Intelligence and National Defense

David R. Shedd

Every successful military plan and operation relies on intelligence. Whether it is a simple field report from a scout about an enemy position or the methodical development of the mosaic of intelligence gathered from myriad sources over years that resulted in the successful raid of Osama bin Laden's Abbottabad compound, intelligence plays a vital role in our national defense. The diversity and rapidly changing nature of the threats we face as a nation underscore the need for sound intelligence in the hands of those who are charged with making decisions about our security.

This is not a new phenomenon. Intelligence has played a role in national defense since well before the United States was founded. Timely intelligence, however, is the beginning of the surprising and often difficult decisions that are made in war, where force is often critical.[1] Since earliest recorded history, accounts of people using espionage to try to understand the intentions of the adversary abound.

- Early Egyptian pharaohs employed agents of espionage to ferret out disloyal subjects and to locate tribes that could be conquered and enslaved. From 1,000 B.C. onwards, Egyptian espionage operations focused on foreign intelligence about the political and military strength of rivals Greece and Rome.[2]

- The legendary story of the Trojan Horse, a wooden structure given to the city of Troy as a gift but which contained several hundred Greek soldiers seeking safe entrance into the heavily fortified rival city, became the symbol of Grecian intelligence prowess.[3]

- The Romans used intelligence to conquer the people of the Italian Peninsula. They used scouts on regular assignments against the Samnites and Gauls, and because of advance intelligence, they could often catch their enemies by launching surprise attacks and rout their camps.[4]

During the 20th century's two world wars, intelligence played a vital role in allowing the United States military and its allies to prevail. Examples that immediately come to mind include Operation Mincemeat, the World War II British-led operation to deceive the Nazis into thinking that Allied forces were planning to attack southern Europe by way of Greece or Sardinia rather than Sicily, as the Nazis had assumed.[5] Another example of the critical role of intelligence was the Allied forces' successful exploitation of the Enigma machine used by the Nazis to encrypt their military transmissions during the war.[6] There were thousands of other intelligence successes, including intelligence-led operations behind enemy lines by the Central Intelligence Agency's predecessor, the Office of Strategic Services (OSS).

Of course, as one would expect, there also have been intelligence failures with profound ramifications. One notable and recent such failure resulted in a faulty case for the invasion of Iraq in March 2003. Notwithstanding many grievances by the U.S. and the international community with the Iraqi despotic regime of Saddam Hussein, the case for war was based fundamentally on what turned out to be erroneous intelligence assessments concerning the threat posed by Iraq's weapons of mass destruction (WMD). Post-invasion, it was determined that no meaningful WMD program was in place in Iraq at the time of invasion.[7] The WMD Commission highlighted this failure in their transmittal letter to President George W. Bush in the spring of 2005:

> We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. This was a major intelligence failure. Its principal causes were the Intelligence Community's inability to collect good information about Iraq's WMD programs, serious errors in analyzing what information it could gather, and a failure to make clear just how much of its analysis was based on assumptions, rather than good evidence. On a matter of this importance, we simply cannot afford failures of this magnitude.[8]

Each of the topical essays in The Heritage Foundation's 2015 *Index of U.S. Military Strength,* which range from broad subjects like "What Is National Security?" to "The Importance of Special Operations Forces Today and Going Forward," works from the premise that a robust U.S. intelligence capability is critical to our nation's defense. But what is intelligence, what role does it play in our national defense, and why is it important?

The classic definition of intelligence captured by Mark Lowenthal encompasses information, process, organization, and products. This essay will largely focus on information as intelligence.[9] What are the component parts of the intelligence enterprise, and what roles does each component play in providing for the common defense? What is the current status of the Defense Intelligence Enterprise, its current demands, and its ability to handle a growing demand for both tactical and strategic intelligence?

The purpose of this essay is to present in one place an overview of intelligence as it relates to national defense, and in particular to military affairs, and to answer several questions including:

- How is intelligence acquired, processed, integrated and disseminated?
- What current problems and limitations exist in the intelligence enterprise, and what solutions or adjustments are necessary?
- How has the broad spectrum of threats facing our country affected intelligence collection efforts?
- What more can or should be done?

We will explain how to think about intelligence, factors that affect its current status, and how the Intelligence Community (IC) is changing with the world of military planning and operations so that senior policymakers, the Congress, and Combatant Commanders can take better advantage of the special role of intelligence in our nation's defense.

What Is Intelligence, and Why Is It So Critical?

Intelligence is "the ability to learn or understand or to deal with new or trying situations."[10] In the context of military operations, it is "information concerning an enemy or possible enemy or an area."[11]

A 2012 Joint Chiefs of Staff publication states that "commanders use intelligence to anticipate the battle, visualize and understand the full spectrum of the operational environment, and influence the outcome of operations."[12] Intelligence "enables commanders at all levels to focus their combat power and to provide full-dimensional force protection across the range of military operations."[13]

Intelligence potentially gives our men and women in uniform—our warfighters—information dominance and operational advantage over our adversaries. And the list of potential adversaries is growing. Concurrently, our comparative military advantage is starting to wane,[14] but even as American military power declines, the demands made on the military are increasing.[15] For example, the former Commandant of the Marine Corps, General James Amos, recently said that in view of projected U.S. defense budget cuts on the one hand and the explosion of international crises and threats to U.S. interests on the other, he expected his service and the Joint Force, at a minimum, to be asked "to do the same with less."[16] The same cautionary note pertains to the Intelligence Community: As demand increases for a decreasing force, the remaining resources will be asked to do more even in a declining resource environment.

That might be acceptable for a country other than the United States, but as Daniel Gouré wrote in the 2015 *Index*, United States power and presence are the foundation on which the present international order is built.[17] Put another way, the U.S. military is the linchpin of the global security system.[18]

Today, that system is under increasing pressure from a variety of state and non-state actors. We are facing threats from old and new adversaries with tried and proven techniques as well as new techniques such as the potential and growing ability to attack information technology systems that are a critical part of virtually every economic and security sector in the United States.

Intelligence collection is more difficult in today's world because access is increasingly reduced to the secrets we must know. Denial and deception by our adversaries are sophisticated. Intelligence revelations by Edward Snowden and other leaked information have undercut our ability to obtain secrets by revealing intelligence methods and have undermined trust among America's allies. Russia's Vladimir Putin relies on traditional Russian military power to intimidate a neighbor such as Ukraine while using cyber to promote disinformation. China is modernizing its weapons systems and military forces at a startling pace. The non-state actors from Islamic extremists to drug cartels and organized crime organizations have at their disposal a wide array of technology that facilitates communication.

All levels of decision makers from the President to the warfighter should expect to receive accurate and timely intelligence to inform their plans and decisions notwithstanding the challenges the Intelligence Community faces from trying to acquire secrets about these countries and/or organizations. Intelligence customers should expect nothing but the best output from intelligence professionals.

In the National Military Strategy published in June 2015, the Chairman of the Joint Chiefs of Staff wrote: "We now face multiple, simultaneous security challenges from traditional state actors and trans-regional networks of sub-state groups—all taking advantage of rapid technological change. Future conflicts will come more rapidly, last longer, and take place on a much more technically challenging battlefield."[19] The same document mentions with concern such nations as Russia, China, and North Korea and such non-state actors as al-Qaeda and the Islamic State.

The most current National Intelligence Strategy, published in 2014, highlights that "the United States faces a complex and evolving security environment with extremely dangerous, pervasive, and elusive threats."[20] It goes on to describe the global environment wherein "power is becoming more diffuse. New alignments and informal networks—outside of traditional power blocs and national governments—will increasingly have significant impact in economic, social, and political affairs."[21] The grassroots voices from "[p]rivate, public, governmental, commercial, and ideological players" will grow in influence as a result of social media outlets,[22] and "[t]he projected rise of a global middle class and its growing expectations will fuel economic and political change."[23] Resolving such complex security challenges will require U.S. intelligence attention to a broader array of actors.

The elements of the U.S. national intelligence organizations are focused on key nation-states that continue to pursue agendas that challenge U.S. interests around the globe. China's strategic intentions with regard to its ambitious military modernization remain opaque and therefore present a concern. Russia is likely to continue to reassert power and influence in ways that undermine U.S. interests. "North Korea's pursuit of nuclear and ballistic missile capabilities and its international intransigence" also command attention.[24] The Intelligence Strategy further highlights that:

> Iran's nuclear efforts remain a key concern, in addition to its missile programs, support for terrorism, regime dynamics, and other developing military capabilities. The potential for greater instability in the Middle East and North Africa will require continued [U.S. intelligence] vigilance.... Violent extremist groups and transnational criminal networks threaten U.S. security and challenge the U.S. both in the homeland and abroad. Al-Qa'ida, its affiliates, and adherents, continue to plot against U.S. and Western interests, and seek to use weapons of mass destruction if possible.[25]

Intelligence remains essential to understanding and responding to these diverse threats that have a direct bearing on our national defense.

The United States Intelligence Community

"The U.S. Intelligence Community is a coalition of 17 agencies and organizations" that comprise the American intelligence apparatus.[26] The IC is led by the Director of National Intelligence (DNI), a position created in 2004 under the Intelligence Reform and Terrorism Prevention Act (IRTPA),[27] and operates in a unified manner to ensure that intergovernmental intelligence activities are undertaken in a coordinated and tightly integrated manner for the purpose of gathering and analyzing the intelligence necessary to conduct foreign relations and to protect the national security of the United States.[28]

Representations of many of these IC elements collect and produce analysis outside of Washington at Combatant Commands, the Service Centers, and U.S. embassies. Ensuring that the Washington-based intelligence capabilities are well integrated in the field is critical so that all elements operate as an enterprise irrespective of location.

One way to think of the Intelligence Community is to single out the Office of the Director of National Intelligence (ODNI) as a stand-alone element setting the strategic direction for the IC but not having an operational role. The six program management IC organizations are listed and described below under a separate heading. With the exception of the Federal Bureau of Investigation, which reports to the Attorney General, and the CIA, which reports to the DNI, the other four program managers are agencies fully dedicated to the intelligence mission and are under the authority, direction, and control of the Secretary of Defense. The IC has five departmental intelligence elements with boutique intelligence missions, also described below. Finally, the five military services, including the Coast Guard, have intelligence offices that support their respective services.

Office of the Director of National Intelligence

The Office of the Director of National Intelligence serves as the head of the 17 agencies that comprise the Intelligence Community. The purpose of the DNI is to "lead intelligence integration" and "forge an IC that delivers the most insightful intelligence possible."[29] The 9/11 terrorist attacks on the United States prompted the President and Congress to reform the IC, and in 2004, the position of DNI was created as part of the IRTPA. The DNI is subject to the authority of the President of the United States and serves as a chief adviser on intelligence matters related to national security.[30]

Program Management Agencies

Central Intelligence Agency. In 1947, President Harry Truman signed the National Security Act, which led to the creation of the Central Intelligence Agency (CIA) on July 26, 1947. The attack on Pearl Harbor and subsequent urgencies of World War II prompted the United States to create a group to conduct foreign intelligence operations. Over the years, the CIA has evolved and expanded its role as an intelligence organization with operatives in countries around the globe.

The CIA remains the primary external intelligence agency operating outside of the United States. It is organized into five components: the Directorate of Operations, the Directorate of Analysis, the Directorate of Science and Technology, the Directorate of Support, and the recently created Directorate of Digital Innovation. Using both human and signals intelligence sources, the CIA "collects, analyzes, and disseminates intelligence gathered on foreign nations."[31] According to its mission statement, the Agency's "information, insights, and actions consistently provide tactical and strategic advantage for the United States."[32]

From 1947, when the National Security Act was enacted, until passage of the IRTPA in December 2004, the CIA was led by the Director of Central Intelligence (DCI).[33] In April 2005, when the first Director of National Intelligence took office, many of the IRTPA reforms went into effect. These reforms turned the Director of Central Intelligence into the Director of the Central Intelligence Agency to emphasize that the D/CIA is responsible for running the CIA while the DNI directs the entire Intelligence Community.[34] The D/CIA reports to the DNI.[35]

Defense Intelligence Agency. Operating under the jurisdiction of the Department of Defense (DOD) but also as a member of the Intelligence Community under the purview of the DNI, the Defense Intelligence Agency (DIA) is the major producer of information related to foreign military intelligence. As a combat support agency within the DOD, the DIA collects and analyzes intelligence on foreign militaries, conducts surveillance and reconnaissance operations, and provides crucial information to warfighters, defense policymakers, and force planners.[36]

The DIA is organized into four directorates: the Directorate of Operations, Directorate for Analysis, Directorate for Science and Technology, and Directorate for Mission Services. There also are five centers. Four cover regions around the globe: the Americas Center, Asia/Pacific Center, Europe/Eurasia Center, and Middle East/Africa Center. The fifth, the Defense Combating Terrorism Center, is focused on transnational terrorism threats and support for counterterrorism operations by the warfighter.

National Geospatial-Intelligence Agency. Initially formed in 1972 as the Defense Mapping Agency (DMA) and later renamed the National Imagery and Mapping Agency (NIMA), the National Geospatial-Intelligence Agency (NGA) serves a dual role as DOD combat support and U.S. Intelligence Community agency, as do all of the department's intelligence elements. Cartographers, analysts, and other NGA personnel gather imagery and furnish geospatial analytical products applicable to national security, military operations, and humanitarian aid efforts.[37]

National Reconnaissance Office. The National Reconnaissance Office (NRO) is responsible for the development and operation of U.S. reconnaissance satellites. As a combat support agency, the NRO provides these reconnaissance capabilities to other agencies, such as the CIA or DOD. The NRO's products are of great importance to national security because they can be used to "warn of potential trouble spots around the world, help plan military operations, and monitor the environment."[38]

National Security Agency/Central Security Service. The National Security Agency (NSA) is at the forefront of communications and information technology, serving as a critical enabler of sensitive intelligence collection. As a combat support agency:

> The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.[39]

Aside from lending support to other Intelligence Community agencies, the NSA also aids military customers, national policymakers, counterterrorism and counterintelligence communities, and key international allies.[40]

Federal Bureau of Investigation. Intelligence has been an important function of the FBI, especially over the past few decades in supporting law enforcement activities. The FBI's updated intelligence role is now codified in Executive Order 12333 as amended by Executive Order 13470 on July 30, 2008. Under the supervision of the Attorney General, the bureau's role is to:

1. Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director [of National Intelligence];

2. Conduct counterintelligence activities; and

3. Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations....[41]

These changes in the FBI's intelligence role emerged from the 9/11 Commission report and the IRTPA of 2004, which sought to close the gap between foreign and domestic intelligence collection and intelligence sharing. The FBI has organized itself since then to meet the intelligence-collection and intelligence-analysis mission. In 2014, FBI Director James Comey created the FBI's Intelligence Branch to "lead the integration of intelligence and operations across the organization."[42] The Intelligence Branch is now responsible for "all intelligence strategy, resources, policies, and functions."[43]

Departmental Intelligence Elements

Department of Energy. The primary focus of the Department of Energy's Office of Intelligence and Counterintelligence is to protect, enable, and represent the vast scientific brain trust resident in DOE laboratories and plants.[44] While the DOE's Office of Intelligence and Counterintelligence does not have the authority to conduct the collection of foreign intelligence, it often assists with analysis of the information gathered by other intelligence agencies. The Department of Energy and its Office of Intelligence and Counterintelligence specialize in the following areas of intelligence concern: nuclear weapons, nuclear proliferation, nuclear energy, and energy security.

Department of Homeland Security. The Department of Homeland Security (DHS) was created in 2002 in response to the 9/11 terrorist attacks. Within the DHS, the Office of Intelligence and Analysis (I&A) collects and analyzes intelligence and information in an effort to identify and assess current and future threats to the U.S. Through the National Network of Fusion Centers, the DHS disseminates I&A intelligence and information to federal, state, and local authorities.[45] I&A focuses on four major areas: promoting understanding of threats through intelligence analysis, collecting open-source information and intelligence pertinent to homeland security, sharing information necessary for action, and managing intelligence for the homeland security enterprise.[46]

Department of State. The Bureau of Intelligence and Research (INR) serves as the Department of State's intelligence arm, collecting relevant intelligence and information and providing the Secretary of State with analysis of significant global events. Through all-source intelligence, diplomatic reporting, public opinion polling, and interaction with U.S. and foreign scholars, the INR seeks to inform the State Department of global events or trends that affect U.S. foreign policy.[47] In addition to serving as the Secretary of State's primary intelligence adviser, the INR also supports other policymakers, ambassadors, and embassy staff.[48]

Department of the Treasury. The Office of Terrorism and Financial Intelligence (TFI) is the agency within the Department of the Treasury that is responsible for intelligence operations. The TFI develops and implements U.S. government strategies aimed at "safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction proliferators, money launderers, drug kingpins, and other national security threats."[49] The Office of Intelligence and Analysis (OIA), created under the TFI in 2004, "advances national security and protects financial integrity by informing Treasury decisions with timely, relevant, and accurate intelligence and analysis."[50]

Drug Enforcement Administration. Under the jurisdiction of the Department of Justice, the Drug Enforcement Administration (DEA) is tasked with enforcing current federal laws and regulations on controlled substances. While the DEA has gathered intelligence since the 1970s, the Office of National Security Intelligence (ONSI) was created in 2006 and works with other members of the U.S. Intelligence Community "to enhance the U.S.'s efforts to reduce the supply of drugs, protect national security, and combat global terrorism."[51]

Military Service Components

Air Force Intelligence. "The U.S. Air Force Intelligence, Surveillance, and Reconnaissance (USAF ISR) Enterprise is America's primary source of finished intelligence derived from airborne, space, and cyberspace sensors."[52] Originally founded in 1948 as the Air Intelligence Agency, the USAF ISR collects and analyzes data on foreign countries and forces around the world, expediting critical information to troops on the ground. Examples of USAF ISR intelligence include (but are not limited to) electronic surveillance, photographic surveillance, and weather and mapping data.

Army Intelligence. U.S. Army Intelligence, or G-2, is organized into five major military intelligence (MI) disciplines in the Army: Imagery Intelligence, Signals Intelligence, Human Intelligence, Measurement and Signature Intelligence, and Counterintelligence and Security Countermeasures. While Army intelligence dates back to the earliest days of the U.S. Army, the chief uniting force, the U.S. Army's Intelligence and Security Command (INSCOM), was formally established in 1977. The purpose of U.S. Army Intelligence is to enable effective Army planning and operations. Its role includes "policy formulation, planning, programming, budgeting, management, staff supervision, evaluation, and providing oversight for intelligence activities for the Department of the Army."[53]

Coast Guard Intelligence. Coast Guard Intelligence (CGI) is the military intelligence branch of the U.S. Coast Guard. In addition to this role, CGI also serves an investigative function. Created in 1915, CGI has been altered continuously so that it can best fit the needs of the Coast Guard. Today, under the Department of Homeland Security, CGI seeks to produce "information on maritime and port security, search and rescue, and counter-narcotics."[54]

Marine Corps Intelligence. The Marine Corps' intelligence component, the Marine Corps Intelligence Activity (MCIA), exists to supply battlefield commanders with the necessary tactical and operational intelligence to carry out their respective functions. The intelligence department of the Marine Corps "has service staff responsibility for geospatial intelligence, advanced geospatial intelligence, signals intelligence, human intelligence, [and] counterintelligence, and ensures there is a single synchronized strategy for the development of the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise."[55]

Navy Intelligence. The U.S. Navy's intelligence element has been in place since 1882. The Office of Naval Intelligence (ONI) is the oldest component of the U.S. Intelligence Community and is headquartered at the National Maritime Intelligence Center in Suitland, Maryland. According to the U.S. Navy, "ONI produces relevant maritime intelligence and moves that intelligence rapidly to key strategic, operational, and tactical decision makers."[56]

Intelligence and the Warfighter

The IC's 17 elements operate essentially as a loosely federated system under DNI, departmental, and (in the case of the CIA) presidential authorities. Until enactment of the 2004 IRTPA, changes in the IC were evolutionary. The changes brought about by the IRTPA, which included establishing the Office of the Director of National Intelligence and limiting the Director of Central Intelligence to running the CIA, were dramatic. The advent of the FBI as a full IC member among the federation of elements also introduced a major change.

The changes have been less pronounced for the combat support agencies—the National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, and National Reconnaissance Office—and for the uniformed services' intelligence elements within the Department of Defense (DOD). When the IRTPA was being debated, then-Secretary of Defense Donald Rumsfeld placed significant limits on the level of reform of all DOD intelligence elements that he would find acceptable, which Congress and the President codified into law to ensure unified command over, and intelligence support for, the Department of Defense.[57]

The wars in Iraq and Afghanistan have provided ample opportunity for the Intelligence Community and especially the combat support agencies to provide intelligence to the warfighter. That intelligence today often combines human intelligence (HUMINT), signals intelligence (SIGINT) and geospatial imagery (GEOINT) to enable our soldiers, airmen, sailors, and marines to achieve success against the enemy. That intelligence, thanks to modern technology, may reach the warfighter simultaneously as it reaches the commander in chief.

The operation that resulted in the death of al-Qaeda's leader in Iraq, Abu Musab al-Zarqawi, in early June 2006 illustrates the intelligence support on the ground that has enabled battlefield successes. U.S. military spokesman Major General William Caldwell stated, "We had absolutely no doubt whatsoever that Zarqawi was in the house," adding that the success required "a painstaking intelligence effort" in which "we were able to start tracking [al-Zarqawi's associate], monitor his movements and establish when he was doing his linkup with al-Zarqawi." According to Caldwell, "It truly was a very long, painstaking, deliberate exploitation of intelligence, information gathering, human sources, electronics, signal intelligence that was done over…many, many weeks."[58]

Intelligence Acquisition, Processing, Integration, and Dissemination

The intelligence process that results in a product is often referred to as the "intelligence cycle." The intelligence cycle is a six-step process that covers everything from the acquisition of intelligence to its dissemination to end users. (See Figure 2, "The Intelligence Cycle.") The cycle is fed by information collected from many sources: clandestine and overt human sources, signals and cyber-based intelligence, imagery, open sources, and technical means such as telemetry.

Acquisition of the information is based on a system of requirements generated primarily by the users of intelligence. The information that results, often referred to as raw or unevaluated information, is then used to prepare a finished analytical product for use by policymakers, our warfighters, and other consumers such as Congress. The best analytical products prepared by the intelligence professional will draw from all available sources of information.

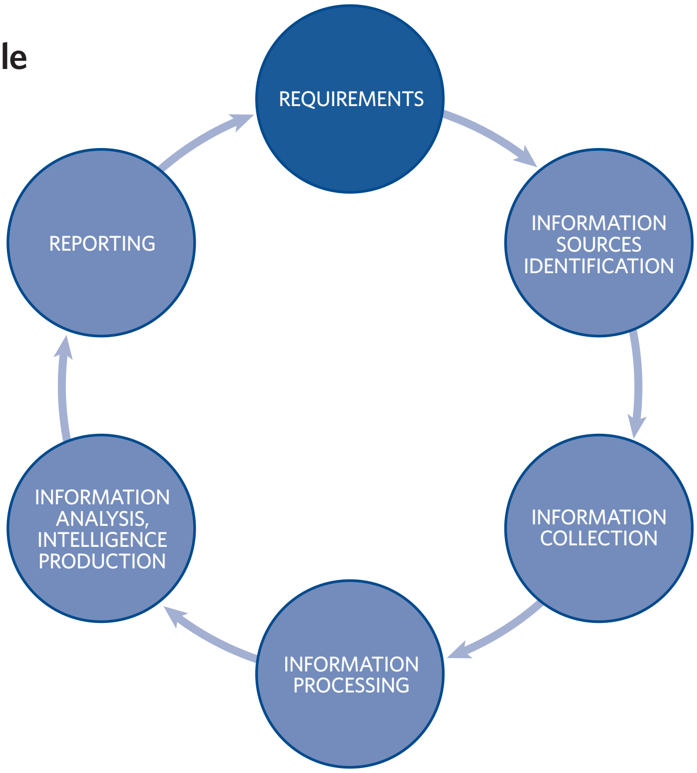
To provide the best support for its consumers, the IC is working to ensure that the process is strengthened through tighter integration. The means for achieving enhanced integration are critical in attaining increased efficiencies in leveraging the various intelligence disciplines to meet common objectives for the users of intelligence.

The Intelligence Community's 17 elements serve as the backbone of the American intelligence system. Each element inside and outside of the defense-based intelligence organizations contributes specific collection and analytical expertise that serves to inform the security community's understanding of the threats and adversaries or to meet the unique requirements associated with the military services. There has been a significant change in the trends for the intelligence mission over the past 15 years. The attacks on the U.S. homeland on September 11, 2001, created an important shift in how intelligence resources are allocated today, both for collection and for analysis.

As noted thematically by DNI James Clapper in the Intelligence Community's 2015 Worldwide

FIGURE 2

The Intelligence Cycle


REQUIREMENTS
INFORMATION SOURCES IDENTIFICATION
INFORMATION COLLECTION
INFORMATION PROCESSING
INFORMATION ANALYSIS, INTELLIGENCE PRODUCTION
REPORTING

Source: Kudelski Security, "The Intelligence Cycle," https://www.kudelskisecurity.com/services/advanced-threat-intelligence.html#working-together (accessed August 21, 2015).

heritage.org

Threat Assessment, cyber threats are on the rise, as are conflicts around the globe that are marked by diversity, as seen through the resurgence of Russia's destabilizing efforts, Iran's use of proxies to foment instability in the Middle East, and North Korea's ever-present threat to use nuclear weapons. At the same time, Islamic extremism is on the rise and far from contained to one geographic area.[59]

To achieve a better understanding of the hidden plans and intentions of these and other adversaries, it is imperative that all of the nation's intelligence capabilities and, by extension, investments are made in a manner that focuses on U.S. defense capabilities and decision making and ultimately ensures that the U.S. retains superior military capabilities compared to other countries and is able to prevail in any conflict.

Problems, Limitations, and Solutions

The threats to U.S. national security are increasingly diverse and complex. Traditionally, when facing a crisis, American decision makers would see the crisis spike but then soon settle down. Today, we see a different and disturbing trend concerning "hot spots." The national security challenges appear to be chronic and at times acute, with no foreseeable end to a crisis-riddled world.

Nonetheless, the policymaker and the warfighter will continue to rely on accurate and timely intelligence that can guide their decisions, from responding to threat warnings to implementing a plan of action in response to threats as they materialize. IC customers, including the uniformed operators, have come to expect information that moves rapidly through the intelligence cycle. They deserve nothing less despite a number of significant challenges and limitations that confront U.S. intelligence.

Specifically, American intelligence faces several significant problems and limitations in building and then maintaining intelligence capabilities and capacity in the 21st century. Among these critical problems and limitations are:

- Rapidly changing technology, such as multiple options for communication information, that enables adversaries to challenge and potentially defeat U.S. collection capabilities in the air and space, on the ground, and at sea;

- The significantly greater difficulty of collecting human intelligence, given the advent of biometrics and other personal identifying capabilities and the increased array and diversity of targets;

- The increasing difficulty of processing and deriving value from vast amounts of data collected;

- Resolving privacy and civil liberties matters associated with accessing and processing "content data" involving U.S. citizens in social media outlets; and

- The expanded use of industrial base encryption, which could severely limit intelligence access to the plans and intentions associated with those who wish us harm.

There are no simple or quick solutions to the challenges facing U.S. intelligence, but the problems are not insurmountable. Several key actions can contribute to finding long-term solutions to these challenges. They start with ensuring that the best and brightest intelligence professionals are hired, retained, and then given all of the specialized training and technology necessary to equip them for success. Further integration of officers with a wide variety of skills among the IC elements—physically and/or virtually—against specific mission objectives is likewise essential.

Additionally, continued sharing of information is vital with appropriate "insider threat" protections in place.[60] Human intelligence operations will need to adapt continually to stay ahead of the threats posed by adversaries' use of technology. Policies promulgated by the DNI are required to address the mounting uncertainty among intelligence professionals about how to handle U.S. person information acquired by means of open sources. For the IC to be successful, it must be agile and integrated with other agencies and partners and must have a firm grasp of the operational environment.[61]

One of the lessons learned from the wars in Iraq and Afghanistan is that integrating intelligence into operations increases the likelihood of a successful military plan and operation.[62] Experience on the ground in the war zones underscored the importance of having the intelligence professional working alongside the operator for at least two critical reasons:

- The operators learned they could feed requirements into a collection process that was better refined by working with the intelligence professional.

- The delivery time for potentially highly perishable material was much faster when the intelligence officer worked directly with the operator to apply that intelligence to specific operations.

Challenges remain, however, in ensuring collaboration against emerging threats such as those presented by an adversary's use of cyberspace. Both non-state actors and governments are improving their offensive and defensive cyber capabilities and enhancing their ability to use social media to communicate and promote their agendas (or causes) and justify aggressive behavior while operating with impunity outside of borders.[63]

Enhancing intelligence collection and analysis to serve the Intelligence Community's wide array of customers is an ongoing process. Determining where investments in intelligence need to be made remains critical to improving the IC's intelligence capacity and capabilities to address not only current intelligence demands, but also those that will evolve as adversaries change their methods to thwart defense capabilities. Along with the changing nature of the threats, the role that intelligence must play in shaping U.S. defense strategy and investments takes on greater significance in the face of fiscal austerity as defense spending contracts.

Within the Department of Defense, the effort to unify the defense intelligence components falls to the Undersecretary of Defense for Intelligence (USD/I) and is known as the Pentagon's Defense Intelligence Enterprise (DIE). (See text box, "Defense Intelligence Enterprise.") The DIE is governed by policies directed by the USD/I.[64]

Collaboration among the various DIE elements has improved, especially because of the growing demand from intelligence customers for products that provide a multi-disciplinary quality and are not necessarily produced by personnel located in one organization or facility. Continuing resistance from DIE elements to drafting and publishing joint analytical products leads to some duplication of effort, and access to relevant information by all DIE components remains a challenge.

The DIE emerged in 2003 from the establishment of the office of the USD/I in the DOD under Secretary

DEFENSE INTELLIGENCE ENTERPRISE

The Enterprise is composed of intelligence, counterintelligence, and security components of the Defense Department's Joint Staff, Combatant Commands, Military Departments, and other Department elements, as well as those organizations under the authority, direction, and control of the Under Secretary of Defense for Intelligence.

Source: U.S. Defense Intelligence Agency, 2012–2017 Defense Intelligence Agency Strategy: One Mission. One Team. One Agency, p. 3, http://www.dia.mil/Portals/27/Documents/About/2012-2017-DIA-Strategic-Plan.pdf (accessed August 20, 2015).

of Defense Rumsfeld.[65] Former USD/I Dr. Michael Vickers has noted that:

> [The intent of defense-focused intelligence transformation] is not just to deal with the challenges we face and to make sure we sustain the intelligence advantage for our policymakers and operators decades into the future.... [I]t's also to inform and enable some of the new strategic and operational approaches that will be required to deal with these challenges.[66]

The DIE has focused on identifying ways to resource, develop, and process critical intelligence requirements most effectively in support of operations that can and ultimately must make the knowledge derived from the collectors instantly available to operators and analysts.

While dollars and cents are not everything, good intelligence does cost money. Congress funds America's intelligence activities through two separate programs: the National Intelligence Program (NIP),[67] which the DNI oversees, and the Military Intelligence Program (MIP), which the Secretary of Defense executes with the DNI's advice.[68] For much of the past decade, the DOD has focused on fighting terrorism and countering violent insurgencies and has been funded for expanded and sustained operations in this area, but fiscal conditions have changed. Both the defense and intelligence budgets are falling. Consider the changes in fiscal year budget requests as reflected in Chart 1.

Though the FY 2015 intelligence budget appropriation has not yet been disclosed,[69] the Administration's FY 2016 budget request, submitted on February 2, 2015, included a request of $53.9 billion for the National Intelligence Program.[70] The Department of Defense requested $17.9 billion for the Military Intelligence Program in FY 2016.[71] (See Chart 1.)

In absolute terms, it is difficult to ascertain the exact dollar value of intelligence. What is easier to understand is that cutting funding for intelligence at a time when threats are increasing in number and complexity will result inevitably in a commensurate decrease in the IC's ability to meet the growing demands from the intelligence customer. Against that backdrop, the declining budgets have given rise to a debate about whether less funding for intelligence will increase the risk to the nation after the decade of spending growth that followed 9/11.[72] In response to this debate, two points should be considered.

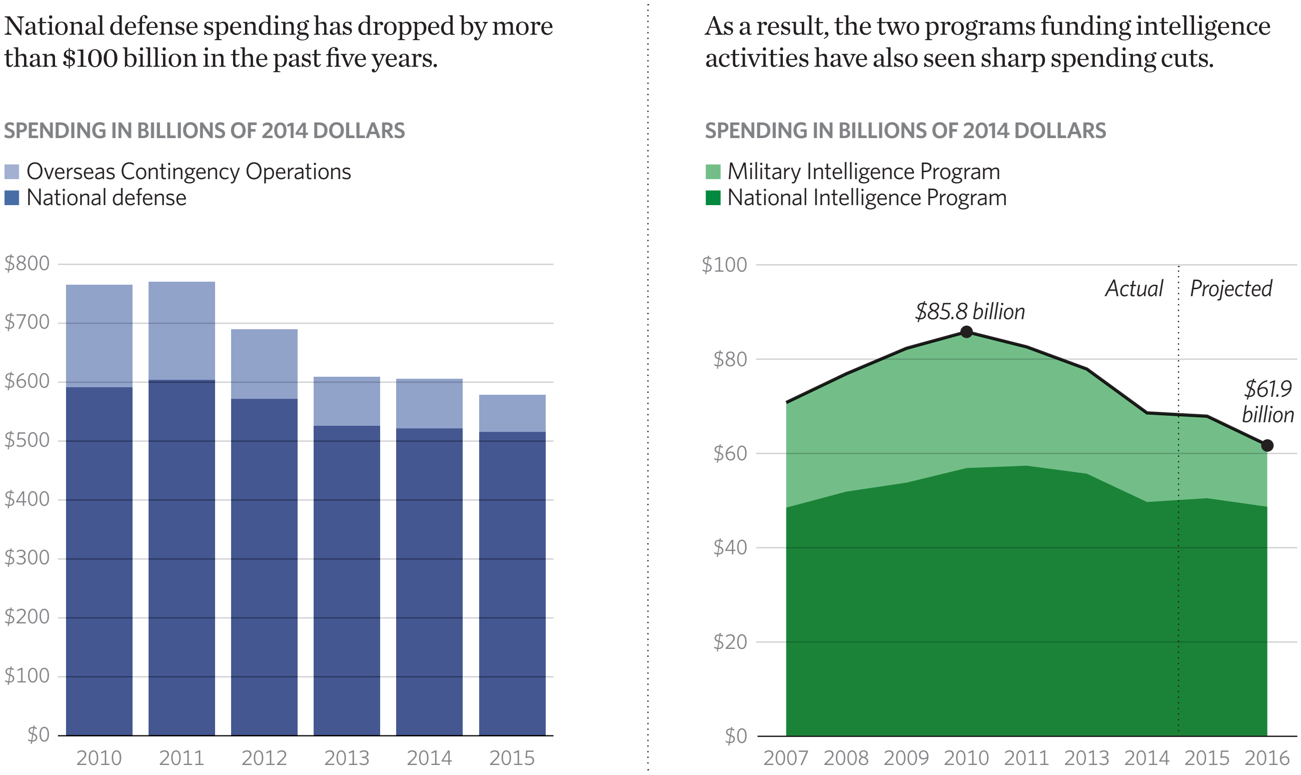
First, the commitment to intelligence funding is an indicator of commitment to maintaining and/or building intelligence capabilities and capacity to meet both current and future challenges. There is no direct and uniform connection between more money spent and better knowledge gained. A well-trained analyst, a well-placed asset, a conscientious technologist, or a watchful FBI agent can contribute more to our national security in some circumstances than a costly satellite or imagery device.

Furthermore, an integrated workforce can amount to more than the mere sum of its parts, and by leveraging the various components of the Intelligence Community together, more can be achieved with less than ever before. However, gaining insight into the intent and workings of competitors and enemies should not become critically dependent on a few conscientious or watchful analysts. Too much is at stake to trade capacity for luck.

Second, that being said, some intelligence capabilities do require significant investment. For instance, building the next generation of defense intelligence capabilities requires investment in research and development, and grooming the next generation of intelligence officers means spending now to train and nurture their talents. Will a budget reduction mean the end of American intelligence dominance? Probably not, but that does not mean we should not be concerned that further cuts might be applied in a helter-skelter fashion that is penny-wise and pound-foolish.

CHART 1

National Defense and Intelligence Spending on the Decline



National defense spending has dropped by more than $100 billion in the past five years.

As a result, the two programs funding intelligence activities have also seen sharp spending cuts.

Source: U.S. Government Publishing Office, "Budget of the United States Government," http://www.gpo.gov/fdsys/browse/collectionGPO.action?collectionCode=BUDGET (accessed August 14, 2015), and FAS Intelligence Resource Program, "Intelligence Budget Data," http://fas.org/irp/budget/ (accessed August 21, 2015).

heritage.org

Achieving a More Effective Defense Intelligence Enterprise

In order to improve what is already a significant U.S. defense capability supported by extraordinary intelligence capabilities, American intelligence should continue on the path of enhancing the integration of intelligence obtained from all sources and by all IC elements. Further, it will be increasingly important that integrated intelligence be tailored to answer strategic as well as tactical questions for customers and provide timely support to warfighter and President alike. To accomplish this, the Enterprise must have the ability to draw from all forms of collection sources that range from clandestinely acquired intelligence to open-source information.

To improve U.S. defense intelligence capabilities, components of the Defense Intelligence Enterprise should focus their attention on three key areas:

- *Ensuring that information technology (IT) investments provide secure global IT solutions applied to large holdings of data that make information easily and securely accessible across the Defense Intelligence Enterprise.* Breaking down barriers to information sharing across various defense components where data are currently restricted for bureaucratic reasons remains a significant issue. The users of intelligence need timely discovery and exploitation of the intelligence in a secure but collaborative environment.

As the Pentagon thinks about the IT enterprise, it must account not only for traditional foreign partners, but also for newly emerging intelligence country partners. The IC elements that collect and disseminate sensitive information must also be assured that the information is protected from insiders and others who seek to compromise intelligence. This assurance can be achieved only by means of real-time audit capabilities with respect to the handling of sensitive information.

- *Applying scarce resources to training in order to match the challenges of the intelligence workforce.* Investments in cyber, foreign language, and analytical training to address modern challenges are critical to take full advantage of technological improvements. We need a more networked and integrated workforce of analysts and collectors working side-by-side.

  The large number of Washington-based analysts and intelligence professionals who shape the collection requirements must be significantly better interconnected with the smaller cadre of experts at the Combatant Commands and the military Service Centers—the Army's National Ground Intelligence Center, the Air Force's National Air and Space Intelligence Center, the Navy's Office of Naval Intelligence, and the Marines' Center for Intelligence Analysis—in order to reap the benefits of deep subject expertise. Conversely, an integrated and collaborative workforce will ensure that military planners and operators who are under pressure to meet tactical and operational requirements have access to their peers in Washington who can help by providing strategic context for tactical intelligence and real-world events that operators face every day.

- *Combining the intelligence budget allocations for the National and Military Intelligence Programs to improve the efficiency of the allocation of resources to intelligence capabilities.* Combining both budgets will also provide for increased flexibility in resource allocation while minimizing redundancy of intelligence resources against dynamically changing threats.

  Achieving this combination of funding will require reforms among overlapping congressional oversight committees as well as agreements between the Secretary of Defense and the DNI on setting joint investment priorities. As it pertains to defense intelligence investments, properly assessing the value of the intelligence output is critical to maintaining and improving the ability of our military forces to win the war.

Conclusion

Intelligence has always played an important role in our national defense. The demand for accurate intelligence delivered on a timely basis will only increase as the complexity of the threats facing the U.S. and its allies grows.

To be effective, both in today's environment and for the foreseeable future, our defense capabilities will require that intelligence be integrated into all levels of operational planning. We can expect that the demand for more precise intelligence on our adversaries will grow. The needs by each of the uniformed services and the Combatant Commands will require that the defense and non-defense intelligence components of the Intelligence Community align their resources, capabilities, and mission goals to the point where information sharing and integration become common practice.

The goal of the entire intelligence enterprise should always be to create new knowledge, including actionable knowledge that aids decision makers in preventing conflicts where possible or winning the conflict should conflict be necessary. At the same time, the entire American Defense Intelligence Enterprise requires more integration of its multi-disciplinary capabilities such as the collection platforms and analytic expertise that reside in various agencies and organizations.

Defense intelligence for and by the military services and the Combatant Commands will place a high premium on the ability to access real-time information ranging from HUMINT to SIGINT, GEOINT, and open-source information. This expanded interconnected intelligence process will free expert analysts to focus on more complex higher-order analysis. A secure IT network linking all relevant intelligence sources and operators will be a crucial enabler. The end result will be a more timely, efficient, flexible, and effective Defense Intelligence Enterprise that draws on information from all elements of the Intelligence Community and makes our nation more secure for current and future traditional and non-conventional military operations.

Endnotes:

1. See, for example, John Keegan, *Intelligence in War: Knowledge of the Enemy, From Napoleon to Al-Qaeda* (New York: Alfred A. Knopf, 2003).
2. Adrienne Wilmoth Lerner, "Espionage and Intelligence, Early Historical Foundations," *Encyclopedia of Espionage, Intelligence, and Security*, 2015, http://www.faqs.org/espionage/Ep-Fo/Espionage-and-Intelligence-Early-Historical-Foundations.html (accessed July 22, 2015).
3. Ibid.
4. Ibid.
5. Ben MacIntyre, *Operation Mincemeat: How a Dead Man and a Bizarre Plan Fooled the Nazis and Assured an Allied Victory* (New York: Broadway Paperbacks, 2011).
6. Fact Sheet, "War of Secrets: Cryptology in WWII," National Museum of the US Air Force, May 1, 2015, http://www.nationalmuseum.af.mil/Visit/MuseumExhibits/FactSheets/Display/tabid/509/Article/196193/war-of-secrets-cryptology-in-wwii.aspx (accessed August 2, 2015).
7. The Honorable Laurence H. Silberman et al., Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, letter to President George W. Bush, March 31, 2005, p. 1, http://fas.org/irp/offdocs/wmd_transmittal_letter.pdf (accessed July 22, 2015).
8. Ibid.
9. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed. (Washington: CQ Press, 2011), p. 8.
10. "Intelligence," Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/intelligence (accessed July 22, 2015).
11. Ibid.
12. U.S. Department of Defense, Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01, January 5, 2012, p. xi. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf (accessed July 22, 2015).
13. Ibid.
14. Claudette Roulo, "Cuts Make Intelligence Failures Likely, Top Intel Official Says," American Forces Press Service, April 18, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119809 (accessed August 2, 2015); Tate Nurkin, "Analysis: Declining US Military Spending Pressures Defence Contractors," IHS Jane's 360, September 19, 2014, http://www.janes.com/article/43346/analysis-declining-us-military-spending-pressures-defence-contractors (accessed July 22, 2015); The Hon. John M. McHugh, Secretary of the Army, and General Raymond T. Odierno, Chief of Staff, United States Army, testimony in hearing, *The Postures of the Department of the Army and the Department of the Air Force*, Committee on Armed Services, U.S. Senate, March 18, 2015, http://www.armed-services.senate.gov/hearings/15-03-18-the-postures-of-the-department-of-the-army-and-the-department-of-the-air-force (accessed July 22, 2015).
15. See Daniel Gouré, "Building the Right Military for a New Era: The Need for an Enduring Analytic Framework," in *2015 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2015), p. 32, http://www.index.heritage.org/militarystrength/militarystrength/important-essays-analysis/building-right-military-new-era/.
16. Ibid.
17. Ibid., p. 28.
18. Ibid., p. 33.
19. "Chairman's Foreword," in U.S. Department of Defense, Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015: The United States Military's Contribution to National Security*, June 2015, p. i, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf (accessed August 2, 2015).
20. "Strategic Environment," in Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America 2014*, p. 4, http://www.dni.gov/files/documents/2014_NIS_Publication.pdf (accessed August 2, 2015).
21. Ibid.
22. Ibid.
23. Ibid.
24. Ibid.
25. Ibid.
26. Office of the Director of National Intelligence, "Intelligence Community," http://www.odni.gov/index.php (accessed July 22, 2015).
27. Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, December 17, 2004.
28. George W. Bush, Executive Order 13470, "Further Amendments to Executive Order 12333, United States Intelligence Activities," July 30, 2008, http://www.gpo.gov/fdsys/pkg/WCPD-2008-08-04/pdf/WCPD-2008-08-04-Pg1064.pdf (accessed August 2, 2015).
29. Office of the Director of National Intelligence, "Mission, Vision & Goals," http://www.dni.gov/index.php/about/mission (accessed July 22, 2015).
30. Intelligence Reform and Terrorism Prevention Act of 2004.
31. Paul Szoldra, "These 17 Agencies Make Up the Most Sophisticated Spy Network in the World," *Business Insider*, May 11, 2013, http://www.businessinsider.com/17-agencies-of-the-us-intelligence-community-2013-5?op=1 (accessed July 22, 2015).

32. Central Intelligence Agency, "CIA Vision, Mission, Ethos & Challenges," last updated December 16, 2013, https://www.cia.gov/about-cia/cia-vision-mission-values (accessed August 3, 2015).
33. National Security Act of 1947, 50 U.S.C. Ch. 15 § 102(a) (1947).
34. Intelligence Reform and Terrorism Prevention Act of 2004, § 103(a).
35. Ibid.
36. Office of the Director of National Intelligence, "Members of the IC: Defense Intelligence Agency," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#dia (accessed August 3, 2015).
37. Office of the Director of National Intelligence, "Members of the IC: National Geospatial-Intelligence Agency," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#nga (accessed August 3, 2015).
38. Office of the Director of National Intelligence, "Members of the IC: National Reconnaissance Office," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#nro (accessed August 3, 2015).
39. National Security Agency/Central Security Service, "Mission," last modified April 15, 2011, https://www.nsa.gov/about/mission/index.shtml (accessed July 22, 2015).
40. Ibid.
41. Executive Order 13470.
42. Federal Bureau of Investigation, Intelligence Branch, "Intelligence Branch Overview," https://www.fbi.gov/about-us/intelligence/intelligence-branch-overview (accessed July 22, 2015).
43. Ibid.
44. Office of the Director of National Intelligence, "Members of the IC: Department of Energy," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#doe (accessed August 3, 2015).
45. U.S. Department of Homeland Security, "Office of Intelligence and Analysis Mission," last published date June 29, 2015, http://www.dhs.gov/office-intelligence-and-analysis-mission (accessed August 3, 2015).
46. Office of the Director of National Intelligence, "Members of the IC: Department of Homeland Security," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#dhs (accessed August 3, 2015).
47. Office of the Director of National Intelligence, "Members of the IC: Department of State," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#dos (accessed August 3, 2015).
48. Szoldra, "These 17 Agencies Make Up the Most Sophisticated Spy Network in the World."
49. Office of the Director of National Intelligence, "Members of the IC: Department of the Treasury," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#dot (accessed August 3, 2015).
50. U.S. Department of the Treasury, "About: Terrorism and Financial Intelligence: Office of Intelligence and Analysis (OIA)," last updated August 16, 2012, http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Intelligence-Analysis.aspx (accessed August 3, 2015).
51. Office of the Director of National Intelligence, "Members of the IC: Drug Enforcement Administration," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#doj (accessed August 3, 2015).
52. Office of the Director of National Intelligence, "Members of the IC: Air Force Intelligence," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#usaf (accessed August 3, 2015).
53. Office of the Director of National Intelligence, "Members of the IC: Army Intelligence," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#usa (accessed August 3, 2015).
54. Szoldra, "These 17 Agencies Make Up the Most Sophisticated Spy Network in the World."
55. Office of the Director of National Intelligence, "Members of the IC: Marine Corps Intelligence," http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#usmc (accessed August 3, 2015).
56. Office of Naval Intelligence, "Our Mission," http://www.oni.navy.mil/This_is_ONI/our_mission.html (accessed July 22, 2015).
57. Michael V. Hayden, "The State of the Craft: Is Intelligence Reform Working?" *World Affairs*, September/October 2010, http://www.worldaffairsjournal.org/article/state-craft-intelligence-reform-working (accessed August 3, 2015); Michael Allen, *Blinking Red: Crisis and Compromise in American Intelligence After 9/11* (Lincoln, NE: Potomac Books, 2013).
58. Associated Press, "Al-Qaida in Iraq's al-Zarqawi 'Terminated,'" NBC News, updated June 8, 2006, http://www.nbcnews.com/id/13195017/ns/world_news-mideast_n_africa/t/al-qaida-iraqs-al-zarqawi-terminated/#.Va_4z_lVhBc (accessed August 3, 2015).
59. James R. Clapper, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee," February 26, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (accessed July 22, 2015).
60. For more on insider threats, see Federal Bureau of Investigation, "The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy," https://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat (accessed August 3, 2015).

61. Claudette Roulo, “Changing World Challenges U.S. Intelligence Community,” American Forces Press Service, November 21, 2013, http://www.defense.gov/news/newsarticle.aspx?id=121201 (accessed August 3, 2015).

62. Lieutenant General Michael T. Flynn, United States Army, and Brigadier General Charles A. Flynn, United States Army, “Integrating Intelligence and Information: ‘Ten Points for the Commander,’” *Military Review*, January–February 2012, pp. 4–8, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20120229_art005.pdf (accessed August 3, 2015).

63. Clapper, “Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee,” p. 1.

64. U.S. Department of Defense, “Marcel Lettre: Acting Under Secretary of Defense for Intelligence,” http://www.defense.gov/bios/biographydetail.aspx?biographyid=381 (accessed August 3, 2015).

65. Janet A. McDonnell, “The Office of the Under Secretary of Defense for Intelligence: The First 10 Years,” *Studies in Intelligence*, Vol. 58, No. 1 (Extracts, March 2014), p. 9, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-58-no-1/pdfs/McDonnell-Ten%20Years%20of%20USDI.pdf (accessed August 3, 2015).

66. Cheryl Pellerin, “Vickers: Intelligence Enterprise Poised for Historic Transition,” DOD News, Defense Media Activity, January 21, 2015, http://www.defense.gov/news/newsarticle.aspx?id=128006 (accessed July 22, 2015).

67. Fact Sheet, “National Intelligence Program,” Office of the Director of National Intelligence, 2015, http://www.dni.gov/files/documents/FY%202016%20NIP%20Fact%20Sheet.pdf (accessed August 3, 2015).

68. News release, “DoD Releases Military Intelligence Program Base Request for Fiscal Year 2016,” U.S. Department of Defense, February 2, 2015, http://www.defense.gov/releases/release.aspx?releaseid=17128 (accessed August 3, 2015).

69. News release, “DNI Releases Updated Budget Figure for FY 2015 Appropriations Requested for the National Intelligence Program,” Office of the Director of National Intelligence, November 21, 2014, http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1141-dni-releases-updated-budget-figure-for-fy-2015-appropriations-requested-for-the-national-intelligence-program-14 (accessed July 22, 2015).

70. News release, “DNI Releases Requested Budget Figure for FY2016 Appropriations for the National Intelligence Program,” Office of the Director of National Intelligence, February 2, 2015, http://www.fas.org/irp/news/2015/02/nip-2016.pdf (accessed August 3, 2015).

71. News release, “DoD Releases Military Intelligence Program Base Request for Fiscal Year 2016.”

72. See, for example, Federation of American Scientists, “Intelligence Resource Program,” website, http://fas.org/irp/ (accessed August 3, 2015).