumb drive. Thus, we have human-enabled cyber (as opposed to an attack over the World Wide Web), just as there was human-enabled SIGINT in collection. Second, although it is assumed that the main target was Iran, several other countries also had Stuxnet intrusions. Third, the source of the attack remains unknown. Several countries were opposed to Iran's ongoing nuclear activities, many of whom could have produced the malware. It is unlikely that the actual source would voluntarily reveal itself. Fourth, Stuxnet is a case of using one transnational issue, cyberspace, to create a result in another one, WMD proliferation. Finally, whoever created Stuxnet and for whatever purpose, it was a very advanced piece of malware designed for effect not in cyberspace but in the physical world of industrial systems. As such, Stuxnet has been seen as a harbinger of more dangerous attacks to come against other such systems—whether dams, power plants, electrical grids, factories, or water treatment plants.

Unfortunately, cyberspace provides a medium by which nations—or non-state actors—can carry out campaigns and retaliation against one another during peacetime and presumably without the risks of more overt military acts. For example, in 2012–2013, Iran apparently launched a series of cyber attacks on U.S. banks, U.S. and foreign energy firms, and on the Saudi oil fields. These were seen as being twofold in nature: as retaliation for the Stuxnet attack and as a means of retaliating for the economic sanctions imposed as a result of Iran's nuclear program. In 2012, Iran announced that certain ministries would be off the World Wide Web for a month in what was seen as way of avoiding further hostile cyber attacks. In December 2014, the firm Cylance published a detailed report on the breadth of Iran's cyber activities, which it called Operation Cleaver. According to press reports, the Obama administration ordered cyber attacks on Iran's nuclear program and

offered cyber defensive support to friendly states in the Middle East and in East Asia that might be cyber targets of Iran and North Korea, respectively. Should attacks and counterattacks like these rise to a level where one state or another decided to move to conventional weapons, that state would once again face the problem of attribution. Press accounts in late 2015 stated that there was an increase in "sophisticated" Iranian cyber espionage attacks against State Department employees working on Iran and the Middle East. Some observers thought this might be a reaction by Iranian hardliners opposed to the nuclear agreement, either to undermine the agreement or to find ways to continue hostile action against the United States.

Both nation-states and international bodies have been working on rules of engagement and rules of conduct for cyberspace. U.S. officials have said that a U.S. offensive cyber attack on foreign computers would require presidential authorization but defensive action against cyberspace attacks could be conducted by commanders on their own. The degree and intensity of that response would have to be defined further, especially if commanders acted on their own authority. According to press reports, an Obama administration policy review concluded that the president has the authority to launch a preemptive cyber attack if there is credible intelligence of an imminent major cyber attack. According to press accounts, President Obama signed Presidential Policy Directive 20 in 2012 that establishes principles and processes for the use of cyber operations.

Internationally, NATO sponsored the drafting of the *Tallinn Manual on International Law Applicable to Cyber Warfare* (usually referred to as the Tallinn Manual). The manual sets forth definitions of various legal issues regarding cyberspace, such as sovereignty, and attempts to create rules for the conduct of cyber operations or reaction to these operations. Although only suggestions at this point, the Tallinn Manual may be the starting point for an international discussion of conduct in cyberspace, which may then affect related intelligence operations. For example, the Tallinn Manual says that hackers are legitimate military targets but also states that Stuxnet constituted "an act of force" against Iran and therefore was illegal according to international law, but the drafters were divided on whether this constituted an "armed attack." Critics of the Tallinn Manual point out that the Russian cyber attack on Estonia in 2007 was not seen by NATO as an act of force on a member nation and the alliance therefore did not invoke Article V, which calls upon NATO members to come to an ally's defense.

In conclusion, the continuing evolution of cyberspace and cyber operations takes both policy and intelligence into relatively new areas, where issues of policy, goals, doctrine, and roles and responsibilities are still being debated and formed.

Terrorism

The September 2001 attacks led to a greatly increased U.S. focus on terrorism, which became the primary national security issue, although not dominating intelligence activities as did the Soviet issue during the cold war.

Historical Context. The intelligence community's interest in terrorism pre-dates the 2001 attacks. First, there had been a series of earlier attacks by al Qaeda on U.S. interests, beginning with the first attack on the World Trade Center in New York in February 1993. Second, it is also important to remember that terrorism is a recurring phenomenon in international politics. In the late nineteenth century, there was a series of anarchist assassinations, killing President Sadi Carnot of France (1894), Empress Elisabeth of Austria–Hungary (1898), and President William McKinley of the United States (1901). In the United States from 1917 to 1920, there was the Red Scare, largely a series of bombings by anarchists, labor radicals, and pro-Soviet individuals. In the 1970s and 1980s, there were several strands of terrorism: European and Japanese radicals (West Germany's Baader Meinhof Gang or Red Army Faction; Italy's Red Brigades; Japan's Japanese Red Army); various Middle East terrorist groups (Black September, the Abu Nidal Organization, and others); and state-based terrorism (including Libya, Iran, North Korea). These strands sometimes came together in cooperative terrorist attacks. Thus, one can argue that the U.S. intelligence community has had more than forty years of experience with terrorism.

However, unlike the consistency of the Soviet target, terrorism has been a shifting target as groups rise and fall or are defeated and as the locus of terrorism changes. Therefore, it may be fair to say that there is more generic experience with terrorism than specific experience as terrorist threats continue to morph. Moreover, the earlier terrorist campaigns all were political in nature. The current terrorist threat has a self-selected religious basis, which makes it much more difficult to discuss as a policy issue because of our concerns about religious freedom and our understandable desire not to blame an entire religion for the acts of a faction within that religion. The religious aspect of modern terrorism also poses an analytic challenge in that Western states (with the exception of Northern Ireland and former Yugoslavia, if we include the Balkans) largely stopped fighting about religion in the seventeenth or early eighteenth centuries. Ironically, the next "ism" that some assumed would come about to replace communism as a foe—religious fanaticism—may actually be a historical throwback, at least in terms of Western experience.

Lessons From the Cold War. To understand the difficulties inherent in tracking and forestalling terrorism, one must recall the intelligence legacies of the

cold war. Terrorist groups, unlike the Soviet Union, typically do not operate from large, easily identifiable infrastructures and do not rely on extensive communications networks. As more becomes known publicly about U.S. intelligence sources and methods, terrorists have made greater efforts to avoid detection. For example, al Qaeda leader Osama bin Laden reportedly gave up the use of cell phones and fax machines to avoid being located by the United States. Ironically, it was bin Laden's reliance on human couriers to communicate that helped lead to his safe house in Pakistan. Also, terrorist groups do not conduct large-scale repetitive exercises, as do organized military forces. Thus, the visible signature of terrorists is much smaller than that of the Soviet Union or any nation-state. But the intelligence community still has, to a decreasing extent, a cold war legacy collection system developed to track a large political–military structure. Indeed, such a collection infrastructure remains necessary to track events in nation-states that are of interest or concern. Another major distinction between the Soviet target and the terrorist target has been noted by John McLaughlin, former deputy DCI: In the case of the Soviets we had a good sense of their capabilities but not their intentions. In the case of the terrorists, we know their intentions but not their capabilities.

As noted in chapter 11, the Islamic State (ISIL, ISIS, or Daesh) may be seen as an exception to some of the above observations since ISIL has pretension to be a state and is, for the time being, behaving like a "quasi-state," in that it occupies territory and conducts both military operations and terrorist attacks. ISIL also recruits much more widely than typical terrorist groups, which have tended to be small and rather insular. ISIL has used social media very effectively to draw recruits from several Western countries. This is a complicating factor, making it more difficult to find the right way to analyze ISIL. Nick Rasmussen, director of the National Counterterrorism Center (NCTC), said in congressional testimony in October 2015 that the ISIL threat was viewed as a spectrum, from the implications of its quasi-state status to its role in inspiring individuals to act. Several press accounts suggest that the intelligence community and policy makers took some time before they fully understood the threat represented by ISIL and how it differed from other terrorist problems. The rise of ISIL has also raised the question of which group is the greatest terrorist threat, which is an important question in terms of resource allocation. In that same testimony, Rasmussen stated that al Qaeda and its affiliates were still "a principal counterterrorism priority," but that was before the series of attacks in November 2015 for which ISIL claimed responsibility: a major bombing in Beirut, the downing of a Russian airliner over the Sinai, and the series of attacks in Paris. (In 2014, Boko Haram accounted for more victims than any other terrorist group.) The December 2015 shootings in San Bernardino, California, also appear to have an ISIL nexus, if only as an inspiration to the two people who committed the attack.

There has been recurrent controversy over whether ISIL has been contained or not, with President Obama earlier asserting they were contained and later press articles suggesting that an interagency intelligence assessment held an opposite view. Determining relative success against terrorist groups is often difficult. In the case of ISIL, it should theoretically be somewhat easier in that they hold fixed positions. However, their position remains somewhat amorphous, leading to the potential for renewed debates within intelligence and between intelligence and policy over whether or not ISIL is contained, not very different from debates during the Vietnam War (see chap. 2) on relative success of U.S. military efforts.

Analysts sometimes refer to **chatter** when they describe intelligence on terrorism. "Chatter" is a difficult term to define. It refers less to precise intelligence than to patterns of intelligence: communications and movements of known or suspected terrorists. As chatter increases—more messages, even those that may not contain direct references to attacks—or as suspects suddenly drop from sight, an increased urgency is felt about the possibility of an attack. In that sense, chatter is much like indications and warning (I&W)—anything that represents a change in observed patterns is the subject of increased attention. But chatter is also imprecise and, as terrorists learn more about how the United States collects intelligence, chatter can decrease for reasons other than pending operations. According to press accounts, the August 2013 U.S. alert that closed embassies in the Muslim world was based on fairly persuasive chatter.

In the aftermath of the September 2001 attacks, familiar claims were made that the United States was overly reliant on technical intelligence (TECHINT) and needed more human intelligence (HUMINT). Although HUMINT can, theoretically, collect terrorist-related intelligence that TECHINT cannot, the realities of terrorism must again be examined. Terrorist groups, and certainly their leadership cells, tend to be small and well known to one another. They have tended to operate in parts of the world where the United States does not have ready access. Even if trained agents were available who knew the required language and could be provided with a plausible cover story for their presence in one of these areas, penetrating the terrorist organization would remain problematic at best. One does not simply show up in Kabul, ask for the local al Qaeda or ISIL recruiting office, and then request to see the person in charge. (The press made much in this regard of the activities of the American John Walker Lindh in Afghanistan. Lindh was captured fighting for the Taliban, not for al Qaeda, in 2001. Recruitment into the Taliban was fairly simple. One had to be a self-professed Muslim willing to carry a gun—a far easier task than joining al Qaeda.) Finally, if HUMINT penetration were to be achieved, the new recruit would likely be asked to take part in some operation to prove his or her commitment to the cause. This raises important moral and ethical issues

for intelligence. How far would the United States be willing to go to sustain a HUMINT penetration—putting an agent's life at risk by taking part in a terrorist operation, possibly directed against U.S. personnel?

Some advocacy for more HUMINT was odd in that it seemed to treat HUMINT as a numbers issue: That is, if enough agents were sent, penetrating the target would prove inevitable. Such a scenario shows a fundamental misunderstanding of how HUMINT operates and the nature of the terrorist target. HUMINT is not an en masse activity. It relies on precision.

Finally, much of U.S. HUMINT against the Soviet Union was carried out in foreign diplomatic posts outside the Soviet Union, where Soviet officials were present and more accessible. Terrorists do not have this same overt overseas presence and thus present a smaller accessible target.

This does not mean that human penetrations of terrorist cells are impossible. As with the Soviet Union, a walk-in may occur. This apparently was the case with Ilich Ramirez Sánchez, a Venezuelan-born terrorist better known as Carlos the Jackal. He apparently was betrayed either by someone in his organization or by his Sudanese hosts. Walk-ins remain fortuitous, although, as discussed later, they can come as a result of ongoing successes against terrorists.

Beyond HUMINT, the terrorist target puts a premium on several types of intelligence:

- Signals intelligence (SIGINT): Very broadly defined, to include a wide variety of communications, including a presumed extensive presence on the World Wide Web and the Dark Web
- Open-source intelligence (OSINT): To collect and dissect the many public statements made by terrorist leaders and factions and, now, tracking their various social media sites
- Measurement and signatures intelligence (MASINT): To collect against acquisition of various types of WMD
- Geospatial intelligence (GEOINT): To collect against ISIL, which holds territory, but also against other groups that may have camps or staging areas

Media exploitation is also a very important part of the campaign against terrorists. For example, the operation that killed bin Laden also retrieved computers and associated materials that will be exploited for links to other terrorists, plans for operations, and so on. Finally, terrorism is an intelligence issue in which foreign liaison is very important, as is true for all transnational issues.

State Sponsorship of Terrorism. State sponsorship of, or at least acquiescence to, terrorism makes the intelligence issue more complicated. The intelligence

community must collect not only against the terrorists but also against other governments and their intelligence services. At one level, this is easier than is the terrorist collection itself, as it falls within more common intelligence practice. However, it also puts an additional strain on intelligence resources. Liaison relationships may be questionable in such cases. For example, the government of Pakistan had been relatively supportive of U.S. operations in Afghanistan up to a point, but the Pakistani Inter-Service Intelligence (ISI) was also a longtime sponsor of the Taliban. As noted earlier, bin Laden's longtime presence in a relatively open area of Pakistan raised questions about their ultimate support. State sponsorship also raises the issue of the failed states. Here it is useful to know if the terrorists are actually being hosted by the government, as was the case in Sudan and Afghanistan for bin Laden, or whether the lack of internal order simply provides an atmosphere where terrorists can work relatively freely, perhaps without official sanction. The lack of Pakistani authority over its western border region with Afghanistan, known as the Federally Administered Tribal Areas (FATA), was one of the reasons analysts presumed this to be where bin Laden was hiding rather in what was assumed to be the more exposed area of Pakistan not far from the capital. Again, bin Laden's five-year residence in Abbottabad raised questions about some Pakistani complicity at some level in their government. A Pakistani commission that investigated this issue found "gross incompetence . . . collective failures . . . [and] culpable negligence" on the part of the Pakistani military and security services but did not charge anyone with colluding with bin Laden. In March 2015, DCIA John Brennan noted that Iran was a state sponsor of terrorism and would likely continue to be, regardless of the nuclear agreement. Finally, ISIL again represents a hybrid situation, a terrorist group that has taken on some aspects of a state, including holding territory and trading in some commodities.

Closely related to state sponsorship is the even murkier question of relations between and among terrorist groups. For example, Libya had contact with factions of the Irish Republican Army. The Japanese Red Army worked with the Popular Front for the Liberation of Palestine (PFLP). Members of an Irish Republican Army faction were arrested after spending time with the armed rebels in Colombia (Fuerzas Armadas de Colombia, FARC). Such ties are both important and difficult to track or disrupt. The issue of ties among terrorist groups is important in the current campaign against terrorists both as a means of assessing threat and of assessing success. For example, most of the al Qaeda members who planned the September 11 attack are either captured or dead; al Qaeda's safe haven in Afghanistan has been overrun. One of the concerns raised by these successes has been the effect on al Qaeda's command and control. Is it still a unitary group, planning and ordering attacks from wherever its leaders

are, or has it, in effect, become a franchised activity, with like-minded cells inspiring one another and occasionally working together but not necessarily in direct command and control? This morphing of al Qaeda into more regionally focused groups was evident in Mali in 2013, for example. The Touaregs in northeastern Mali are a Berber people who felt oppressed by the African rulers who are based largely in the west. Allying with African-based al Qaeda cells was less an expression of a Touareg commitment to terrorism or to jihad than a search for convenient allies. Boko Haram in Nigeria has ties to al Qaeda but has also pledged loyalty to ISIL. Thus, as the campaign against terrorists continues, it will be necessary to discern distinctions between local grievances and alliances of convenience as opposed to actual terrorists. It is also necessary to understand which groups may be in conflict with one another as potential opportunities to combat them. But as NCTC director Rasmussen has noted, this can also serve to create more uncertainty in terrorism analysis as well.

Some of the materials captured in May 2011 after bin Laden's death suggest that he was more involved in ongoing attack planning than had previously been the assumption. Similarly, once an attack has occurred, it is important to know if it has been planned or ordered by an external group or has been carried out by indigenous individuals. The September 11 attack clearly was carried out by terrorists who entered the United States. However, the attacks in Madrid (2004) appear to have been directed by terrorists in Morocco, for whom a direct connection to al Qaeda has not been proven. The 2005 attack in London also appears not to be connected directly to al Qaeda, although some of the bombers had been in madrassas (religious schools) in Pakistan. Similarly, Maj. Nidal Hasan, convicted in the 2009 Fort Hood shootings, was inspired by and in communication with Anwar al-Awlaki, but it has not been established that Awlaki ordered the attack. A conclusion of this sort may be more troubling because it indicates an indigenous problem that will be much more difficult to identify: radicalized, home-grown terrorists. The November 2015 attacks in Paris had a nexus in Belgium, leading to questions about security and intelligence cooperation within the free-travel Schengen Zone. Also, on a per capita basis, more ISIL foreign recruits have come from Belgium than any other European country. It is widely thought that the arrest of one of the Paris terrorists in Brussels precipitated the Brussels attack in March 2016—not the decision on whether or not to attack but the decision to attack then, lest other conspirators be arrested. This question of connections among various terrorist groups also indicates why so much emphasis is put on **link analysis**, that is, establishing connections between various people to get a sense of their broader social networks. This is also one of the major types of information gleaned by phone surveillance, connections between people, in addition to the actual content of their conversations.

War on Terrorists. The intelligence services have two roles in the campaign against terrorists: defense and offense. Defense consists of preventing future attacks by disrupting terrorists or deterring them. This means, in turn, trying to obtain both detailed intelligence about any attacks that are being planned as well as ongoing intelligence about terrorist organizations and their intentions and capabilities. One of the most difficult aspects of defense is learning to think like a terrorist. This means not only being able to conceive of attacks that many analysts would consider too horrific to contemplate for long but also to appreciate the importance of randomness, which is a key ingredient of terror. It has been suggested that terrorist analysts focus too much on specific dates and events (holiday travel periods, major sporting events, national holidays). Although these dates have symbolic value or indicate periods when large numbers of people are either traveling or gathering in one place, they also may be easier to defend against. Of the major terrorist attacks that have occurred to date, only two—the failed Millennium attack at the beginning of 2000 and the attempted on-board bombing of an airliner on Christmas day 2009—were tied to an iconic date. In other words, this may be another case of mirror imaging. How successful are analysts at thinking like terrorists versus thinking like Westerners thinking like terrorists?

Offense consists of identifying, locating, and then attacking terrorists. These activities are important not only for eliminating terrorists but for introducing uncertainty into their activities and making it more difficult for the terrorists to organize, plan, and train. Offensive activities go from analysis into operations and raise questions about assassinations, renditions, detentions, and the continued use of UAVs. As with all other intelligence operations, decisions on these types of activities, or their limits, properly belong to policy makers, not intelligence officers. The war on terrorists adds another intelligence burden: support to military operations. This requirement encompasses both the usual military-related support and new activities. For example, the press has reported that the CIA has a Special Activities Division in the the Directorate of Operations (DO) that was engaged in operations against the Taliban and al Qaeda. Although little is known publicly about the division, it would appear to occupy a niche between Special Forces and the DO's paramilitary activities in support of indigenous groups, such as the contras or the mujahidin. Also, important developments have been made in geospatial intelligence with the use of unmanned aerial vehicles and commercial imagery. All of these issues came into play in the May 2011 operation in which bin Laden was killed. There have been press reports stating that one consequence of the Arab Spring has been the loss of some useful intelligence sources in the security services of the affected states.

One of the most difficult aspects of the campaign against terrorism is trying to gauge the relative degree of success. Unlike conventional wars, there are

no battle fronts moving one way or another. Nor is it clear that the absence of another attack entirely means success. Again, it is possible that the nature of al Qaeda has changed under the pressure of the U.S. response since 2001, going from a more centrally controlled structure to a looser one in which there may be many small centers of activity rather than a central one. If this is so, then the intelligence agencies face uncertainty about what this means for the future of terrorist attacks and for the best way to counter terrorists, both defensively and offensively. It is known that al Qaeda has fairly long planning cycles. Therefore, a quiescent period may simply be somewhere in this cycle. Also, it matters how one thinks about the terrorist issue. Although the United States has not been successfully attacked by al Qaeda since 2001, the other attacks—Bali (2002 and 2005), Madrid (2004), London (2005 and attempted 2007), Algeria (2007), and several others all suggest that it is better to look at the terror issue on a global basis. This certainly appears to be the case after the spate of attacks claimed by ISIL in November 2015. Moreover, in a global and clandestine war, it is difficult for intelligence or security agencies to meet the apparent political requirement of stopping any and all attacks. One of the truisms of warfare is that "the enemy has a will of his own." Although no one wants to be cavalier about future attacks and casualties, a standard of stopping all future attacks is doomed to failure. Terrorists, like any other group, need successes. President Obama said as much in his May 23, 2013, speech at the National Defense University: "Neither I, nor any President, can promise the total defeat of terror." Thus, long periods of no attacks or thwarted attacks can be seen as counterterrorist successes but they cannot go on indefinitely. Controlling the frequency and nature of successful attacks is a more realistic approach than a standard of no future attacks at all.

The death of bin Laden is an important psychological victory, but it is unlikely to mean an end to al Qaeda or other terrorist groups. Whether he is replaceable as an inspirational leader remains to be seen.

For several years, U.S. officials had claimed that al Qaeda was on the verge of defeat. This was based, in part, on the fact that almost all the original core al Qaeda leaders involved in planning the 2001 attacks were either dead or captured. It was also based on analysis, since proved incorrect, that the Arab Spring would undermine the appeal of al Qaeda and similar groups. Instead, the ensuing political unrest offered opportunities for extremists to exploit, particularly in Libya but also in Egypt. The U.S. alert in 2013 that closed nineteen embassies or consulates in the Muslim world appeared to undercut claims of success, as the threats were al Qaeda–based, centering on al Qaeda in the Arabian Peninsula (AQAP), which operates out of Yemen. There is broad agreement that al Qaeda has morphed into more regionally based pockets, as noted above, although in the case of the 2013 alert there were apparently

communications between Ayman al-Zawahiri, who succeeded bin Laden as the head of al Qaeda, and Nasser al-Wuhayshi, the head of AQAP. (Some commentators also thought that the Obama administration wanted to avoid another embassy assault like that in Benghazi in 2012. See chap. 9.) It is probably necessary to draw a distinction between the ability of these groups to conduct terrorism in their regions and their ability to conduct large-scale operations against the United States or Europe similar to 2001 and 2015. This does not mean that U.S.-targeted operations are no longer possible, but they have likely become much more difficult to conduct. It is also important to recognize that a group (or military) can be losing but still be capable of some offensive action.

There has also been a change in the terrorist threat with the rise of "lone wolves," terrorists acting on their own who may be motivated by various radical ideas but who are not controlled by terrorist groups. The Tsarnaev brothers, who attacked the Boston Marathon in 2013, fall into this group, as may Maj. Hasan. Lone wolves are, by definition, more difficult to spot in advance of their acts and again raise difficult questions about civil liberties and surveillance. The December 2015 San Bernardino, California, attack can be characterized as a lone wolf, albeit possibly inspired by ISIL. The possibility of ISIL volunteers returning to the United States or other countries, possibly to commit terrorism, has increased the lone-wolf concern.

Lessons Learned. For each of the nations that have been attacked, the degree to which they have learned the lessons that led to their earlier vulnerability is an important question. For the United States, however, the "lessons" of September 11 are not necessarily clear or agreed upon. There does seem to be agreement that information sharing, especially between the CIA and the FBI, was highly flawed, although it does not necessarily follow that the numerous improvements made in information sharing will foil the next attack. Better sharing techniques and technologies are hollow if the necessary information or intelligence is not available. The 9/11 Commission and some other analysts have catalogued several missed opportunities in the period before the September 11 attack that they believe might have disrupted the plot. The problem, analytically, is that almost all of these missed opportunities would have had to fall into place, and even then the outcome would be uncertain. We know, for example, that the attackers had substitutes in case some were denied entry into the United States, as did happen. No critic, including the 9/11 Commission, has shown how the missed opportunities would have led to the tactical intelligence necessary to identify the specific four flights on September 11. It is also important to keep in mind that many of the security practices that we now take for granted did not exist on the day of the attack. Part of

the problem in assessing the causes of the attack is also political. It is more comforting for the public and for officials to believe that we can identify and remedy the several factors that made us vulnerable in 2001 because then we can return to some greater sense of safety. But if the flaws are more subtle than some believe or if the remedies appear to be more difficult to implement, then we must live with a continuing sense of vulnerability.

Moreover, the repeated emphasis on information sharing and on checking "all of the databases" runs the risk of creating analytical paralysis. Analysts may become so concerned about sharing and about checking all available data that they cannot bring themselves to act on the information or to set others into action out of fear that something may have been missed. Neither extreme is correct and much depends on the nature of the situation, but it can be argued that the emphasis on information sharing has reached a point of minimal further returns. The reaction to the failed December 2009 attempt to set off a bomb on an airplane landing at Detroit is instructive. One of the U.S. reactions to Umar Abdulmutallab's ability to come as close as he did to a successful attack was to expand the watch list of people either suspected of being threats or banned from flights. Although an expanded watch list may make it less likely that a would-be terrorist can board a plane, it also increases the amount of searching that has to be done to make the watch list system effective. For example, according to press reports in 2012, the "no fly" list doubled to more than 21,000 names in one year.

The access to fairly broad amounts of intelligence given to and exploited by Bradley Manning and Edward Snowden is likely to have the effect of setting greater limits on access and intelligence sharing, thus undoing some of the changes made after 2001.

The September 2001 attacks raised new questions about intelligence–law enforcement organization, coordination, and cooperation. DHS, the National Counterterrorism Center (NCTC), and the FBI's new National Security Branch are all efforts to deal with this issue. The 2004 intelligence reform law puts a major emphasis on information sharing, which is an important aspect of all intelligence. There have been recurrent discussions about whether the United States needs to create an MI5, referring to Britain's Security Service, which is responsible for domestic security and is part of the Home Office. (See chap. 15 for details.) The FBI is not quite analogous to MI5 and has limits on what it can do beyond those activities that are considered federal crimes. The FBI has had difficulty making the transition to greater emphasis on terrorism and also had difficulty making the shift from a largely law enforcement agency to more of an intelligence agency. The legal difficulty encountered in the United States is inherent in the federal system, which places responsibility for local law enforcement on the states and their cities or counties. As a means

of improving liaison between the federal and local levels, a series of fusion centers, called **Joint Terrorism Task Forces (JTTFs)**, have been formed, although the majority of them tend to be staffed by state law enforcement personnel. Their ability to provide the desired liaison and integration and future remains uncertain.

The rather large and rapid proliferation of federal, state, and local offices to deal with terrorism has also attracted criticism—from the DHS inspector general, the Government Accountability Office (GAO), and a Senate subcommittee—about unnecessary overlapping, lack of communication, useless reporting, and the inevitable reorientation of some state and local resources back to traditional police issues. GAO also found that DHS helped the fusion centers create "baseline capabilities" but questioned whether these had any effect on homeland security—in other words, the ability to relate outcomes to expenditures. The fusion centers have been a particular source of concern. Some of this may be unavoidable in a complex and large federal republic, but these critiques also suggest that it may also be useful to review the structure, number, and role of these various centers. Part of the problem is political. These various centers are sources of federal funds for localities. Second, no one wants to scale back or shut down a fusion center and then have an attack take place, with the inevitable questions that will follow. President Obama's May 2013 speech may signal a change of emphasis.

Once one gets beyond the traditional national security community, the issue of clearances comes up. Very few officials at the state, local, and tribal levels have clearances. Very few seem to want them. So an immediate issue is how to pass along terrorist information without revealing sources and methods. This issue first arose as DHS was being formed. Sen. Richard Shelby, R-AL, insisted that DHS have access to all raw intelligence. DCI Tenet refused to go along with this and was supported by the incoming DHS secretary, Tom Ridge. Ridge stated his view that if the DCI passed threat information, then he (Ridge) would assume it was well-sourced and needed to be acted upon. This rather commonsense approach is preferable to either withholding information from first responders because they are not cleared or requiring that they obtain clearances.

A more serious problem is doctrinal. Over a decade after 2001, U.S. policy makers and intelligence officers are still working out what homeland security intelligence (sometimes called HSINT—pronounced "hiz-int") means. Doctrine matters because it helps determine what intelligence needs to be shared with whom and how quickly. This discussion is still under way, but some have advocated that DHS serve as a bridge between federal intelligence agencies of all sorts and the first responders, helping translate national intelligence down to the first responders and helping pass along detailed local knowledge from the

first responders to the intelligence agencies. This means that DHS would take on responsibility for deciding which threats were passed and which were not, undoubtedly in consultation with other intelligence agencies. Some criteria for selectivity are crucial. Otherwise, DHS becomes a pass through for all threats, flooding the first responders, who recognize that they cannot protect everything all the time and want, most of all, vectoring information to help them safeguard those targets that are most threatened. It is important to recognize that the intelligence agencies and the first responders are working in a relatively new field and still working out the parameters of their actions and their interactions. DHS's Office of Intelligence and Analysis (I&A) is its main—but not only—counterterrorism locus, but I&A has struggled to come up with a meaningful doctrine and role, despite having had a succession of highly skilled veteran intelligence officers as undersecretary. This would seem to suggest that the problems are institutional rather than in leadership.

The FBI has also experienced some difficulties in responding to the terrorist threat, particularly in making the transition from being almost exclusively a law enforcement agency (albeit with some intelligence tasks, particularly counterintelligence) to an agency with a greater intelligence analytic role. Congress mandated the creation of a Review Commission to look at the FBI's role in homeland security. The March 2015 report noted areas where the FBI had made improvements and also noted the need to improve the FBI's intelligence capabilities, particularly in elevating the status of intelligence analysts.

But even information sharing is dependent, first, on information collection. For example, none of the investigations of September 11 found evidence that the one or two pieces of intelligence that might have led to the plot were somehow misdirected or not shared. Such evidence was never collected and may not have been collectible. Officials have also raised concerns about cyber attacks on the United States as part of a terrorist campaign. The main fear is that such actions could affect vital parts of the U.S. infrastructure. Such an attack would likely have even fewer indicators, and the perpetrators might never be known after the attack.

It has been suggested that more time be spent on studying past terrorist efforts, virtually all of which failed to achieve their objectives despite rather lengthy periods of activity. Certain features begin to emerge. First, like all other activities, terrorist operations need success to maintain momentum and to recruit new adherents. This can prove to be a vulnerability for terrorists, as any disruption or deterrence is the equivalent of a defeat. On the other hand, it only takes one spectacular attack to regain momentum. ISIL, however, would appear to be successful in this regard and has attracted recruits from many countries, based less on its appeal as a terrorist group than on its religious

propaganda as the new caliphate, seeking to draw all of the faithful to its banner. Second, it appears that later generations of terrorists are somewhat less fanatical and more susceptible to negotiation—assuming that there is something about which to negotiate. Again, the religious aspect of early twenty-first-century terrorism makes this very difficult. Third, it is important to note that the current campaign against terrorists has created a series of operational and ethical dilemmas not only for intelligence officers but also for the policy makers who direct them. Much of this stems from the sheer novelty of conducting operations against terrorists on the scale that has evolved since 2001. As noted, terrorism has been an issue for U.S. intelligence since the 1970s, but these involved specific groups or individuals. Those terrorists who were apprehended could be tried for specific acts. Post-2001, the scope has widened. In addition to seeking individuals who can be brought to trial, there is a need to destroy terrorist cells and networks by apprehending or killing participants. But these individuals fall into a somewhat uncertain legal status, being neither enemy combatants in the way in which uniformed soldiers of nations are nor indicted criminal suspects.

Operations and intelligence collection against known or possible terrorist threats have also raised legal and ethical issues for intelligence. As noted, the United States has conducted renditions (that is, extraterritorial arrests) that have become issues between the United States and some of its allies, although it is likely that there was knowledge of the U.S. activities at some level in most of these governments. Once captured, some terrorists have been transferred to other nations for interrogation. Critics, including the Senate Intelligence majority staff report, charged that this allowed U.S. intelligence officers to use extraordinary interrogation techniques beyond U.S. territory or to have terrorist suspects be interrogated in nations where harsher methods are sanctioned. This, in turn, led to a debate within the United States about the use of techniques that might be deemed torture. According to press reports, there have been renditions in the Obama administration as well as the George W. Bush administration.

As noted, there has also been a debate about the efficacy of harsher techniques. The Senate Intelligence Committee majority staff report and other critics argue that information obtained under these circumstances cannot be reliable. Several former CIA directors have disagreed, as has the current DCIA, John Brennan.

In addition to these controversies, there have also been issues raised about several means by which intelligence agencies have collected terrorist-related intelligence. The NSA Internet and telephone programs leaked by Edward Snowden are prime examples. The Treasury Department used a tracking program to trace financial transactions within SWIFT (Society for

Worldwide Interbank Financial Telecommunications). Tracking and, where possible, preventing the transfer of funds to terrorists is an essential part of the counterterror strategy. Access to SWIFT allows analysts to know who is transferring funds, the amounts, and the accounts. Press revelations raised the usual concern about privacy. Interestingly, Congress was supportive of the effort to glean useful intelligence from SWIFT. After some European opposition in 2010 to continuing this cooperation, it was renewed, allowing the sharing of bank transfer data presumed to be connected to terrorism. Again, civil liberties groups in Europe and the United States have raised concerns. The FBI came under criticism for its use of national security letters (NSLs), as was discussed in chapter 7.

Several points stand out across these various efforts. First, as stated earlier, the campaign against terrorists has forced the intelligence agencies to reexamine how they operate and the types of information that may be useful. Second, these efforts underscore the multifaceted aspects of countering terrorism and the difficulties inherent in combating it. The terrorism target is, in many ways, much more complex than was the old Soviet foe. Third, even with a well-conceived collection plan, it will be very difficult to coordinate all of these efforts and to use the collected data in ways that produce meaningful results, as opposed to overwhelming analysts with huge databases. Fourth, these efforts will increase the demands for oversight of intelligence, both internally and externally.

The use of drones against terrorists raises several issues. First, the drones are key intelligence collectors, especially in areas where there is not much other access, such as the Afghan–Pakistan border, Yemen, and Somalia. Second, armed drones have proven to be effective tools in killing known or suspected terrorists; their use has increased as much as fourfold under the Obama administration. As will be discussed later (see chap. 13), the United Nations (UN) has raised objections about how the United States uses drones for attacks. Targeted killings of terrorists also became an issue in the case of U.S.-born Anwar al-Awlaki, who had promoted terrorist attacks against the United States and appeared to be connected to several attacks, including that of Maj. Nidal Hasan. The Obama administration reportedly approved placing al-Awlaki on the target list, raising constitutional issues about the deprivation "of life . . . without due process of law" under the Fourth Amendment. The Obama administration argued that international law allows the use of lethal force against persons deemed to be an imminent threat.

Finally, there is the issue of the overall operational tempo at which the counterterrorist campaign has been conducted for over a decade. This has been difficult to sustain for the armed forces as well as for intelligence operators and analysts.

Proliferation

Preventing the proliferation of WMD has been a long-standing goal of U.S. policy, but it is now a more important issue with added dimensions. The United States has always given primary emphasis to nuclear weapons, given their lethal capability and the fact that they were central to the U.S.–Soviet relationship. But even during the cold war, the United States also worked to contain the spread of chemical and biological weapons (CBW or CW and BW). The nexus between terrorism and WMD has given added importance to the issue. Since the Iraq WMD estimate in 2002, intelligence efforts regarding proliferation have been an ongoing source of controversy and of political and sometimes partisan debate.

There are two major strands in proliferation, which are not entirely separate. The first is the requirement to keep track of the WMD activities of nation-states, both for their own sake as factors in regional stability and as possible sources of material to terrorists. Then there is the terrorist nexus itself. Al Qaeda has stated bluntly that one of its goals is to obtain WMD—again, simplifying the intentions question but not the capabilities question. The primary concern in state-based activity is nuclear weapons, although some attention is paid to the CW and BW programs of various states as well. There clearly has been an unwelcome shift in nuclear proliferation since 1998, when India and then Pakistan tested nuclear weapons. Since then, North Korea has claimed to have tested a nuclear weapon twice (October 2006 and April 2009). The February 2004 admissions by Pakistani A. Q. Khan also made public the details of a web of private firms and experts trading in nuclear expertise and technology. In April 2011, the International Atomic Energy Agency (IAEA) confirmed that the Syrian site destroyed by Israeli bombers in September 2007 had been a covert nuclear reactor. There has also been some preliminary success in the agreement between Iran and the P5+1 (the five permanent members of the UN Security Council—the U.S., Britain, France, China, and Russia—plus Germany). However, as noted later, this agreement will raise new intelligence tasks and questions.

Role of Intelligence. The task for intelligence agencies is to identify which nations may be pursuing any or all WMD and then try to determine the state of their programs, as well as connections to other programs, sources of material, expertise, and so forth. This also represents a shift, as a *sub rosa* network of technology and expertise has developed, complicating efforts to isolate and understand programs. The most obvious problem is that these programs all operate covertly and often rely on facilities that are difficult to find. In September 2009, the United States, Britain, and France briefed the IAEA on a hitherto secret Iranian nuclear facility near Qom. Press articles stated that

Western intelligence had been tracking the site since 2006 but it had not yet received public attention. In November 2010, North Korea revealed a new uranium processing facility at its Yongbyon complex, where major facilities had been disabled in 2007 and 2008. Despite Yongbyon's importance as a proliferation intelligence target, the extent and sophistication of these new facilities came as a surprise to many North Korea "watchers." Even when suspect sites are discovered, some of them may have perfectly legal, nonlethal applications as well. This is certainly true of nuclear programs, which can have connections to peaceful uses of nuclear material, such as power plants. At the same time, peaceful nuclear programs can serve as cover for clandestine weapons development.

U.S. intelligence efforts on proliferation continue to be seen through the prism of the October 2002 NIE on Iraq WMD. The absence of WMD in Iraq was a major factor in the impetus behind the 2004 intelligence legislation, which ostensibly addresses the issue of combating terrorism. Of the two issues—September 11 and Iraq WMD—the Iraq issue is far more serious in terms of the future of the intelligence community. For all of the pre–September 11 warnings about al Qaeda hostility, including the possibility of the use of aircraft, insufficient intelligence existed to act upon and disrupt the plot. Nor, in the pre-attack atmosphere, would it have been possible to implement the types of security steps in place now. The Iraq WMD issue, however, raised serious questions about analytic tradecraft, not only in WMD issues but also across the board. The Senate Intelligence Committee focused on the problem of groupthink, but more serious issues may have been at play:

- The effect of not allowing analysts better insight into the nature of HUMINT sources
- The proper way to pose alternative analytic questions that yield true alternative hypotheses instead of supporting or simply refuting the current one
- The need to rethink the prevalence of denial and deception (see chap. 6)
- The larger estimative process (see chap. 6)

The proliferation issue was then made even more contentious politically by the release in December 2007 of the unclassified Key Judgments (KJs) of a new NIE on Iran's nuclear program, which concluded that Iran had halted its nuclear weapons program in 2003, a reversal of the judgments made in a 2005 estimate. As noted earlier, this NIE was also controversial, with some observers questioning whether analysts had political motives in writing these judgments. Again, as noted earlier, a 2015 analysis by the IAEA (International Atomic

Energy Agency), based on partial Iranian responses to questions about its past activities, said Iran was actively designing a nuclear weapon until 2009 but that coordinated efforts to create weapons stopped after 2003, largely agreeing with the NIE.

Iraq WMD, like the Cuban Missile Crisis and a few other intelligence experiences, will probably be a touchstone for years to come in debates over intelligence analysis. (Iraq may also have an ironic and dangerous effect on other would-be proliferators. The lesson they may take away from Iraq's fate could be this: Get a nuclear weapon. Iraq, without a weapon, was overrun with impunity, whereas North Korea, which claims to have tested nuclear weapons, had received some aid in exchange for pledging to end its nuclear weapons program. Libya may offer a similar "lesson," having given up its WMD programs in 2003 and then being attacked by NATO in 2011.)

The role of intelligence in the WMD policy area is fairly obvious: identify proliferation programs early enough to stop them before they are completed. As former DCI Tenet noted in his memoirs, for proliferation policy to be successful, intelligence must identify and discern the nature of a program before a test occurs, not record the fact of a test, as was the usual case in tracking Soviet weapons developments. Intelligence also targets the clandestine international commerce in some of the specialty items required to manufacture WMD. Again, proliferation programs are, by their very nature, covert. Thus, the types of collection that the United States must undertake tend to come from the clandestine side of the intelligence community. The evidence of nascent programs—as well as mature programs—that U.S. intelligence might obtain may be ambiguous. Fuzzy information complicates the ability of policy makers to confront potential proliferators with confidence or to convince other nations that a problem exists. As the exposure of Khan's nuclear proliferation network shows, however, doing so is not an impossible task. But it is time-consuming (the effort against Khan went on for years) and sensitive diplomatically. In the case of the Khan network, the sensitivities of Pakistan had to be taken into account, given its stated support for the war on terrorists. Khan's activities also confirmed the international nature of nuclear proliferation. His enterprises spanned three continents and may have been involved in more than just the Pakistan and Libyan programs. This points up another intelligence challenge: determining how vast the interconnections are between would-be proliferators and would-be providers. Although the disruption of the Khan network was a major intelligence success, parts of the program could continue to operate without Khan's guidance.

A January 2014 report by the Defense Science Board was rather pessimistic about the future of nuclear proliferation, suggesting that there would be more potential actors and states that needed to be watched and that current

capabilities for verification, inspection, and monitoring (see below) are inadequate to meet future needs.

The completion of the Joint Comprehensive Plan of Action between Iran and the P5+1 that went into effect in October 2015 brings intelligence back to the familiar field of arms control **monitoring** and **verification**. As noted earlier (chap. 1), it is important to understand the difference between these two activities. Monitoring is an intelligence activity, keeping track of activities in foreign countries. U.S. intelligence conducts monitoring because the activities in certain countries are of importance to U.S. national security. Monitoring occurs whether or not there are arms control agreements. During the course of monitoring, activities may be observed that call into question compliance with agreements. These activities are reported to the policy community, which then makes a policy judgment on verification—that is, whether or not the activity in question is a possible violation and what should be done about it.

Although the distinction between the intelligence and policy functions in arms control seems clear, politics intrudes and tends to drag intelligence into policy debates. The first order of questioning is the adequacy of the monitoring provisions in the agreement itself. These cannot be ironclad between sovereign states and usually assume some level of cooperation, as well as some level of resistance. Assuming these provisions are adequate—a judgment that the intelligence community is asked to reach—the U.S. military and intelligence community tend to be supportive of such agreements, as they offer some transparency and predictability into weapons programs that are seen as potential threats.

The monitoring provisions of the Iranian agreement are a combination of data disclosures about past activities, monitoring, and inspections. DNI Clapper has said that he was confident that this combination would "make it nearly impossible for Iran to develop a covert enrichment effort without detection." Critics of the agreement raised questions about the decision to allow Iran to collect samples from the Parchin military base, suspected of being a nuclear experimentation site, and to give these samples to the IAEA (International Atomic Energy Agency), rather than have the IAEA collect them. The collection was done, according to the IAEA, where it could be seen by surveillance devices.

Some have also raised questions about the completeness of the data disclosures. The initial position of the P5+1 was that Iran had to be completely forthcoming about its past activities. Arms control agreements often rest on data exchanges, and this was seen, initially, as a necessary part of the negotiation. However, the United States decided that an agreement that dismantled Iran's capability for fifteen years was of greater importance and that the past activity was not entirely relevant given the completion of the agreement. Some question

this approach, arguing that it goes to the question of Iran's honesty and also its overall level of knowledge and expertise once the agreement ends in fifteen years. The December 2015 IAEA report on Iran's past activities was based on Iran's answers to about three-quarters of the questions they were asked.

There will inevitably be Iranian actions that will require clarification and may raise concerns about compliance. For intelligence, this will be very much like the issues that arose during the cold war concerning Soviet compliance with arms control agreements. If the cold war experience is any guide, the debate will break down into two opposing views: (1) those who see any signs of noncompliance as indicators of Iranian bad faith and therefore want to abandon the agreement and Iran's relief from sanctions and (2) those who will argue that the overall agreement is more important than minor transgressions. Decisions on the meaning of activity and resulting actions are political ones and are not made by intelligence agencies, but these agencies will inevitably be drawn into the political debate. In the case of the Iranian agreement, these decisions are made more complex by the fact that it is a multilateral agreement and not a bilateral one. Should the U.S. discover Iranian actions that appear to be violations, it may be necessary to share sensitive intelligence with other powers—including Russia and China—in order to convince them as well. Sharing this intelligence, however, is no guarantee that other powers will agree as to a violation, as they may have diverging interests in terms of the agreement. In October 2015, Iran tested a new long-range ballistic missile just before Iran's Parliament voted to approve the agreement. Some saw this test as a violation of the agreement.

It should also be noted that Russian compliance with arms control agreements returned as an issue in 2014, when the United States accused Russia of violating the 1987 Intermediate Nuclear Forces (INF) Treaty by testing a ground-launched cruise missile (GLCM) banned by the treaty. Russia has refused to address U.S. concerns. This issue—and any possible Iranian violations—take us back to the arms control policy question first raised by Fred Ikle in 1961: "After detection—what?"

Stopping Proliferation. Beyond the problem of amassing convincing intelligence lies this policy question: How can a would-be proliferator be stopped? The preferred means is diplomacy, but the track record in this area is unimpressive. To date, no nation has been talked out of developing nuclear weapons by diplomacy alone. Iran may prove to be an exception, but the 2015 agreement has a fifteen-year duration. Politically, that is a long way off, but it does raise the possibility that in 2030, Iran will be free to begin a nuclear weapons program.

The United States has used its influence, and its leverage as the guarantor of a state's national security, to pressure a state into desisting from nuclear

weapons development. Press accounts allege that the United States used this method with Taiwan in the 1980s. Some other nations—for reasons of their own—decided to abandon nuclear programs. Japan and Sweden chose not to develop programs. Argentina and Brazil agreed bilaterally to abandon their fledging efforts. The white South African government gave up its nuclear weapons and its capabilities on the eve of the black majority's advent to power. Libya's admission in 2003 that it had a range of covert WMD programs that it had formerly denied was largely a result of two factors: successful HUMINT that caught shipments going to Libya and Libya's concerns about potential U.S. actions after the invasion of Iraq. The Libya case was an intelligence and policy success but not a result of diplomacy. Some other states—most prominently North Korea but also Syria—remain unconvinced by U.S. diplomacy. Given the minimal success of moral suasion, some people have argued that the only workable solution is an active nonproliferation policy—intervening to destroy the capability, as both Israel and the 1991 Persian Gulf War allies did with Iraq and as Israel did with Syria. (*See box, "Iraq's Nuclear Program: A Cautionary Tale."*)

Iraq's Nuclear Program: A Cautionary Tale

During the 1980s, Iraq was one of the nations whose nuclear weapons program was closely watched by U.S. experts. The existence of a program was not in question; its status was.

On the eve of the 1991 Persian Gulf War, the considered analytical judgment, according to subsequent accounts, was that Iraq was at least five years away from a nuclear capability. After Iraq's defeat in the war, analysts learned that Iraq had been much closer to success, even though Israel had attacked and destroyed some of its facilities some years earlier.

What had gone wrong with U.S. estimates?

Iraq was a closed target, one of the most repressive and heavily policed states in the world. The state's nature makes collection more difficult, but that is not the answer to the question.

The answer lies in an analytical flaw, namely, mirror imaging. To manufacture the fissionable material it required, Iraq chose a method abandoned by the United States in the early days of its own nuclear program after World War II. The method works, but it is a very slow and tedious way to produce fissionable material.

For Iraq, however, it was the perfect method, not because it was slow, but because foreign analysts disregarded it. The method

allowed Iraq to procure materials that were more difficult to associate with a nuclear weapons program, to mask its status. A program of this sort was also more difficult for Western analysts to spot because they largely dismissed the approach out of hand, assuming that Iraq would want—just as the United States and others had—to find the fastest way to produce fissionable material.

In the course of U.S. military action in Iraq that commenced in 2003, expected Iraq WMD programs were not found. Some wondered if analysts had compensated for their earlier error by overinterpreting evidence of a possible program without considering alternative interpretations. The analysts themselves denied this assessment, and none of the postwar investigations of the intelligence community's performance found overinterpretation to have been a factor.

The September 2007 Israeli air strike against a presumed nuclear site in Syria underscores these concerns as well as the inherent ambiguities involved. After the raid, Syria denied that it had occurred, although subsequent commercial imagery revealed considerable Syrian efforts to both clean up and mask the site by extensive bulldozing. In April 2008, the United States released its conclusion that North Korea had been assisting Syria in building a plutonium processing plant, and not a peaceful nuclear use plant, at the site. As noted, the IAEA confirmed that it was a covert nuclear site in April 2011. There are several issues at play in this incident. First, once again there is the circumstance of unilateral military action being taken as a means of ensuring that the program will be stopped. Second, if there was North Korean assistance to Syria, did this indicate a possible violation of North Korea's agreement with the United States (and China, Russia, and Japan) to cease nuclear weapons activity or, at a minimum, an effort to circumvent that agreement by exporting part of its program? Third, it raises the specter of yet another clandestine nuclear relationship to be tracked. Concerns about Syria per se have likely abated given the Assad regime's preoccupation with the civil war, but the role of North Korea and the broader implications of the event remain problematic.

Pakistan's nuclear weaponry has increased concerns about the stability of the Pakistani government. Two factors are at issue: the fractious internal politics of Pakistan and the internal political effects of Pakistan's cooperation with the United States against Muslim terrorists, including the presumed presence of other al Qaeda leaders in Pakistan. According to press accounts, the United States has given Pakistan technical equipment and assistance designed to help safeguard the security of Pakistan's nuclear arsenal, although this effort has

been made more difficult by Pakistan's reluctance to provide details about the nature and location of its weapons. The concern is that Muslim extremists or officials sympathetic to them will get control of a Pakistani bomb or of the fissile material. The May 2011 operation that killed bin Laden affected the Pakistan nuclear issue in two ways. First, given Pakistani claims that they did not know about bin Laden's presence in Abbottabad, it raised U.S. concerns about Pakistani ability to detect threats and to safeguard their nuclear arsenal. Second, the success of the U.S. raid raised Pakistani concerns about some future U.S. operation intended to take over some part of that nuclear arsenal. Press accounts characterize Pakistan's nuclear arsenal as "the fastest growing" today. Immediate U.S. concerns focus on the development and possible deployment of tactical nuclear weapons, which would be much smaller, much more difficult to track, and much easier to steal.

The loose nukes aspect of the issue adds a new and more difficult complication. The Soviet Union agreed with the goal of nuclear nonproliferation, recognizing that it could be a target of would-be proliferators. The prospect of tracking unknown quantities of weapons-grade material (which even Russian and other authorities have been unable to account for with accuracy) and the international movement of experts from former Soviet states is an even more difficult and more troubling issue. The collapse of the post-Soviet economy and the end of the privileged status that scientists once enjoyed were seen as incentives to would-be proliferators.

CW and BW proliferation require much less expertise and technical capability than nuclear proliferation does. CW and BW weapons are far less accurate than nuclear weapons, but the random terror they portend is part of their appeal to nations and terrorists. Such programs are more difficult than nuclear programs to identify and track. The anthrax scare in the United States in late 2001 underscores these points and also indicates how difficult it is to detect this type of attack in advance or to stop it once under way.

The use of CW in the Syrian civil war is also illustrative. The initial question was whether or not CW had been used, especially in a Damascus neighborhood in March 2013. Various states claimed that they had intelligence of the attack, but it was not until the UN inspectors reported in September 2013 that this was confirmed, although the UN report did not place blame for the attack. The Syrian government and its backer Russia continued to claim that the attacks were conducted by the rebels. However, the imminent prospect of a U.S. air attack led to a U.S.-Russian agreement on the elimination of Syria's CW arsenal, which Syria now admitted to possessing, after decades of denial.

The intelligence experience in WMD is mixed. In Iraq, the analysis did not bear out. The exposure of A.Q. Khan's network points out the importance of years of determined analysis and highly successful operations to penetrate

the network until enough intelligence had been established to make the case incontrovertible. The Libyan surrender also owes much to years of collection, analysis, and some highly successful operations. There was also an important benefit years later, when NATO confronted Muammar Qaddafi over his efforts to suppress a revolt, knowing that a large part of his WMD had been removed. Reactions to the 2007 Iran nuclear NIE indicate the continuing controversial nature of proliferation intelligence.

In short, intelligence can bring important assets to bear on WMD proliferation, but it will always be a shadowy area and one liable to analytic missteps. It has become increasingly difficult for the intelligence community to produce analysis on proliferation without its being received in a highly politicized manner. This is the sort of distraction that analysts are taught to rise above or to ignore, but this makes it increasingly difficult to write objectively on proliferation.

Narcotics

Narcotics policy is a difficult area in which to work. The main social policy goal is to prevent individuals, by a variety of means, from using drugs that the government deems addictive and harmful. Almost everyone who has ever worked on narcotics policy has said that it is a domestic issue, not a foreign policy issue. Also, given the fact that individuals use drugs for numerous reasons, preventing their use is a difficult goal to attain. For both practical and political reasons, narcotics has become, in part, a foreign policy problem, because the United States attempts to reduce the overseas production of illegal drugs and to intercept them before or just as they arrive in the country.

The intelligence community is capable of collecting and analyzing intelligence related to the illicit trade in narcotics. The plants from which certain narcotics are derived can be grown in large quantities only in certain parts of the world. Coca is produced in the Andean region of South America. Poppies, from which heroin is made, are grown predominantly in two parts of southern Asia, centering roughly on Afghanistan and Myanmar (formerly Burma). Areas where these plants are processed into narcotics are also fairly well known, as are the routes customarily used to ship the finished products to customer areas. Drugs like methamphetamines, which can be made in small laboratories, present a more difficult policing problem.

The real problem lies in converting this intelligence into successful policy. Efforts at crop eradication and substitution stumble on the simple economic choices facing local farmers. Narcotics crops pay more to growers than do food crops. Processing facilities, although U.S. intelligence can locate them,

tend to be small and numerous. Drugs are so profitable that small amounts, which are easily shipped, are economically attractive. Shippers can use any number of routes, which they can change in response to pressure and efforts at interdiction. Finally, narcotics activities yield money in sufficient amounts to subvert the local authorities—civil, military, and police. This has been a persistent problem in Mexico, where competition among narcotics traffickers has also led to increasing violence across the country and just across the border from the United States. Thus, narcotics becomes an issue in the possible destabilization of the southwestern border of the United States. As noted, the Obama administration agreed to support Mexican counternarcotics efforts with the use of unmanned aerial vehicles (UAVs) over the shared border.

All experienced policy makers point to the importance of a domestic answer. If people do not have an interest in using illegal drugs, then everything else—growth, processing, shipping, and even price—becomes irrelevant. The drugs become valueless commodities. But the elusiveness of a successful domestic response leads policy makers back to foreign policy. (Legalizing drugs might not have the same effect on production and distribution as eliminating demand, because a black market might arise to compete with government-approved providers.)

The conjunction of the narcotics trade with international crime and with terrorism adds a further dimension to the intelligence-gathering and policy-making problem. The profits from sales of narcotics, instead of being an end in themselves, now become the means to fund a different end. Also, new and more difficult demands are put on intelligence, because terrorists and criminals operate clandestinely. The United States must be able to establish intelligence about networks, contacts, relationships among individuals and groups, flows of capital, and so forth. For example, guerrilla and right-wing paramilitary groups in Colombia used cocaine to finance their operations. It therefore becomes necessary to draw distinctions between various narcotics producers in terms of their relative importance as an intelligence and policy priority. During the crack cocaine epidemic in the United States in the 1980s, the key areas of concern were Peru and Colombia. However, with the rise of terrorism as a priority, much greater attention was put on the opium crop in Afghanistan.

Finally, narcotics crosses the line between foreign and domestic intelligence and between intelligence and law enforcement. The point at which an issue is handed from one agency to another is not always clear but is important, raising both practical and legal questions, some of which can impede prosecution. The status of the Drug Enforcement Administration (DEA) is an interesting bellwether. Formally part of the Justice Department, the DEA has moved in and out of the intelligence community. The DEA was considered to be part of the intelligence community in the late 1970s and early 1980s but

then reverted to its former position as a law enforcement agency. In 2006, however, the DEA's Office of National Security Intelligence was formally made part of the intelligence community specifically because of the link between drugs and terrorism.

Economics

Economics can be subdivided into several issues: U.S. economic competitiveness overseas, U.S. trading relations, **foreign economic espionage** and possible countermeasures, and the intelligence community's ability to forecast major international economic shifts that may have serious consequences for the U.S. economy.

During the late 1980s, some people maintained that several of these issues (overseas competitiveness, trading relations, foreign economic espionage, **industrial espionage** undertaken by businesses, and possible countermeasures) could be addressed, in part, through a closer connection between intelligence and U.S. businesses. Few advocates of closer intelligence–business collaboration, however, had substantial answers for some of the more compelling questions that it raised (which is one reason that this approach was quickly rejected):

- If the intelligence community were to share intelligence with businesses, how would they safeguard the sources and methods used in obtaining the information? If the underlying sources and methods could not be shared, would businesses accept the intelligence?
- With whom would the intelligence be shared, or, in other words, what constitutes a "U.S. company"? In an age of multinational corporations, the concept is not easy to define.
- Given that every business sector has many competitive businesses, which ones would the community provide with intelligence? What would be the basis for selecting recipients and nonrecipients of the intelligence?
- Would providing intelligence be part of an implicit quid pro quo on the part of the government—that some action should or should not be taken by industry in exchange for access to intelligence?

Foreign Economic Espionage. The collection of foreign economic intelligence by other nations was also controversial. An aggressive collection policy was central to those proposing greater intelligence support to business. Supporters of the policy cited cases in which supposed friends of the United States, such

as France, were caught engaging in such activity. Advocates saw similar activity by the United States as fighting fire with fire. Critics argued that to do so would justify the initial hostile action. They also raised some of the arguments about the limits on how such information might be used. But then-DCI Gates put it best when he said that no U.S. intelligence officer was "willing to die for General Motors."

Allegations of U.S. economic espionage arose in the late 1990s concerning a government program called **ECHELON**. In simplest terms, ECHELON searches through collected SIGINT, using key words via a computer. Key-word searching allows more material to be processed and exploited. Some European officials claimed that ECHELON was being used to steal advanced technology secrets, which were then being passed to U.S. firms to enhance their competitiveness. Former DCI R. James Woolsey (1993–1995), in a stinging article in 2000, held that ECHELON was used to detect attempts by European firms to bribe foreign officials to make sales and to uncover the illicit transfer of dual-use technologies—technologies that have both commercial and WMD applications, such as supercomputers and some chemicals. Cyber intrusions have now become the major focus of concern in safeguarding competitive economic information. China has been the main center of U.S. attention, although this has been blunted somewhat by the Snowden revelations, which undercut some of the U.S. position. As noted above, presidents Obama and Xi reached "common understanding" in September 2015 not to use cyber intrusions to steal intellectual property.

U.S. policy makers viewed foreign economic counterintelligence as largely noncontroversial. Most of them considered it a proper response to foreign economic intelligence, although questions were raised about the extent of the problem. Press accounts of the issue often cited the same shopworn cases, creating echo—the impression of a larger problem through repetition. But the problem may be underreported, given that many businesses do not want to admit that they have been the victims of successful foreign intelligence operations or of major cyber intrusions unless they have no choice, as in the case of the loss of customer data. Some people also argue that foreign economic counterintelligence, although necessary, treats the symptom but not the cause. They acknowledge that blunting attempts at economic intelligence collection may be important but contend that the issue should be addressed at a political level—perhaps by negotiations that offer nations the choice of cessation or countermeasures.

Legislation passed during the 105th Congress (1997–1999) extended the role of FBI counterintelligence in the business information area, which has been controversial. The legislation reflects a continuing expansion of FBI authority in the gray areas between foreign and domestic intelligence and between intelligence and law enforcement.

Forecasting Major Economic Shifts. Beyond the counterintelligence aspects of economics is the day-to-day tracking of trends and events. At least four serious currency-related crises have occurred since the end of the cold war. In 1995, Mexico experienced a peso meltdown, which the intelligence community apparently handled well, giving policy makers significant advance warning. In 1998, the two-year Thai economic crisis turned into a full Asian economic debacle, encompassing Indonesia, Malaysia, the Philippines, and South Korea. Little has been said about intelligence performance in this crisis. The 2000–2001 Argentine financial collapse was long evident. The global recession that began in 2007 with the collapse of the housing bubble in the United States, which many had foreseen, then played out internationally to a depth that was largely unexpected. The ensuing crisis in the Euro-zone was perhaps the primary example of unforeseen consequences. The likelihood that other such crises will occur in years to come underscores the importance of economic intelligence in this area, especially given the greater interrelatedness of the global financial market.

Competition for Materials. Trends in international trade are of obvious national interest. There is a growing international competition for raw materials, primarily between China and India—which are still industrial (as opposed to post-industrial) states—but involving other nations as well. This competition includes oil, iron ore, and other minerals. The China–India rivalry is important because it affects world commodity prices and it has political ramifications. For example, China was reluctant to press Sudan's government to allow foreign peacekeepers into the Darfur region, where the Sudanese government conducted a genocidal ethnic war against local tribes, in part because Sudan is an increasingly important source of oil for China. This competition also reveals a dependency in terms of China, in particular, sustaining its economic growth, which can become useful in developing opportunity analysis.

China's predominant control of rare earth metals, estimated by some to be 95 percent, became a concern. These elements are crucial for a variety of advanced technologies, including computers and cell phones. China's manipulation of rare earth metal exports has serious industrial and trade implications, but it also must be examined as a possible insight into how China views its role internationally.

Energy. Oil and natural gas are also important economic intelligence issues for several reasons. The most obvious is their effect on the domestic economy. In addition, control of energy supplies translates into both a source of income and political power. What is interesting is the sheer volatility of this sector and its effects. Beginning with the Arab oil embargo of 1973, the general consensus

was that the oil-producing states, concentrated in OPEC (Organization of Petroleum Exporting Countries), would have continuing streams of wealth and great power given Western dependency. However, OPEC proved to be a fractious bloc, with various members violating production quotas for reasons of their own. At a certain point, politics trumped energy, with Saudi Arabia making up for shortfalls caused by embargoes on Iraq or Iran. In the first decade of the twenty-first century, the high international energy prices became important factors in the re-emergence of a more powerful Russia, whose economics are wholly dependent on the export of commodities (oil, gas, gold, timber) and in the less compelling power of problematic states like Venezuela and Iran—although Iran was limited by sanctions tied to its nuclear program. There is also another nexus to terrorism, as the Saudi oil fields are both a target for terrorists as a means of disrupting Western economies, one of al Qaeda's stated goals, and an economic opportunity, should al Qaeda succeed in taking over the Saudi kingdom.

However, by the second decade of the century, energy power had shifted again. New methods for extracting oil and natural gas have led to new estimates that suggest energy independence for the United States in about two decades and a worldwide glut of natural gas, which directly affects Russia and its leverage over parts of Europe if liquid natural gas (LNG) facilities can be built in Europe to allow new gas supplies. Saudi Arabia has purposely kept oil production high in order to suppress prices, a policy aimed at Russia and Iran, even though Iranian oil was sanctioned, and at the emerging new shale sources in the United States. With Iran now free to export again as part of the nuclear agreement, the likelihood is that oil prices will remain low or go lower. Several intelligence questions follow. The first is the accuracy of any oil market prognostications. The second is the likely geopolitical effect of markedly lower prices on key players. How long can Saudi Arabia afford to produce oil below its necessary price level? How will Iran react to the possibility that sanctions relief does not translate into economic gain? Finally, how will Putin react to a declining Russian economy? Will this make him seek foreign adventures to divert Russian public opinion?

Finally, economics are always important as a possible precipitating cause of political instability. This can range from the stresses felt in the European Union to the recurring concerns in the Chinese government about its ability to hold onto power should the growing but still nascent economy stall or experience a recession.

Financial Intelligence. An increasingly important part of economic intelligence is financial intelligence (sometimes called **FININT**)—in simplest terms, following money flows, especially those related to illicit or illegal activities.

Today, it is no longer necessary (or practical) to move large sums of money physically. Most major transactions, either domestic or international, take place electronically, over the World Wide Web. Therefore, financial intelligence quickly shades into cyber intelligence as well.

Several activities are of interest in financial intelligence. Some are rather obvious, such as terrorism and narcotics trafficking. Others include proliferation; international sanctions regimes; and corrupt practices, such as bribery or money laundering. As noted above, the SWIFT system tracks movements of money in the international banking system. But now there is the advent of "crypto-currencies," such as Bitcoin, a peer-to-peer payment system that relies on a block chain, a continuously updated database that acts as a ledger for all transactions within Bitcoin. Bitcoin and other similar products have been variously characterized as a financial service or a virtual currency, according to the U.S. Treasury. The value of Bitcoins has been highly volatile, ranging between US$0.30 and US$1,242 between 2011 and 2013. (In May 2016, Bitcoin was valued at US$454.) Because there is no banking intermediary, Bitcoin and other crypto-currencies have an obvious appeal for illegal transactions or even for licit transactions involving large sums that might attract unwanted attention.

There is also a law enforcement aspect to financial intelligence, providing information used to ensure the enforcement of various banking and securities laws.

In terms of collection, financial intelligence will be primarily SIGINT or HUMINT and some OSINT as well. The analytic burden falls primarily on the Treasury Department, which has had an Office of Intelligence and Analysis (OIA) since 2004. (There had been an Office of National Security at Treasury since 1961.) OIA is part of the intelligence community and focuses on the financial aspects of the various issues noted above. There are several other offices at Treasury dealing with aspects of financial intelligence, and they all (including OIA) come under an undersecretary for terrorism and financial intelligence.

Demographics

Demographics, the characteristics of population in terms of age and sex distribution, is not usually thought of as an intelligence issue, but may become one over the next several years. The often used, and often disagreed with, characterization is that "demographics are destiny."

The issue for the intelligence community is how certain demographic trends will affect the stability and behavior of various states or regions. There

are two major concerns, both of which focus on divergences from the normal distribution of age groups within a population. Simply put, there should be fewer old people and more young people because of birth rates, death rates, and life expectancy. The numbers should be in some rough proportion, often ideally portrayed as a pyramid, with the younger groups at the bottom and the older at the top. A key part of the pyramid is the middle band, those people who can work to support the young and the old.

However, there are a number of nations where the ratios are skewed. In Africa, South Asia, and the Middle East there is a "youth bulge," that is, a disproportionately young population, leading to fewer opportunities for employment, let alone advancement. Some, but not all, analysts believe that youth bulges lead to instability because of a view, especially among males, that they have no opportunities, making them more susceptible to involvement with narcotics or to disaffected behaviors like terrorism.

In several developed nations, there is the opposite problem, a rapidly aging population in which there are low death rates but also low birth rates. This creates a different economic problem, as the working population needed to support the elderly shrinks while the elderly grow. This is of particular concern in Japan. Japan's population is expected to decline from 127 million in 2010 to 90 million in 2055, some 41 percent of whom will be over sixty-five. Russia will experience a similar decline, with roughly similar numbers. Russia's population is shrinking by about 750,000 people annually as deaths exceed births. Alarmingly, for Russian leaders, the Muslim part of the Russian population has very high birth rates. Italy and Germany are also experiencing population declines, albeit less severe, which is why some in Europe have seen the refugee flow from the Middle East as a positive thing. Finally, by 2040, China will begin to feel the effects of the one-child-per-family policy, instituted in 1979 and abandoned in 2015, as its population also shows signs of decline and aging with too few workers to support them. Despite the end of the one-child policy, there are early indications that many couples will continue to adhere to it because of the economic costs of raising more children. China also faces a severe male–female imbalance in many regions, as males are most often the preferred offspring for Chinese couples if they are limited to only one child. This sex imbalance may have destabilizing political results.

Interestingly, demographers argue that programs urging couples to have more children, as seen in China, or incentivizing them via economic benefits, as seen in Russia, tend not to have much effect on the birthrate, while greater gender equality does appear to improve the number of births.

Other than through pandemic or war, the world has never experienced this sort of demographic shift. Although there is little need for sensitive intelligence

collection on this issue, there is a need to begin to explore the possible political and economic ramifications.

Health and the Environment

Health and environmental issues are relatively new to the intelligence agenda. They have sometimes been treated as one issue but are now more often treated separately. The health issue gained increasing prominence because of the AIDS (acquired immune deficiency syndrome) pandemic and smaller outbreaks of deadly diseases, such as the Ebola virus and SARS (severe acute respiratory syndrome) in East Asia and now the Zika virus in the Western hemisphere. The intelligence task with respect to health is largely one of tracking patterns of infection, but a large gap exists between intelligence and policy. Take AIDS as an example. The causes, means of infection, and results of AIDS are well known. Although the disease strikes people worldwide, some areas, notably eastern and central Africa, have extremely high concentrations of AIDS cases. The intelligence community's ability to track rates of infection and mortality has little effect on any useful international policy. Many of the African governments that face the highest rates of AIDS infection have chosen, for a variety of reasons, to ignore or even to deny their health crisis. The same had been true of the government of China, although it now admits the seriousness of the AIDS problem. In the case of Africa, local culture is a major factor in the spread of AIDS: toleration of polygamous relationships and low literacy rates, thus making even minimal efforts at education about prevention more difficult, and minimal use of prophylactics. Nor is it clear what these nations or the international community should be doing in the absence of any cure for the disease. Outsiders' attempts to change the cultural factors that facilitate the spread of AIDS would not only be difficult to make but also would probably be resisted as interference.

A major issue surrounding health-related crises is tracking official foreign government statements against other intelligence to determine both the extent of the health problem and the openness of the government involved. This has been a point of contention with China over SARS. For the United States, two issues are involved. One is the duty to warn, as in terrorism, that is, to alert U.S. citizens and others about potential health risks overseas. The other is an insight into the behavior of another government. Tracking an issue of this sort is a combination of clandestine intelligence (such as SIGINT between foreign officials) and open sources (such as reports by travelers, hospital admissions, larger than normal requests for drugs, and so on).

Again, there is a nexus to terrorism. Outbreaks of certain diseases (such as anthrax, smallpox) must be studied to determine if they are natural occurrences

or terrorist attacks. Even if it can be proven that an attack is **bioterror**, determining the point of origin can prove to be extremely difficult, as was the case with the anthrax mail attacks in the United States in 2001. In such instances, there will also be tremendous political pressure (governmental and public) to provide an answer as quickly as possible.

The environment issue is also somewhat amorphous. The basic goal—preserving a healthier global ecology—stumbles when it comes down to practicalities. As has been the case with international efforts to deal with AIDS, the nations at the center of the issue have different interests and preferences. The international community may believe that it has a vested interest in the preservation of some local ecological habitat, such as a rain forest. However, the nation whose land it is may be more interested in its own economic development than in the stewardship of a world ecological resource.

The basic intelligence tasks are identifying major threats to the environment, identifying states whose policies may be harmful to the environment, and tracking major changes in the environment. Again, a gap separates intelligence from what policy makers are supposed to do with it. Substantial intelligence community involvement in environmental policy dates back only to the late stages of the cold war. A longer-range intelligence concern that has begun to receive more attention is the possible economic and political consequences of global climate change, including droughts, flooding, more violent weather, resulting shifts of population, and the potential for either political or military intervention.

If nations enter into treaties to limit certain emissions, such as greenhouse gases, then the intelligence community may be asked to assist in monitoring compliance with these treaties. This will be more complex and likely more ambiguous than monitoring compliance with arms control treaties.

Much of the intelligence about the health and environment issues can be carried out by means of open sources. Commercial infrared satellites can track environmental changes. The spread of disease also can be tracked overtly. Intelligence on these issues has tended to suffer from the inattention of policy makers and from the fact that overt means of collecting intelligence have been less fully developed than the clandestine means. The fact that much intelligence for health and environmental issues can be drawn from OSINT tends also to make these less compelling issues for intelligence officers, who revert to their professional ethos that their job is to steal secrets. There is debate about the degree to which the intelligence community should devote resources to the climate issue. In 2011, the Defense Science Board—an expert advisory group—recommended that the DNI establish a group to study the economic and political effects of climate change. But a year later, the CIA closed its Center on Climate Change and National Security, which had been created in 2009.

The CIA also had a program called MEDEA (Measurements of Earth Data for Environmental Analysis), which allowed the sharing of sensitive environmental data with scientists. MEDEA began in the 1990s but was curtailed early in the George W. Bush administration (2001–2009). DCIA Leon Panetta revived MEDEA in 2010, but it was closed again in 2015 as a result of opposition in Congress, where some members do not see environmental issues as an area on which the intelligence community should be focusing. On the other hand, the Defense Department issued a "2014 Climate Change Adaptation Roadmap," to begin planning for operations in a changing environment.

Access to water is an important issue in its own right and in relationship to global climate change. The issue is driven, in part, by the growth in global population, which puts increasing demands on all water sources, both surface and aquifers. Building dams, to control flooding and to create reservoirs, has political and environmental consequences. For example, China's population and its continued economic growth is outpacing available water resources and water, unlike oil or minerals, cannot be shipped in sufficient quantities to make any appreciable difference. The growing need for water worldwide has serious policy implications and is an area in which more intelligence analysis may be required over the next few years. In February 2012, the intelligence community released an assessment on global water security, drafted at the request of Secretary of State Hillary Clinton. Looking out ten years, the assessment concluded that water problems would "contribute to instability in states important to the U.S." but that "a water-related state-on-state conflict is unlikely."

In a related area, in September 2015, the intelligence community released an assessment on global food security, an issue mentioned in DNI Clapper's 2015 Worldwide Threat Assessment. Concerns were raised about the adequacy of future food supplies in regions deemed to be important to U.S. national security, including the Middle East, South Asia, and Latin America.

Peacekeeping Operations

Since the end of the cold war, international peacekeeping operations have expanded dramatically. Regional outbursts of violence, most of them within the borders of one country (or former country), have required the imposition of external troops to restore and then maintain peace. Peacekeeping operations are a direct reflection of the failed-states issue discussed in the previous chapter. The external troops have customarily been formed into multinational units. Although many of these nations have experience in allied operations—at least training operations—the participants tend to cross the boundaries of old

alliances. UN-mandated forces in Bosnia, for example, included NATO allies (Britain, France, Italy, Spain, and the United States) and their former Warsaw Pact foes (Russia, Ukraine), along with other nations. A similar array has been formed in Afghanistan. Successful military operations require strong intelligence support; multinational operations require intelligence sharing. But even in the aftermath of the cold war, some U.S. policy makers and intelligence officials are reluctant to share intelligence with former foes, non-allies, and even some allies. Responsible civil and military officials may find themselves torn between the need to keep peacekeeping partners well informed to carry out successful operations and the recognition that sources and methods may be compromised even beyond the limited peacekeeping theater of operations.

The use of peacekeeping or other internationally sanctioned operations for unilateral intelligence purposes became an issue in 1999. A former member of the UN Special Commission (UNSCOM)—which was responsible for monitoring Iraqi destruction of its WMD—alleged that the United States used a UNSCOM inspection team to plant intelligence collection devices. Some saw the U.S. action as a necessary precaution against a hostile state; others believed it violated the basis of the UNSCOM mission.

Support to the Military

Supporting military forces engaged in combat operations, sometimes called support to military operations (SMO), is one of the highest intelligence demands. A key aspect of SMO is the concept of **dominant battlefield awareness (DBA)**. At the National Defense University in June 1995, then-DCI John M. Deutch (1995–1997) defined DBA as the integration of imagery intelligence (IMINT), SIGINT, and HUMINT to give "commanders real-time, or near real-time, all-weather, comprehensive, continuous surveillance and information about the battlespace in which they operate. . . . Dominant battlefield awareness, if achieved, will reduce—never totally eliminate—the 'fog of war,' and provide you, the military commanders, with an unprecedented combat advantage." DBA refers to the totality of information that is available to all commanders at all levels. It is not a single type of report or activity. DBA is closely tied to the **revolution in military affairs (RMA)**. RMA is an ongoing broad doctrinal evolution and debate about the likely nature of future warfare, encompassing technology, strategy, tactics, and the use of intelligence.

DBA reflects at least two trends. The first is the great strides that U.S. intelligence has made in collecting and disseminating intelligence to military commanders in the field. Commanders believe that this superiority allows them to use forces more effectively so as to achieve ends more quickly and with fewer

casualties. The second is the so-called lessons learned from the first Gulf War about the problems in bringing intelligence to the field and getting the right intelligence to the right military user.

Although Deutch cautioned that the "fog of war" (a term coined by nineteenth-century Prussian general and military theorist Karl von Clausewitz for the confusion and uncertainty that are inevitable in any combat) will never be eliminated, many advocates of DBA seem not to have heard him. DBA is often oversold as the ability to bring near-total intelligence to commanders. This hyperbole puts intelligence on the spot for capabilities it does not have. Unrealistically high expectations may lead commanders to place greater reliance on intelligence (which may not be forthcoming) and less on their own instincts when dealing with the fog of war, which is the ultimate skill of a combat commander. (Gen. William T. Sherman observed that Gen. Ulysses S. Grant was the superior commander because he was unconcerned about what the enemy was doing when out of sight.)

DOD official statements on the topic are somewhat confusing. The two key documents are Joint Vision 2010 and Joint Vision 2020. Both emphasize the importance of DBA and the role of intelligence but tend to use intelligence and information technology interchangeably. However, information technology is a means to, but is not the same thing as, intelligence.

Another problem with DBA is that delivering on its promise could require the intelligence community to allocate a large percentage of collection assets to the task, to the detriment of other priorities elsewhere in the world. As with SMO, the question "How much is enough?" is pertinent. Finally, an essential ingredient in successful DBA is getting the right type and amount of information to the right user. An army commander's intelligence needs differ from those of an infantry squad leader or a combat pilot. Some critics are concerned that too much information is pushed down to users who have no need for it, flooding them with irrelevant intelligence simply because the means are available to do so. As a result, their jobs are made more difficult.

The military campaign in Iraq that began in 2003 illustrated both the promise and the problems involved in DBA and RMA. The vastly superior strategic and tactical intelligence of the United States and its allied forces enhanced both the general campaign plan—including the decision to make a dash for Baghdad with a fairly small number of forces—and the ability to locate, identify, and attack in detail regular Iraqi forces. But the war also pointed out that the evolution of U.S. military doctrine continues to put pressure on intelligence for increasing degrees of support. Given the likelihood that the size of U.S. forces (as opposed to their mobility and lethality) will decrease under budget pressure, intelligence will increasingly be seen as one of the factors that allows these relatively small forces to achieve both dominance

and victory. How much support is entailed and what it means for the shape and practice of intelligence are not entirely clear. Also, it remains uncertain how the DNI fits into the relationship between intelligence agencies—especially those such as the National Geospatial-Intelligence Agency (NGA) and NSA, which are national but are also designated in law as combat support agencies—and DOD. The situation is especially murky because the DNI does not control any of the agencies upon which the military relies for intelligence support. The DNI could be bypassed by DOD as it seeks intelligence support from national and defense agencies.

A harsher view of intelligence support to the military in counterinsurgency warfare surfaced in January 2010, when Maj. Gen. Michael T. Flynn co-authored and published a critique. The paper argued that intelligence in the field focused too much on insurgent groups but could not answer basic but essential questions about the overall operating environment. This was a remarkable critique to be published by a serving officer, let alone one who was at the time the deputy chief of staff/intelligence for the international force in Afghanistan. (Lt. Gen. Flynn was the director of the Defense Intelligence Agency [DIA], 2012–2014.)

The strike against bin Laden, on the other hand, showed how intelligence and the military could produce a near flawless outcome in a very well-defined operation of high risk but limited scope.

A major issue for intelligence support to military operations is the nature of the likely engagement. The United States is less likely to be involved in a major nation-state conflict than it is in unconventional conflicts such as counterinsurgency (COIN). As noted above, the intelligence requirements of these types of conflicts are more difficult as the enemy forces are smaller, more covert targets. At the same time, the Obama administration's "rebalance" to the Pacific is more strategic in nature, calling upon a set of intelligence skills that may have atrophied in the last decade.

Conclusion

In the first decade after the end of the cold war (using as a benchmark the breaching of the Berlin Wall in 1989), the U.S. national security agenda remained largely unformed, not in terms of which issues mattered but which of them mattered the most, which would receive the highest priority over time (as opposed to immediate reactions to events), and what the United States would be willing to do to achieve its preferred ends. In the absence of clear definition, the intelligence community found it difficult to perform. Intelligence officials have a broad understanding of policy makers' preferences and immediate interests, but these do not provide the basis for making a coherent set of plans for investments, collection

systems, personnel recruitment, and training. The war on terrorists offered some clarity in that it has given one issue priority over all the others, although not to the same extent as the old Soviet issue. Moreover, the terrorism issue is different from the Soviet issue in many important respects, thus emphasizing the importance of the cold war legacy for the intelligence community, as well as the need to transcend this legacy. As noted, after over a decade, President Obama signaled a change in the relative emphasis on the terrorism issue.

Many issues in the new U.S. intelligence agenda share an important hallmark: the gap between the intelligence community's ability to provide intelligence and the policy makers' ability to craft policies to address the issues and to use the intelligence. This gap may even be seen in the war against terrorists. If the disparity persists, the intelligence community and its policy clients may become disaffected. Clients want to be more than just informed; they want to act (that is, to receive opportunity analysis). And intelligence is not meant to be collected and then filed away. It is intended to assist people in making decisions or taking action. This is not to suggest that the intelligence community will suddenly disappear. But it may come to be seen as less central and necessary—a provider of information that is interesting but not as useful as it has been in the past because of the changed nature of the issues and the rapidity with which overall policy emphasis shifts—shifts that are difficult for intelligence to match, especially at the analytical level.

Key Terms

attribution

backdoor encryption

battle damage assessment (BDA)

bioterror

chatter

computer network attack (CNA)

computer network exploitation (CNE)

cyber operational preparation of the environment (cyber OPE)

dominant battlefield awareness (DBA)

ECHELON

financial intelligence (FININT)

foreign economic espionage

industrial espionage

information operations

Joint Terrorism Task Forces (JTTFs)

link analysis

monitoring

revolution in military affairs (RMA)

verification

Further Readings

Writings on the post–cold war intelligence agenda remain somewhat scattered across issue areas, reflecting the nature of the debate itself.

General

Colby, William. "The Changing Role of Intelligence." *World Outlook* 13 (summer 1991): 77–90.

Goodman, Allan E. "The Future of U.S. Intelligence." *Intelligence and National Security* 11 (October 1996): 645–656.

Goodman, Allan E., and Bruce D. Berkowitz. *The Need to Know: Report of the Twentieth Century Fund Task Force on Covert Action and American Democracy*. New York: Twentieth Century Fund, 1992.

Goodman, Allan E., Gregory F. Treverton, and Philip Zelikow. *In From the Cold: Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence.* New York: Twentieth Century Fund, 1996.

Johnson, Loch K. *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*. New York: New York University Press, 2000.

Johnson, Loch K., and Kevin J. Scheid. "Spending for Spies: Intelligence Budgeting in the Aftermath of the Cold War." *Public Budgeting and Finance* 17 (winter 1997): 7–27.

U.S. National Intelligence Council. *Global Trends 2030: Alternative Worlds.* Washington, D.C.: National Intelligence Council, 2012.

Cyberspace

Aldrich, Richard W. *The International Legal Implications of Information Warfare.* Colorado Springs: U.S. Air Force Institute for National Security Studies, 1996.

Chang, Amy. *Warring State: China's Cybersecurity Strategy*. Washington, D.C.: Center for a New American Strategy, 2014. (Available at http://www.cnas.org/chinas-cybersecurity-strategy#.VkPNbL8nqNI.)

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986–2012.* Washington, D.C.: The Atlantic Council and the Cyber Conflict Studies Association, 2013.

———. "A Short History of Cyber Conflict in the United States." Cyber Conflict Studies Association. Washington, D.C., September 13, 2010.

Intelligence and National Security Alliance. *Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats.* Arlington, VA, September 2015. (Available at http://www.insaonline.org/i/d/a/b/CyberIntel_PrepTalent.aspx.)

———. *Operational Cyber Intelligence*. Arlington, VA, October 2014. (Available at http://www.insaonline.org/i/d/a/b/OCI_whitepaper.aspx.)

———. *Strategic Cyber Intelligence.* Arlington, VA, March 2014. (Available at http://www.insaonline.org/i/d/a/b/StrategicCyberWP.aspx.)

Kerr, Paul K., John Rollins, and Catherine A. Theohary. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* CRS Report R41524. Washington, D.C.: Congressional Research Service, December 9, 2010.

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.* 2013. (Available at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.)

Schmitt, Michael N., general ed. *Tallinn Manual on International Law Applicable to Cyber Warfare*. Cambridge, U.K.: Cambridge University Press, 2013. (Also available at http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf.)

Stokes, Mark A., and L. C. Russell Hsiao. *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests*. Arlington, VA: Project 2049 Institute, October 29, 2012. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-079.pdf

U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, D.C., July 2011. (Available at www.defense.gov/news/d20110714cyber.pdf.)

U.S. Director of National Intelligence. Statement for the Record. Worldwide Cyber Threats. House Permanent Select Committee on Intelligence. Washington, D.C., September 10, 2015. (Available at http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf.)

Dominant Battlefield Awareness

Nolte, William. "Keeping Pace With the Revolution in Military Affairs." *Studies in Intelligence* 48 (2004): 1–10.

Economics

Fort, Randall M. *Economic Espionage: Problems and Prospects*. Washington, D.C.: Consortium for the Study of Intelligence, 1993.

Hulnick, Arthur S. "The Uneasy Relationship Between Intelligence and Private Industry." *International Journal of Intelligence and Counterintelligence* 9 (spring 1996): 17–31.

Lowenthal, Mark M. "Keep James Bond out of GM." *International Economy* (July–August 1992): 52–54.

U.S. National Counterintelligence Executive. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2008*. Washington, D.C., July 23, 2009.

Woolsey, R. James. "Why We Spy on Our Allies." *Wall Street Journal*, March 17, 2000, A18.

Zarate, Juan C. *Treasury's War: The Unleashing of a New Era of Financial Warfare*. New York: PublicAffairs Books, 2013.

Zelikow, Philip. "American Economic Intelligence: Past Practice and Future Principles." *Intelligence and National Security* 12 (January 1997): 164–177.

Health and Environment

CNA Corporation. "National Security and the Threat of Climate Change." Alexandria, VA, 2007.

U.S. Department of Defense. *2014 Climate Change Adaptation Roadmap*. Washington, D.C., June 2014. (Available at http://www.acq.osd.mil/ie/download/CCARprint_wForeword_c.pdf.)

U.S. Office of the Director of National Intelligence. *Global Food Security*. Intelligence Community Assessment 2015-04. Washington, D.C., September 22, 2015. (Available at http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Global_Food_Security_ICA.pdf.)

———. *Global Water Security*. Intelligence Community Assessment 2012-08. Washington, D.C., February 2, 2012. (Available at http://www.dni.gov/files/documents/Newsroom/Press%20Releases/ICA_Global%20Water%20Security.pdf.)

Law Enforcement

Hulnick, Arthur S. "Intelligence and Law Enforcement." *International Journal of Intelligence and Counterintelligence* 10 (fall 1997): 269–286.

Snider, L. Britt, with Elizabeth Rindskopf and John Coleman. *Relating Intelligence and Law Enforcement: Problems and Prospects.* Washington, D.C.: Consortium for the Study of Intelligence, 1994.

Narcotics

Best, Richard A., Jr., and Mark M. Lowenthal. *The U.S. Intelligence Community and the Counternarcotics Effort*. Washington, D.C.: Congressional Research Service, 1992.

Peacekeeping

Best, Richard A., Jr. *Peacekeeping: Intelligence Requirements*. CRS Report 92–74F. Washington, D.C.: Congressional Research Service, 1994.

Johnston, Paul. "No Cloak and Dagger Required: Intelligence Support to UN Peacekeeping." *Intelligence and National Security* 12 (October 1997): 102–112.

Pickert, Perry L. *Intelligence for Multilateral Decision and Action.* Ed. Russell G. Swenson. Washington, D.C.: Joint Military Intelligence College, 1997.

Proliferation

Hansen, Keith A. *Intelligence and Nuclear Proliferation: Lesson Learned*. Paris, France: Institut Francais des Relations Internationales (IFRI), Summer 2011. (Available at http://www.ifri.org/downloads/pp38hansen.pdf.)

Ikle, Fred Charles. "After Detection—What?" *Foreign Affairs* 39 (January 1961): 208–220.

International Atomic Energy Agency. *Final Assessment on Past and Present Outstanding Issues Regarding Iran's Nuclear Programme*. GOV/2015/68. December 2, 2015. (Available at http://isis-online.org/uploads/isis-reports/documents/IAEA_PMD_Assessment_2Dec2015.pdf.)

Kerr, Paul K. *Iran's Nuclear Program: Tehran's Compliance With International Obligations*. Congressional Research Service Report R40094. Washington, D.C., September 18, 2012.

Nikitin, Mary Beth. *North Korea's Nuclear Weapons: Technical Issues.* Congressional Research Service Report RL34256. Washington, D.C., April 3, 2013.

U.S. Department of Defense, Defense Science Board. *Task Force Report: Assessment of Nuclear Monitoring and Verification Technologies*. Washington. D.C., January 2014. (Available at http://www.acq.osd.mil/dsb/reports/NuclearMonitoringAndVerificationTechnologies.pdf.)

U.S. National Intelligence Council. *National Intelligence Estimate: Iran: Nuclear Intentions and Capabilities.* Washington, D.C.: NIC, December 2007. (Available at http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20071203_release.pdf.)

Support to the Military

Deutch, John M. Speech at National Defense University, Washington, D.C., June 14, 1995. (Available at http://www.defense.gov/speeches/speech.aspx?speechid=922.)

Flynn, Michael T., Michael J. Pottinger, and Paul D. Batchelor. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.* Washington, D.C.: Center for a New American Security, 2010. (Available at www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.)

Terrorism

Best, Richard A., Jr. "The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns." CRS Report R41022. Washington, D.C.: Congressional Research Service, January 15, 2010.

Byman, Daniel. "The Intelligence War on Terrorism." *Intelligence and National Security* 29 (December 2014): 837–863.

Cilluffo, Frank J., Ronald A. Marks, and George C. Salmoiraghi. "The Use and Limits of U.S. Intelligence." *Washington Quarterly* 25 (winter 2002): 61–74.

Grimmett, Richard F. "Terrorism: Key Recommendations of the 9/11 Commission and Recent Major Commissions and Inquiries." Washington, D.C.: Congressional Research Service, CRS Report RL32519, August 11, 2004.

Jameson, W. George. "Intelligence and the Law: Introduction to the Legal and Policy Framework Governing Intelligence Community Counterterrorism Efforts." In *The Law of Counterterrorism.* Ed. Lynne K. Zusman. Washington, D.C.: American Bar Association, September 2011.

Marks, Ronald A. *Spying in America in the Post 9/11 World.* Santa Barbara, CA: Praeger, 2010.

Masse, Todd, and John Rollins. "A Summary of Fusion Centers: Core Issues and Options for Congress." Washington, D.C.: Congressional Research Service, CRS Report RL 34177, September 19, 2007.

Randol, Mark A. "Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches." CRS Report RL33616. Washington, D.C.: Congressional Research Service, January 14, 2009.

———. "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress." CRS Report R40602. Washington, D.C.: Congressional Research Service, March 19, 2010.

Steiner, James E. "Needed: State-level, Integrated Intelligence Enterprises." *Studies in Intelligence* 53 (September 2009): 1–10.

———. *Homeland Security Intelligence.* Thousand Oaks, CA: CQ Press, 2015.

Treverton, Gregory F. *Intelligence in an Age of Terror.* New York: Cambridge University Press, 2009.

Treverton, Gregory F., et al. *State and Local Intelligence in the War on Terrorism*. Washington, D.C.: Rand Corporation, 2005.

U.S. Department of Homeland Security, Office of the Inspector General. *Major Management and Performance Challenges Facing the Department of Homeland Security*. Report OIG-16-07. Washington, D.C, November 13, 2015. (Available at https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-07-Nov15.pdf.)