Intelligence Failures: Matters of Homeland and National Security

Manuel F. Zamora

Angelo State University, Center for Security Studies

ABSTRACT

The intelligence community and others agree that the end of the Cold War proved to be a watershed for the U.S. strategy concerning homeland and national security forever. Following the attacks on 9/11, a new security concern proliferated: Diffuse, complex, loosely-knit insurgent and extremist groups, bound in many cases by ideological and political beliefs, pose surprises and asymmetric threats to the U.S. The issues and challenges associated within this context involve political strategies and decisions, oversight, funding, structure, and constitutional issues. Intelligence failures involving recent events, such as the *Boston Marathon bombing*, *Wikileaks*, the *Benghazi* assault, *Fast and Furious*, and the initial failure to bring *Osama bin Laden* to justice, amplify the need for maturity and efficacy of policies, such as clearer national strategies, improved management of data and information, enhanced criminal sanctions for national security breaches, a better understanding of the intelligence process, increased coordination, and mediating tension between security needs and civil liberties inherent in a democracy.

Key words: Intelligence community, 9/11, security, liberties, democracy

Intelligence Failures: Matters of Homeland and National Security

A nation's ability to acquire and act upon the intelligence she processes often determines whether a security breach will cause her significant harm. The issues and challenges associated with intelligence in a post-9/11 world have become greater, more complex, sophisticated, and difficult to detect, anticipate, and effectively resolve. The U.S. policy on intelligence within this context has struggled to keep up with this dynamic and immeasurable change. The U.S. intelligence community (IC) operates with clear oversight and accountability, emphasizing the protection of human rights and the rule of law. The fundamental structure of the U.S. approach to intelligence comports to this system of checks and balances[1].

In order to understand the intelligence issues and challenges, it is necessary to understand that, unlike the Cold War, where the adversary is well-known and threats are assessed in terms of military capability, there is a different, asymmetric threat. Today, sources state that small groups of terrorist conspirators, irregular resistance groups in the Middle East, and so-called rogue regimes in N. Korea and Iran are significant threats. The threats lie principally in their plans, which are not detectable by satellites, and in the handfuls of instruments of destruction they may acquire that are easier to hide than Soviet missile complexes or armored divisions (Betts, 2007, p. 7). The dawn of this new era of complexity brings challenges that are numerous, unprecedented, unstable, turbulent, and unpredictable. They extend beyond the traditional domain of any single government agency and have thus diversified the issues and challenges of post 9/11 security policy (Gates 2007). We begin the discussion on intelligence issues and challenges within the context of global change and its impact.

Background

The trajectory and domain of intelligence changed when the Cold War ended, around 1991; again, immediately after the al-Qaeda attacks of 9/11/2001; and now recently, with a better understanding that today a new national threat climate exists. The challenge for the IC is to understand this context, the culture, and its rationality, particularly in improving intelligence in the current environment. The danger and challenges of old have been joined by new forces of instability and conflict. These include:

- A new and more malignant form of global terrorism rooted in extremist and violent *jihadism*[2];

[1] The intelligence community is part of, and works for, the executive branch. For example, the National Security Act states that the National Intelligence Council "shall prepare national intelligence estimates for the Government" (the president or the president's senior cabinet officers)(Betts, 2007, p. 244). The U.S. system of "separation of powers" ensures effective government and protection of citizen rights via responsibilities of the executive, legislative, and judicial branches of government.

[2] For a discussion of the affiliates, allies, and sympathizers see *U.S. Community, Worldwide Threat Assessment, Statement for the Record*, Senate Select Committee on Intelligence (retrieved from http://www.intelligence.senate.gov/130312/clapper.pdf). *Jihadism* is a "defensive, just war" (http://www.jihadwatch/ 2007/) or an extreme version of Islamism, in which unbelievers are worthy of attack because their sole purpose is to destroy Islam. Therefore, violence must be used to create the *Caliphate*, which

- New manifestations of ethnic, tribal, and sectarian conflict all over the world;
- The proliferation of weapons of mass destruction;
- Failed and failing states;
- States enriched with oil profits and discontented with the current international order; and
- Centrifugal forces in other countries that threaten national unity, stability, and internal peace – but also with implications for regional and global security (Gates, 2007).

To address these issues, significant change should take place, including a clearer philosophy and strategy on national security, new decision-making thought processes, reformed structure and function of organizations, integrated intelligence, improved funding, information-sharing, and joint collaboration. The change will be historic and monumental. To understand its context, a person must examine the intelligence climate change.

Demise of the Superpower Adversary

Analysts and historians agree that former Soviet leader Mikhail Gorbachev played a pivotal role in the events leading to the fall of the Berlin Wall and beyond. His policies of restructuring and openness contributed to the dissolution of communist power in Eastern Europe and ultimately led to the collapse of the Soviet Union. On July 31, 1991, U.S. President George Bush and Soviet President Mikhail Gorbachev signed the Strategic Arms Reduction Treaty (START 1), reducing strategic nuclear weapons and leading to transparency and verification provisions. The START 1 treaty expired in 2009[3], and was reauthorized by President Barack Obama and Russian President Dmitry Medvedev on May 14, 2010.

"Russia and U.S. Presidents say the new START treaty marks the end of the Cold War," retrieved from http://en.rian.ru/world/20100514/159012782.html.

maintains a struggle against unbelievers (from http://www.web.mit.edu/ssp/seminars/wed_archieves06spring/habeck.html).

[3] Treaty obligations included a 15 year duration, in addition to mutual reduction of warheads to 6,000, banning new types of heavy ICMS and SLBMs, testing missiles equipped with greater numbers of warheads than established by the Treaty, data exchange (including numbers and locations of strategic delivery vehicles), on-site inspections, perimeter and portal monitoring of plants, a ban on encryption of telemetry transmitted from ballistic missiles during test launches and exchange of all such telemetry, and bilateral consultations (retrieved from http://www.nti.org/treaties-and-regimes/treaties-between-united-states-america-and-union-soviet-socialist-republics-strategic-offensive-reductions-start-i-start-ii/; and http://en.rian.ru/world/20100408/158483818.html).

The change in threat focus proved to be of utmost relevance to the U.S. IC; the principal U.S. adversary had been the Soviet Union, and threats had been measured primarily in terms of field military forces or Marxist allies in other countries"(Gates, 2007). "America's principal adversary was a coalition of lumbering, bureaucratic, and technologically-challenged nation-states led by the Soviet Union" (Lederman 2009). "These entities were easier to locate and monitor than are al Qaeda-inspired cells or the small numbers of weapons of mass destruction that hostile states such as N. Korea may hide" (Gates, 2007). Furthermore, "during the Cold War, about two-thirds of the total U.S. intelligence budget was focused on Soviet Union and NATO military concerns, and most of that on order-of-battle data – the type, number, location, and weaponry of armed forces and over half the nation's intelligence budget was allocated to military subjects" (Gates, 2007). **This context must be mentioned in the study of intelligence evolution within the U.S. political, economic, and social milieu because it provokes thought into dealing with elusive, smaller, agile, and anonymous enemies**. Therefore, our priorities must change to better deal with 'asymmetric warfare' [the smaller, irregular forces – insurgents, guerrillas, terrorists]; the mainstay of the contemporary battlefield (Gates, 2007).

The New Era

Failing to adapt to a dynamic, networked world is a significant barrier to intelligence success in the post 9/11 era. "The attacks on 9/11 showed us that the Cold War 'need to know' system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes and secretive pockets of the nation's most valuable information" (Budlinger & Smith, 2011, p. 1)[4]. The "virtual reorganization" in the new era of intelligence reveals how agencies at all levels across government and their employees must better coordinate, collaborate, and communicate. The paragraphs that follow discuss the issues and challenges to intelligence within the new era, - post 9/11.

Issues and Challenges

Significant progress has been accomplished within the IC; however, it is not without resistance. Recently, James Clapper, the Director of National Intelligence, stated,

> We've made significant progress in reducing the cultural, information technology and policy barriers to sharing information among agencies, and we continue to explore new strategies for integrating our intelligence efforts. We no longer operate largely on the principle of compartmentalization, that is,

[4] Zoe Budinger, President of Markle Foundation, served as chair to the Task Force on National Security in the Information Age. She was Advisory Board member on the President's Foreign Intelligence Committee and the Department of Defense Technology and Privacy Advisory Committee. Mr. Smith is former General Counsel for the CIA and currently serves on the CIA's External Advisory Board. He is a member of the Markle Task Force. Budinger & Smith determined that a significant factor to lost "operational opportunities" in the War on Terror, is a "Wall" between law enforcement and intelligence, characterized by a CIA analyst who told the 9/11 Commission that he did not volunteer information he knew about a suspected terrorist when shown a surveillance photo by the FBI because 'he was not authorized to answer FBI questions regarding CIA information' (Kean et al., 2004, p. 269; *9/11 Commission Report*). These and other similar issues are discussed by Zegart (2005) in her analysis of adaptation failure within complex organizations, particularly those in the IC.

> sharing information based on "need to know." We now start from the imperative of "responsibility to share," in order to collaborate with and better support our intelligence consumers—from the White House to the foxhole (Clapper, 2011, Retrieved from http://online.wsj.com/article/).

However, the paragraphs that follow reveal a significant concern that all is not as peachy or rosy. For example, the U.S. Department of Justice is quite clear in its assessment of the IC. Improvement areas are:

- Improved investigations and criminal prosecutions;
- Structural changes are needed to enhance counterterrorism efforts;
- Legal changes permeate the working environment;
- Privacy and civil liberties of Americans raise questions; and
- Partnerships and collaborations are needed to better manage new information (retrieved from www.justice.gov/911/counterparts.html).

We now turn to a review of several issues and challenges involving the intelligence community. **Appendix A** below identifies various current issues and challenges. However, this paper is limited to a discussion of this author's top three. The remaining issues are fodder for future publication.

Issue: Executive level clarity on U.S. policy; Challenges include foreign relations, effect of decision-making, and defense planning. The job of decision makers in the IC is to make decisions, so they cannot defer judgment in ambiguous situations. If the circumstances lack clarity, an abundance of conflicting data or information, or a lack of time for rigorous assessment exists:

> Ambiguity abets instinct and allows intuition to drive analysis; intelligence may fail because the data is too permissive for policy judgment rather than too constraining. When fragments of evidence support various interpretations, ambiguity is exploited by wishfulness: [The] greater the ambiguity, the greater the impact of preconceptions. Cognitive theory suggests that uncertainty provokes decision makers to separate rather than integrate their values, to deny that inconsistencies between values exist, and even to see contradictory values as mutually supportive (Betts, 2007, p. 31).

These dynamics support the need for clear policies, strategies and visions, in part, to address cognitive difficulties. Betts (2007) believes that failure in perspective, pathologies in communication, and paradox of perception lead to intelligence failure, and "In the best-known cases, the most crucial mistakes have often been committed by the decision makers. Policy premises constrict perception, and administrative workloads constrain reflection. The available information seldom points unambiguously to the correct conclusion" (p. 19).

Accordingly, Trujillo (2012), notes that ambiguity of evidence, ambivalence of judgment, and the atrophy of reforms lead to inevitable intelligence failures. Intelligence reform is needed

not only because intelligence is one link in the chain of executive branch counterterrorism activities, but also because it is critical for improving the performance of each executive branch activity against terrorism (Lederman, 2009, p. 90). Cumulatively, these observations support the need for the executive branch to develop clear policies. The challenges, one of which is discussed below on the Pakistan foreign relations and diplomacy issue, also include defining a strategy for national defense[5].

The need for clear policy is also significant to reduce the self-interest of presidents, legislators, and government bureaucrats, which work against executive branch reform, one of the three adaptation failures identified by Zegart (2005). A clear policy on national security includes within it an understanding of the imperative for organizational change necessary to meet the threat climate. Policy also includes setting executive and agency priorities and developing advanced theories of effective organizational behavior and culture within an environment of changing threats and priorities.

Finally, the national strategy must consider dramatically increasing civilian instruments of national security – diplomacy, strategic communications, foreign assistance, civic action, and economic reconstruction and development (Gates, 2007). The use of Provincial Reconstruction Teams (PRT) in Afghanistan and in Iraq are evidence of this strategy's success. The PRTs brought experience and knowledge of agriculture, governance, and other aspects of economic development to work alongside military forces to improve the lives of local populations. This is believed to be an essential tenet in the counterinsurgency effort.

Issue: Funding the intelligence effort; Challenges are budgetary constraints and force multipliers. The next issue involves the funding aspect of intelligence. On February 23, 2009, President Barack Obama stated,

> My highest priority is to keep the American people safe. I believe that Homeland Security is indistinguishable from national security – conceptually and functionally, they should be thought of together rather than separately. Instead of separating these issues, we must create an integrated, effective, and efficient approach to enhance [our] national security of the United States (National Security Strategy, 2010, *Introduction*).

[5] The 2010 National Security Strategy mentions the Armed Forces as the cornerstone of security, but elaborates that the efforts must be complemented by diplomacy and effective foreign policy, governance experts, and intelligence and law enforcement coordination and collaboration. The national strategy is to renew American leadership, shape international order, and enhance the connection between national security, national competitiveness, resilience, and moral example. Therefore, the U.S. is pursuing a comprehensive nonproliferation and nuclear security agenda, holding nations like Iran and N. Korea accountable for failing to meet international obligations, securing all vulnerable nuclear materials from terrorists, pursuing new strategies to protect against biological attacks and challenges to cyber networks. Finally, the U.S. seeks to disrupt, dismantle, and defeat al-Qaeda and all its affiliates throughout the world, realizing that the frontline is Afghanistan and Pakistan. This strategy provides the clear cut direction needed within the IC.

Likewise, on January 27, 2011, DHS Secretary Janet Napolitano reported, "the threats we now face demonstrate that our homeland security is a shared responsibility: only a 'whole of nation approach' will bring us to the level of security and resilience we require" (Budget Statement). A review of funding for national security (FY2010 & FY2012) reveals a decrease of $18.05 billion (Table 1). It is clear that, to adequately control global threats, the IC must reform in structure and function, in part, seeking "force multipliers." The dismantling of al Qaeda, a U.S. strategic objective, given budget constraints, must thus invoke extraordinary effort. Al Qaeda has been described as one part of the excrescence of extremist ideology that has swept across the Middle East and beyond, and a global IC strategy must still be effective despite reduced funding.

Table 1. Narrow View of National and Homeland Security Budget Appropriations[6]

FY2010 and FY2012 Federal Budget Appropriations (in billions)			
Effort/Agency	FY2010	FY2012	
National Defense	$691.00	$670.90	
Department of Homeland Security	$59.10	$56.98	
Department of Justice	$24.03	$28.20	
Total	$774.13	$756.08	$18.05

Issue: Tensions between security needs and civil liberties; challenges include communication, searches and seizures, and surveillance. Many citizens believe that the IC "snoops into the daily lives of Americans, from monitoring library records to eavesdropping on phone calls to collecting data on travel records with virtual impunity[7]" (Kucinich, 2006, p. 10). Surveillance and reasonableness of protected searches and seizures at the following junctions continue to lead to citizen complaints: Airline passenger screening, wiretaps and electronic surveillance, arrests without warrants, oversight of social media, FBI use of national security letters (to acquire financial, credit, and other information on U.S. citizens without court order) (McElhatton, 2011).

"Compromising one element of liberty--privacy—will fortify more important civil liberties" (Betts, 2007, p. 7). Federal agencies continue to gain approval to expand the scope and depth of criminal and civil investigations, including those involving U.S. citizens traveling abroad. The American Civil Liberties Union remains vigilant in seeking to ensure civil liberties

[6] The figures are based upon final appropriations reports distributed by the White House and the Office of Management and Budget (for example, http://www.whitehouse.gov/omb/fy2010_department_justice).

[7] U.S. Rep. Dennis J. Kucinich testimony before the 2006 House Subcommittee on National Security, Emerging Threats and International Relations, questioning the development of the Privacy and Civil Liberties Board at the White House, post 9/11, citing failure of the Board to meet. The Board's authority was derived from the Intelligence Reform and Terrorism Prevention Act of 2004. This has been referred to as a "paper tiger," as the Board had no authority to veto or delay executive branch actions or to order specific remedial actions. In 2007 Congress gave the Board subpoena powers. It remains inactive, with three vacant board positions.

are not encroached upon or suppressed. The challenge for the IC is to remain effective in its operations, yet cautiously yield to protecting constitutional rights.

Evolution of Intelligence Policy (2003-2012)

The most notable IC policy improvements within the past decade are those that restructure organizations to enable closer interaction and coordination and those that provide authority to the IC to acquire information from intelligence sources[8]. Because of their sensitive and classified nature, many policies are not accessible; however, the next paragraphs mention policies that were enacted due to real or perceived intelligence failures and the need to clarify IC operations. The intelligence areas served by the evolution of the policies listed below include efforts by the Bush and Obama Administrations to better organize the intelligence effort by placing intelligence organizations under control of an agency director. The policies evolved to better clarify how criminal and civil investigations can be conducted with greater specificity, so as to protect the privacy and constitutional rights of citizens, both within the U.S., and while abroad. The evolution involves fluid and adaptive efforts, some caused by complaints and arguments presented publicly and directly to oversight and accountability agencies and committees whose responsibilities include seeking legal and civil remedies. The evolution of intelligence policy can be viewed through the following:

- Executive Orders (served to reorganize the IC and specify new responsibilities of the DNI);
- The Intelligence and Terrorism Prevention Act of 2004 (represented reform of better directing the IC);
- USA PATRIOT Act Improvement & Reauthorization Act of 2005 (subsequent 2009; 2011);
- FISA Amendment Act of 2008; and
- FISA Amendment Reauthorization Act of 2012.

Executive Orders

In 2004, President George W. Bush issued Executive Orders 13355 and 13470 creating a National Counterterrorism Center and providing the Director of Central Intelligence with additional budgetary and managerial authority over the 15-member intelligence community. In 2009, President Barack Obama issued Executive Order 13516 strengthening the Intelligence Oversight Board, to report suspected violations of federal law related to intelligence gathering to the U.S. Attorney General (including to the President, to the Director of National Intelligence

[8] Intelligence sources can be people, documents, equipment, or technical sensors, grouped according to major intelligence discipline: geospatial intelligence (GEOINT); human intelligence (HUMINT); signals intelligence (SIGINT); measurement and signature intelligence (MASINT); open-source intelligence (OSINT); technical intelligence (TECHINT); and counterintelligence (CI)" (*Joint Intelligence*. I-5). For additional information, please also see https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/work-of-the-cia.html and http://www.fas.org/irp/nsa/ioss/threat96/part02.htm).

(DNI), and the agency at which the infraction occurred)[9]. President Obama also issued Executive Order 13587, Structural Reforms to Improve the Security of Classified networks and the Responsible Sharing and Safeguarding of Classified Information[10]. In essence, this legislation served to seek a continuation in the sharing of information between member agencies of the IC, and advanced the efforts of the USA Patriot Act and the IRTPA.

The Intelligence and Terrorism Prevention Act of 2004 (December 17, 2004)

The Director of National Intelligence (DNI) became separate from the CIA director and gained authority to lead the IC, serving as the president's principal intelligence advisor. The Act held the DNI accountable for its performance, for determining the intelligence budget, and for submitting proposals to the president for intelligence improvements (Lederman, 2009). The DNI gained authority to transfer up to $150 million from any agency per fiscal year to meet emerging threats (p. 87). The Act created the National Counterterrorism Center and authorized the DNI to create National Intelligence Centers (p. 89).

USA PATRIOT Act Improvement and Reauthorization Act of 2005 (Reauthorized in 2009; 2011). This Act originated from acknowledged intelligence failures attributed to the attacks on 9/11, although the recommendations from the 9/11 Commission was the IRPTA. This reauthorization allows investigators to continue to use vital investigative processes and tactics, to help law enforcement and intelligence agencies protect the nation by destroying the FISA "wall" that prevented effective information sharing between law enforcement and intelligence personnel; and providing national security investigators the tools comparable to those commonly used in criminal cases. The Act updated investigative tools to reflect new technologies and threats, and allowed authorities to obtain search warrants from a single court regardless of where terrorist-related activity occurred. The Reauthorization added dozens of additional safeguards to protect privacy interests and civil liberties (retrieved from www.justice.gov/911/legal.html).

FISA Amendment Act of 2008. The Foreign Intelligence Surveillance Act (FISA) allowed intelligence professionals to more quickly and effectively monitor terrorist communications, while protecting the civil liberties of Americans. It ensured that the intelligence community had tools to determine who terrorists are communicating with, what they are saying and what they may be planning. It provided critical authorities to allow the IC to acquire foreign intelligence information by targeting foreign persons believed to be outside the U.S. It required court orders to target Americans for foreign intelligence surveillance, no matter where they are, and required court review of the procedures used to protect information about Americans. It also provided

[9] The Office of the DNI was established subsequent to the IRTPA, and replaced the DCI following reform of intelligence.

[10] The policy states that national security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management. Therefore, the intent of the order is to direct structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties.

liability protection for companies who help protect the country from terrorism (retrieved from www.justice.gove/911/legal.html).

Reauthorization of FISA Amendments Act (2012). This reauthorization extended Title VII of FISA until December 31, 2017, allowing the statutory framework by which government agencies may, when gathering foreign intelligence information, obtain authorization to conduct wiretapping, or physical searches, utilize pen registers and trap and trace devices, or access specified business records and other tangible things. It provided authorization to obtain court orders from the Foreign Intelligence Surveillance Court (FISC), a specialized court acting as a neutral judicial decision maker (Liu, 2013, p. 2).

The USA PATRIOT ACT Improvement and Reauthorization Act. The Act was reauthorized to improve counter-terrorism efforts in several ways: Use of investigative tools previously used to investigate organized crime and drug trafficking (e.g. surveillance, following suspected terrorists in foreign countries, use of techniques precluding notifications to suspects, and rules for more easily obtaining court orders for business records in national security terrorism cases). The Act facilitates information sharing among agencies, updates the law to reflect the use of new technologies (e.g. victims to hacking incidents may request police assistance), and increased penalties for terrorist crimes. The Act prohibits harboring of terrorists, creates penalties for conspiracy cases, extends statutes of limitations for certain crimes, and punishes bioterrorists and attacks on transit systems.

Intelligence Failures as Driving Legislative Policy Changes

Boston Marathon Bombing. Brothers Dzhakor and Tamerlan Tsarnaev, also University of Massachusetts at Dartmouth students, detonated two improvised explosive devices near the finish line of the Boston Marathon on April 15, 2013. The bombs killed three persons, injured 264 others, and caused a significant amount of damage to real and personal property (*U.S. v. Dzhakor Tsarnaev*, case 113 mj 0-2106 MBB, filed by FBI Special Agent Daniel R. Genck, April 21, 2013, http://www.justice.gov/iso/opa/resources/363201342213441988148.pdf). The low grade explosives contained nails and BBs inside pressure cookers. In his testimony before the House Homeland Security Committee, Boston Police Commissioner Edward Davis stated that "his department had been unaware that the Russian government contacted the FBI in 2011 to warn of Tamerlan Tsarnaev's radical jihadist sympathies and his plans to travel to the northern Caucasus and link up with Islamist separatist and terrorist elements from Dagestan and Chechnya. Nor had he been told, he said, that the FBI had questioned the elder Tsarnaev brother and his family, or that Tamerlan subsequently, in 2012, spent six months in the volatile region of southern Russia" (retrieved from http://www.globalresearch.ca/boston-bombing-suspects-fbi-homeland-security-withheld-information-from-local-state-police/5334671).

The FBI and the CIA acknowledged receiving the warnings from their counterparts in Moscow, and the follow-up probes of the brothers. However, since there was no "derogatory"

information, the case was closed. Nonetheless, Tamerlan Tsarnaev was placed on at least two anti-terror databases[11] .

Wikileaks. Army private Bradley Manning was charged with violating offenses under the Uniform Code of Military Justice, such as aiding the enemy, while a grand jury in Virginia was deciding whether to indict any civilians in connection with the disclosure[12]. "A number of other cases involving charges under the Espionage Act demonstrate the Obama Administration's relatively hardline policy with respect to the prosecution of persons suspected of leaking classified information to the media (Elsea, 2013, *Summary*). Private Manning was accused of containing the diplomatic cables onto a recordable CD and then leaking them to *WikiLeaks*. At the time, the State Department had a policy restricting the use of removable media such as USB drives and CDs. Following the breach, the agency updated that policy and reemphasized to employees a waiver process required for employees to use removable media for any purpose. New policies include auditing and monitoring tools to detect anomalous activity on the State Department's classified networks and systems (Hoover, 2012).

The Search for Osama bin Laden. For five years, Osama bin Laden resided undetected at his residence outside the Pakistan Military Academy in Abbottabad, Pakistan. He was killed during a covert U.S. Naval Special Warfare Development Group and CIA operation on May 2, 2011 (http://global-security-news.com/2011/05/15/osama-bin-laden-an-intelligence-failure-not-just-an-isi-failure-claims-isi-chief/). The Pakistani government later claimed it had supplied information to the U.S. that he was there; ironically, Pakistan had been labeled the "epicenter of terrorism" (Curtis, 2011). Early in 2009, after assuming presidency, Obama "directed CIA Director Leon Panetta to make the killing or capture of Bin Laden the top priority in the war against al-Qaeda. This begs the question, what had been the CIA's top priority until then? [and] how could he frustrate U.S. intelligence for so long?" (Bergmann, 2011)[13].

[11] Richard Falkenrath, former NYPD deputy commissioner for counterterrorism says that the Boston Marathon bombings offer lessons for future U.S. counterterrorism efforts and raises new questions about the suitability of intelligence operations because the intelligence community, and the FBI and CIA in particular, are reliant on more restricted domestic intelligence techniques than more permissive foreign intelligence-gathering techniques used by U.S. authorities focused abroad (retrieved from http://www.cfr.org/counterterrorism/domestic-intelligence-boston-bombings/p30557).

[12] For a thorough review of the issues, including First Amendment issues on the release of the information by Julian Assange, see Criminal Prohibitions of the Publication of Classified Defense Information (Elsea, 2013). WikiLeaks published classified defense documents. The documents were also reported by the *New York Times*, *The Guardian* (UK), *Der Spiegel* (Germany), and included later publication of conversations and interviews with representatives of Al-Jazeera. Other newspapers reporting U.S. covert or clandestine operations overseas called for appointment of a special prosecutor to investigate executive branch leaks.

[13] http://www.foreignpolicy.com/articles/2012/1/3/the_ten_biggest_american_intelligence_failures?page=0,6 Foreign Policy, The Ten Biggest American Intelligence Failures. Friedman (2012) identified issues such as lack of knowledge of culture, language barriers, "ignoring caveats and qualifiers," untimely assessment of satellite images, IC catering to preconceived notions of officials in the executive branch of government, policymaker "downplaying" the warnings, political infighting, scaling back intelligence gathering, underestimating or overestimating military strength to deter aggression, failing to anticipate the "intensity, coordination, and timing of the enemy attack" despite multiple warnings, IC withholding assessments pertinent to doubt on executive action (CIA and the Bay of Pigs); inadequate intelligence-sharing among government agencies, faulty U.S. assumptions about Japan's appetite for carrying out such a brazen attack, and rivalries within the U.S. intelligence community (Pearl Harbor).

This six-year failure to capture bin Laden while in Pakistan represents a myriad of problems. Some of the problems relate to the presence of intelligence gaps and lack of coordination, distrust or lack of diplomacy in the U.S. military forces and the CIA to gain authority to enter Pakistan to accomplish this mission. Related to this is the ability to collaborate with Pakistan on the capture of bin Laden. The implications include: Change to U.S. foreign policy on its relationship with Pakistan, better diplomatic relations, and encouraging stability in the nuclear-armed nation of 180 million people situated at the crossroads of the Middle East and South and Central Asia. If Pakistan's nuclear arsenal falls into terrorists hands, though remote, this would create monumental problems for the U.S. The U.S. needs intelligence officials there to track terrorists; NATO supply lines run through Pakistan to coalition troops in Afghanistan. Meanwhile, the U.S. provided over $6 billion in economic assistance to Pakistan over nine years, and about two-thirds of $20 billion in assistance to Pakistan since 2002 was for military aid for Pakistan's military operations against insurgents along the Afghanistan border (Curtis, 2011). A policy change believed to be related to harboring of bin Laden was the Obama Administration suspension of $500 billion in U.S. security assistance, scheduled as counterinsurgency (COIN) training and equipment (Kronstadt, 2012). This policy change maintains diplomacy and funding for some economic and civilian programs, while decreasing some fiscal support.

Benghazi Attacks and the ATFE Operation "Fast and Furious" Fiasco. The reports released by executive policymakers on these events indicate dishonesty. This author considers them "cover-ups," and categorically, intelligence failures. The U.S. Ambassador and three Americans were killed in the Embassy attack in Benghazi, Libya on September 11, 2012, and the talking points at news conferences emphasized a "spontaneous reaction to an anti-Islamic video sparked the attack" (Curry, 2012). (Although warnings were received, policy makers failed to take appropriate action; policymakers are a significant part of the intelligence process. (For example, for more information, please see http://www.intelligence.senate.gov/benghazi2014/benghazi.pdf.)

The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE) engaged in its largest firearms trafficking case involving the U.S.-Mexico border in 2009, and it was based in the Phoenix Field division. The plan allowed weapons to cross into Mexico through a *gunwalking* investigative technique designed to dismantle the U.S.-based gun trafficking network supplying firearms to the Sinaloa Cartel[14]. "From the beginning, the case was marred by missteps, poor judgments, and an inherently reckless strategy" (Joint Staff Report 2012). The investigation remained open despite the identification of the cartel members, duplicate information from DEA and the FBI, and knowledge of senior ATFE officials, including Director William Hoover. Not until numerous Mexican citizens and Border Patrol Agent Brian Terry were killed was a decision made to make arrests, seize evidence and contraband, and prosecute the case.

[14] In the ATFE initiative, Project Gunrunner, agents allowed licensed firearms dealers to illegally sell weapons meant for drug cartels and their leaders, hoping to capture them and seize the weapons under conditions favorable to the ATFE.

The above cases have implications for diplomacy and foreign policy, and likely led to changes in internal organizational policy to include better oversight and management, accurate news releases when public statements are to be made, and procedures to better protect covert operations and employees. These two cases raise issues of ethical, accountable, and moral behaviors and omissions that cost U.S. citizens their lives. They support the need for clear development of clear IC policies, as well as the need for continuous introspection and oversight. They both suggest failed intelligence and incompetence on multiple levels.

Discussion

Post 9/11 intelligence issues and challenges are deeply rooted in the changes in culture, context, and rationalities of the IC. The once-distant global threats are now at our front door, above and beneath us and in our own backyard. They involve collusion between and among those who want to hurt us, but they include home-grown sympathizers and supporters. The terrorist threats are more agile than ever, and are even more willing to die for their cause than we are willing to live for ours. The national threats include previously unseen relationships and associations such as transnational organized crime groups, international drug trafficking organizations, and foreign terrorist organizations. At the same time, nation-states and insurgencies are still potential threats[15]. They have access to weapons of mass destruction, and are limited only by their imaginations. Technology, improved human intelligence, organizational reform and reorganization, newly developed national security policy, diplomacy, and a better informed executive branch contribute well toward an effective intelligence community[16]. At the same time, the functioning and performance of the IC must be studied as potential "weaknesses in each step of the intelligence cycle, from planning and direction to collection, processing, analysis, and dissemination, as [t]he mobilization of U.S. intelligence against these new threats requires not only redirected resources toward increased human intelligence but also a realignment of attitudes within and among the intelligence bureaucracies" (Johnson, 2006, p. 116). However, despite these factors and dynamics, nothing can stop acts of nature or "lottery-type" luck, where unsuspected threats defeat or penetrate our effective security barriers and disrupt our lives.

Conclusion

The current IC has been effective in maintaining a healthy U.S. homeland and national security effort. However, threats have metastacised beyond Osama bin Laden, and now the

[15] The recent release of declassified intelligence reports includes reports on Russia, China, Iran, and other states that threaten U.S. interests. See USAF Counterproliferation Center report for more information.

[16] For an ethnographic study of the analytic culture within the U.S. intelligence community, please see Dr. Rob Johnston's (2005), Center for the Study of Intelligence (CSI), electronic textbook, available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf. "His findings constitute not just a strong indictment of the way American intelligence performs analysis, but also, and happily, a guide for how to do better" (Gregory F. Treverton, in Johnston (2005), *Forward*, p. xi). "CSI publishes Studies in Intelligence and books and monographs addressing historical, operational, doctrinal, and theoretical aspects of the intelligence profession. It also administers the CIA Museum and maintains the Agency's Historical Intelligence Collection" (p. ii).

security threats are more different than they have ever been. This change has led to equal or greater changes in IC policies, philosophies and perspectives. The asymmetry of the threats and the many new forms they take also require the reformation of the IC structure and function. We have seen significant changes to the IC involve greater efforts to integrate and share information, stronger and more specific verbiage within statutes to explicitly define allowable criminal and civil investigative techniques, and effort to preserve civil liberties. Challenges such as evolving strategies, funding and budgetary constraints, understanding the elusive, unseen, and anonymous actors, and better oversight and accountability remain. There is an understanding that the "rogue bureaucratic elephants beyond the public scrutiny or the control of elected officials and [lack of] unaccountability for intelligence failures" must reform (Ehlers, personal communication, March 2013). "**Harold Wilensky demonstrated that the intelligence function is hindered by hierarchy, centralization, and specialization**. Yet, precisely these characteristics are the essence of any government" (Betts, 2007, p. 26). The degree to which these issues and challenges lead to integration, flexibility, and competence will determine, in this author's opinion, the degree to which the intelligence community is successful in preserving our country and our civil liberties. In the words of the Commission of the Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction (2005), "we need an Intelligence Community that is truly integrated, far more imaginative and willing to run risks, open to a new generation of Americans, and receptive to new technologies" (Correspondence letter to President B. Obama, March 31, 2005, p. 2).

References

Betts, R. K. (2007). *Enemies of Intelligence: Knowledge and Power in American National Security*. Columbia University Press. Kindle Edition.

Budinger, Z. B. & Smith, J. H. (2011). *Ten Years After 9/11: A Status Report on Information Sharing.* Statements before the Senate Committee on Homeland Security and Governmental Affairs.

Clapper, J. R. (2011). How 9/11 transformed the intelligence community. *The Wall Street Journal.* Retrieved from http://online.wsj.com/article/SB10001424053111904537404576554430822300352.html.

Clapper, J.R. (2013). *Statement for the Record. Worldwide Threat Assessment of the U.S. Intelligence Community. Senate Select Committee on Intelligence.* Retrieved from http://www.intelligence.senate.gov/130312/clapper.pdf.

Curtis, L. (2011). After bin Laden: Bringing Change to Pakistan's Counterterrorism Policies." *The Heritage Foundation.* Retrieved from http://www.heritage.org/research/reports/2011/05/after-bin-laden-bringing-change-to-pakistan-counterterrorism-policies.

Curry, T. (2012). "Patraeus Thought at the Outset That Benghazi Attack Was Terrorist Act." *NBC Politics.* Retrieved from http://nbcpolitics.nbcnews.com/_news/2012/11/16/15216937-petraeus-thought-at-the-outset-that-benghazi-attack-was-terrorist-act?lite.

Elsea, J. K. (2013). *Criminal Prohibitions on the Publication of Classified Defense Information.* Congressional Research Service. CRS Report for Congress.

Gates, Robert M. 2007. London Lecture, Kansas State University. U.S. Department of Defense.

Johnson, L. K. (2006). A framework for strengthening U.S. Intelligence. *Yale Journal of International Affairs.* Spring 2006, 116-131. Retrieved from http://yalejournal.org/wp-content/uploads/2011/01/061210johnson.pdf.

Johnston, R. (2005). *Analytic Culture Within the U.S. Intelligence Community: An Ethnographic Study*. The Center for the Study of Intelligence. Government Printing Office. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf.

Joint Staff Report to the U.S. Congress. 2012. *Part I of III: Fast and Furious: The Anatomy of a Failed Operation*. Report to the Committee on Oversight and Government Reform and Committee on the Judiciary.

Liu, E. C. (2013). *Reauthorization of the FISA Amendments Act.* Congressional Research Service. January 2.CRS Report for Congress.

Hoover, N. J. (2012). "State Department CIO: What's Changed Since Wikileaks." *Information Week Government.* Retrieved from http://www.informationweek.com/government/security/state-department-cio-whats-changed-since/232800365.

Kronstadt, A. K. (2012). *Pakistan-U.S. Relations*. Congressional Research Service. Report to Congress.

McElhatton, J. (2011). 9/11 Privacy Board Fails to Meet: Never Filled by Bush or Obama. *The Washington Times.*

National Security Strategy. (2010.) Washington, White House.

The Commission on the Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction: Report to the President of the United States. Retrieved from http://www.nytimes.com/packages/pdf/politics/20050331_wmd_report.pdf

The White House. Executive Order 13587. (2005). *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.*

Trujillo, M., D. (2012). Are Intelligence Failures Inevitable? *E-International Relations,* Retrieved from http://e_ir.info/2012/11/08/are-intelligence-failures-inevitable.

U.S. Department of Justice. *Structural Changes to Enhance Counter-Terrorism Efforts.* Retrieved from http://www.justice.gov/911/counterterrorism.html.

U.S. Congressional Subcommittee on National Security. 2006. *Emerging Threats, and International Relations of the Committee on Government Reform*. House of Representatives, 109th Congress, 2nd session.

Zegart, A. (2005). September 11 and the Adaptation Failure of U.S. Intelligence Agencies. *International Security*, 78-111.

APPENDIX A

Matrix of Issues and Challenges Involving Intelligence

Concerns for the Intelligence Community: How to Enhance Current Capabilities	
Issues	Challenges
Executive level clarity on U.S. policy, strategy and vision	1. Diplomacy; "soft" or "hard" approach; In-between? 2. Identifying and clarifying the specific threats 3. Defense planning 4. Relationships (Domestic, Foreign, National)
Funding of all initiatives and the infrastructure for intelligence	1. Defense appropriations (budgetary constraints) 2. Federal agency support 3. Civilian law enforcement
Technical and technological equipment, training, and methods for management of data and information	1. Hardware (weapons, computers, programs, etc.) 2. Software 3. Databases and access (clearances, MOUs)
Criminal and civil sanctions for national security breaches	1. Rule of law 2. Standards of proof 3. Efforts to stop organized attacks/threats
Mediating the tensions that exist between security needs and civil liberties inherent in a democracy	1. Communications and privacy rights 2. Searches and seizures 3. Immigration
Increased and effective/efficient partnerships, collaborations, and coordinated efforts	1. Language and culture barriers 2. Joint intelligence analysis 3. Organizational support
A better understanding of the intelligence process	1. Intelligence failures 2. Agent - analyst - policy maker relationships 3. Reform and responsiveness
Reform and responsiveness of structure and function of the intelligence community	1. Complex/bureaucratic organizations resist change 2. Executive and legislative mandates 3. Judicial decisions
Personnel and performance issues	1. Micro level (mirror-imaging, communication, paradoxes, etc. 2. Meso level (agency specific) 3. Macro level (DoD, DNI, CIA, etc.)
Concern for the "theory" of intelligence (imperfections and predictabilitly of social phenomenon)	1. Lessons in hindsight do not guarantee improvements in foresight 2. Overcoming theoretical presumptions and assumptions 3. Eliminating paradoxes