International Studies Journal (ISJ)
Vol. 16, No. 3 (63), Winter 2020
Received Date: 29 nevember 2019
Accept Date: 28 Desember 2019
PP: 87-126

Never Again? Learning from September 11 to Improve Tomorrow's Strategic Intelligence[*]

Jenny K. Wright, MSc[**]

Abstract

The aim of this paper is to determine whether the most critical lessons learned from the terrorist attacks against the U.S. on September 11, 2001 have been applied in practice to improve the efficiency of the government institutions entrusted with counterterrorism. The scope of the research is limited to the study of the strategic intelligence capabilities of the U.S. intelligence community (IC) and its role in combating terrorism.

This paper used the systems concept of cross-organizational isomorphism to support the argument that the lessons learned from the individual intelligence organizations within the IC can be applied community-wide through a process of active learning. Furthermore, it argues that sufficient application of these lessons can assist the development of active foresight, i.e. a proactive process through which early warning signs can be identified, actionable intelligence

[*] Dissertation approved for degree of MSc Risk, Crisis and Disaster Management, Department of Civil Safety & Security, University of Leicester, Leicester, United Kingdom. Dissertation Supervisor/Mentor: Dr. Todd R. Higgins (trh6@le.ac.uk)

[**] She is the CEO and Founder of 360 Research & Consulting, and has consulted and conducted research on behalf of various public, private and nonprofit actors including the U.S. Government, Government of Sweden and the International Organization for Migration (IOM) (U.N. Migration). She is the author of Migration in Timor-Leste: A Country Profile 2019, due to be released later this year. She has an MSc from the University of Leicester as well as a BSc and BSS from Mid Sweden University, and is currently completing an LLM at Euclid University. / Email: jwright@360-consultants.com

derived, and potential terror plots thwarted.

A case study was conducted involving a series of consultations with experienced intelligence professionals to discuss systematic failures, paradigm shifts, and organizational improvements since these terrorist attacks. Finally, this paper concludes that while the IC learned significant lessons from the 9/11 attacks, more reforms and resources are needed to maintain the momentum and prevent another major terrorist attack against the U.S.

Keywords

Intelligence; Terrorism; National Security; Homeland Security; Government; Risk Management; Security

Introduction

"In our ever-changing world, America's first line of defense is timely, accurate intelligence that is shared, integrated, analyzed and acted upon quickly and effectively" (President Obama cited in Bellantoni, 2010). Dr. Walter G. Sharp Sr., a Senior Associate Deputy General Counsel for Intelligence at the Department of Defense (DoD), further stated that strengthening the intelligence community (IC) is one of the greatest imperatives of the U.S. Hence, this paper aims to contribute to the intelligence reform debate on how to improve U.S. strategic intelligence capabilities through a process of active learning from the lessons learned from one of the most infamous terrorist attacks and "intelligence failures" in modern history – the hijackings of four commercial airliners by 19 al-Qaeda operatives on September 11, 2001 (hereafter 9/11).

Research Objective and Questions

"Never again" became a common catchphrase following 9/11. However, there were a series of early warning signs – particularly the 1983 Marine barracks bombing in Lebanon, the 1993 attack on the World Trade Center (WTC) in

New York, and the 1995 Bojinka-plot in the Philippines – that could have been recognized and acted upon, if active learning had occurred sooner. The 9/11 attacks are a well-researched case study but emphasis is frequently placed on blame allocation rather than opportunities for organizational development. This paper focuses on how to improve U.S. strategic intelligence capabilities to more efficiently combat terrorism by applying the lessons learned from 9/11. The scope of the research is demarcated by the following research questions:

- What were the most important lessons learned by the IC from 9/11 in terms of strategic intelligence needs in the War on Terror?
- Has the IC sufficiently applied these lessons to improve its capabilities to avert another major terrorist attack on American soil?

This paper aims to contribute to existing literature by guiding the discourse past the intelligence failure of 9/11 and direct it towards the future. It includes an empirical case study of the lessons learned by the IC, which were derived from consultations with almost fifty experienced intelligence professionals. This paper discusses the strategic intelligence reforms implemented to combat the emerging trends within assymetrical warfare and terrorism in the twenty-first century. Opportunities for further active learning from 9/11 will be discussed as well as the possibility to develop so-called "active foresight" and a culture of proactivity rather than reactivity. Lastly, this paper includes a series of recommendations on how to practically improve tomorrow's strategic intelligence in the War on Terror by promoting active learning across the IC.

METHODS OF RESEARCH

The case study was conducted in three stages: *systematic review, survey,* and *data analysis*. A mixture of research methods was applied to improve the accuracy of the findings, including both qualitative and quantitative elements in the data analysis as well as the phenomenological methods (case study) and

positivistic methods (survey). The research consisted of a survey-based formative evaluation. This mixture of quantitative and qualitative methods aims to evaluate the effectiveness of different reforms and was deemed most appropriate as the aim of this paper is to derive recommendations from the survey findings.

A *systematic review* was conducted to identify and synthesize relevant existing literature, in accordance with guidelines by Hart (1999) and Green (2009):

- Searched the *Homeland Security Digital Library*, CIA:s Center *for the* Study *of* Intelligence as well as existing bibliographic databases, e.g. *Social Science Citation Index*, for relevant published works;
- Pursued additional sources found in the bibliographies of identified sources;
- Searched official government websites and defense colleges, etc. for publications and recommended readings;
- Requested unpublished/published work from government agencies as well as selected scholars and institutions; and
- Searched relevant journals and library collections, including Cambridge University Library, for specialist reports and identified publications excluded from electronic sources.

Ultimately, this method generated large amounts of sources and required an extensive screening process. Strict exclusion criteria were applied to eliminate impractical, poor-quality studies. Particular emphasis was put on excluding authors with limited professional experience within the IC. The selection of sources was greatly aided by referrals from key informants (hereafter "informants") participating in the survey. A small number of additional sources were included due to their unique experience and/or opinions in order to obtain a more balanced account of events.

As factual surveys are often criticized for describing "what" but not explaining "why" (Coleman and Moynihan, 1996), the second stage comprised of an empirical observation with a hybrid *survey* combining ten consultations, ten electronic questionnaires, and 33 semi-structured interviews. The first part consisted of consultations, or "exploratory interviews," with a wide-ranging group of subject-matter experts to assess and refine the research problem. The first survey instrument consisted of a structured self-completion questionnaire using an "inverted funnel sequence," i.e. the questions began broadly and gradually narrowed (Nachmias and Nachmias, 1976: 106). Prior to distribution, a pilot test was conducted to identify deficiencies in the design and prevent the collection of inaccurate data. The test pilots were selected from the consultations previously conducted as part of a follow-up session. The feedback was used to revise the first survey instrument, which was administered in written form and distributed among ten of the total 43 informants. While accessing the informants was challenging, and the limited sample makes it difficult to generalize the results, the advantages were many, including obtaining in-depth and first-hand data from a particularly secretive community.

A survey instrument (or interview schedule) was developed for the semi-structured interviews. The interviews were conducted over the phone or face-to-face. Allowing the informants to select the time and setting for the interview was important to build rapport, encouraging candid responses. While face-to-face interviews increase the possibility of bias due to the "interviewer effect" (Fielding, 2009; Selltiz and Jahoda, 1962), they enable greater flexibility to adapt the structure as needed. The combination of research methods intended to ensure triangulation, i.e. enhancing the external validity of findings from one method by enforcing it with findings from additional methods, as well as the participation of experienced IC professionals aimed to limit the influence of

researcher bias on the results.

The aim of the survey was not generalizability but to elicit a deeper understanding of the case study. Hence, the informants were selected via purposive sampling and "handpicked" based on their number of years of professional experience within the IC and/or counterterrorism. The sample was divided into multiple groupings by sector (civilian or military), agency, general area of expertise (collection or analysis), and experience within the field. It was noted that an over-representation of one group might result in sampling bias. An equal balance of civilian and military intelligence professionals was targeted, as well as representation from across the IC. However, the restricted access to informants limited the size and representativeness of the sample. Thus, in order to prevent an "overgeneralization" that may threaten the external validity of the results, note that the responses provided for the purpose of this paper represent the views of the informants, and do not necessarily reflect the official policy or position of any U.S. government agency.

The third and final stage of the research – the *data analysis* – overlapped with the two prior stages in order to enable modification and improvements to the research design and survey instruments based on the results from the consultations and questionnaires.

The dependent variable (DV) in this study is the degree of active learning that has taken place within the IC in terms of strategic intelligence. The IC's ability to learn and improve its counterterrorism capabilities is affected by the following independent variables (IVs): *organizational culture*, *resources*, and *information management* (see Table 1). The possibility of a large variance is great since the independent variables are not necessarily dependent upon each other. They can all, however, make an important impact on the dependent variable. It should be noted that while terrorist organization may be unconventional institutions, they too have an organizational learning curve

(Nordell, 2011). The adaptability of terrorists to adjust their methods according to the counterterrorism efforts implemented might be a confounding variable.

Table 1: Independent Variables and Empirical Indicators

Organizational Culture	• System of thought (e.g. perceptions of the problem, appropriate solutions and best practices). • Willingness and ability to compromise, cooperate, interact, and share information within and between agencies within the IC and with foreign intelligence services.
Resources	• Funding. • Skills (e.g. languages) and training provided. • Collaborative technologies (e.g. databases, to enable sharing of information).
Information Management	• Methods, tools, infrastructure and process of collecting, analyzing and managing intelligence (intelligence cycle, intelligence disciplines, etc.).

Most of the questionnaire data was measured using a four-point ordinal scale for the purpose of validating the statistical tests. Certain variables were too complex to be accurately measured quantitatively and required a more qualitative method. As "sufficiently" and "effectiveness" are subjective terms, a *Discrete Likert Scale* (Likert, 1932) was used. The survey instrument consisted of pre-coded closed items, where the informants were provided with a set number of possible responses, but included ano*ther (please specify)*-category to cater for infrequent responses, but enable prompt data analysis.

The final data and content analysis of the interview transcripts as outlined by Knodel (1993) included application of strict exclusion criteria, limiting the data collated to that pertinent to the research questions, to ensure the validity of measurements and reliability of the data.

CASE STUDY

The modern IC was created at the beginning of the Cold War to prevent "another Pearl Harbor." "The fundamental intelligence failure of Pearl Harbor was that a dedicated and secretive enemy was able to exploit a blind spot in American defenses to achieve absolute tactical and strategic surprise. This is very similar to what al-Qaeda pulled off in 2001" (Sellers, 2011). The failure to prevent the Japanese surprise-attack on Pearl Harbor in 1941 was largely blamed on the poor coordination between agencies (Johnson, 2003: 643), but the inadequate border patrolling procedures and misplaced over-confidence were contributing factors. Regardless, to address this failure, the Truman administration established a unified DoD along with the Central Intelligence Agency (CIA), the National Security Agency (NSA) and the National Security Council under the *National Security Act of 1947* (Bamford, 2001; Warner, 1994) to "hub the wheel of U.S. intelligence" (Ranelagh, 1992: 37).

The predecessor of the today's Director of National Intelligence (DNI) evolved from the 1955 Congressional study that recommended that the Director of Central Intelligence (DCI) at the CIA should employ a deputy to manage the Agency, allowing the director to centrally coordinate the IC. As the DCIs lacked substantial fiscal powers, they were unable to manage the individual elements, or even their own agency, so they established inter-agency centers and temporary task forces to encourage cooperation across the IC. However, the Office of the DCI remained weak. According to former DCI Richard Helms (1966-1973): "Eighty-five percent of every intelligence dollar goes to the military intelligence agencies" (May, 1992: 66). The various agency directors tended to protect their "turf" from any intervention from the DCI and showed greater allegiance to their Cabinet Secretary than to the, in theory, central chief of intelligence (Johnson, 2003: 643).

The IC's overreliance on technical solutions and technical/ signal/

geospatial intelligence (TECHINT/SIGINT/GEOINT) dates back to the Carter administration in the late 1970s when American espionage activities were considerably downsized. Human intelligence (HUMINT) was perceived as intrusive on the target states and the political administration sought to avoid "dirty hands" (Herman, 2002: 385). Following the collapse of the Soviet Union and end of the Cold War, the IC suffered from a form of identity crisis combined with limited direction as from where the next threat would originate. A paradigm shift was needed, but would emerge too late (Andrew et al. 2009; Anderson and Poteat 2010).

System failures often appear "predictable only with the benefit of hindsight" (Elliott, 2002: 95). The WTC in New York suffered a previous terrorist attack in 1993, which presented opportunities for self-isomorphic learning in terms of evacuation and cross-organizational isomorphic learning in terms of improving inter-agency information-sharing. Yet the 9/11 attacks highlighted the devastating effects lost opportunities can have.

POST-9/11 DEVELOPMENTS

Following the 2001 attacks, American domestic policies re-focused on coordinating intelligence efforts, and the most visible results of U.S. foreign policy were the wars in Afghanistan and Iraq (Cole and Lobel, 2007: Kristol, 2005). The Bush administration's declaration of a global war on terror in the wake of 9/11 was criticized for, among other things, confusing a tactic with the enemy (Reveron and Stevenson Murer, 2006). The questions remain of how to fight a tactic and how to measure success (Levitsky, 2002). The War on Terror is nothing like the four major wars that the U.S. fought during the half century prior to 9/11: World War II, the Korean War, the Vietnam War and the Persian Gulf War (Levitsky, 2002). Additionally, the War on Terror requires a higher "intelligence-to-force ratio to identify the threat relative to the amount of force required to neutralize it" than was required during the Cold War, and a

conventional defense force is only sufficient when faced with a state-level threat (Reveron, 2006).

Post-9/11, it became evident that there was more than one failure within the IC and that the system itself was, thus, faulty (U.S. Congress, 2002; Steven and Gunaratna, 2004). The first failure of the IC was the "failure of imagination" (Davis et al., 2005: 25), by inaccurately interpreting the meaning of previous attacks (Schultz and Vogt, 2003: 21), both domestic (e.g. the first WTC-attack) and abroad (e.g. the Bojinka plot and the bombings of two U.S. embassies in Africa), as well as rejecting the possibility of a second attack on the WTC and "weaponizing" commercial aircrafts (Borch, 2003; White, 2002; Devine, 2009: 23). As one of the informants stated: "We should have learned long ago that the ocean can no longer protect us." Secondly, the IC lacked sufficient knowledge to track terrorist assets (Napoleoni and Carisch, 2005: 28; Roth et al., 2004: 13), particularly their use of the hawala[1] system to transfer funds (Haberfeld and von Hassell, 2009: 124), and this posed a challenge to "follow the money." Thirdly, while the threat level of al-Qaeda launching a large-scale terrorist attack against the U.S. was well-known by 1999 (Wright, 2006), the limited synergistic cooperation due to so-called "home-rule" rivalries was the greatest weakness of the IC (Bruneau, 2007; Storbeck, 2005). As Keegan (2004: 385) remarked: "No rivalries are more intense than those between intelligence services working, by different means, on the same side." Those rivalries have been identified as the main cause behind poor planning and duplication of efforts (Haberfeld and von Hassell, 2009: 136). The IC did not coordinate their "watchlists" of terror suspects, nor did they share information of known al-Qaeda associates and their sudden interest in aviation (Gladwell, 2003;

[1] *Hawala* is an ancient trust-based, informal money transfer system similar to the Western Union, but there are no records of the transactions (Perkel, 2004). This poses a significant challenge when tracking terrorist finances.

National Commission on Terrorism, 2002: 147). Fourthly, with the exception of CIA's *Operation Redbook,* which was terminated in the late 1990s, "no government agency would systematically analyze terrorists' travel patterns until after 9/11, thus missing critical opportunities to disrupt their plans" (Eldridge et al., 2004, preface). Fifthly, according to the DoD, the lack of investment in HUMINT and analytical expertise directly resulted in the failure to identify the terrorist cell behind the attacks by "connecting the dots" between seemingly benign activities and the terrorist threat potential prior to 9/11 (Jones, 2002). Finally, the post-9/11 top-down pressures on analysts to find supporting intelligence to rationalize military action, e.g. "discovering" weapons of mass destruction (WMDs) in Iraq (Reid, 2003), is of grave concern and threatens the legitimacy and integrity of the IC.

Countless congressional investigations, conferences and publications as well as the 9/11 Commission Report identified a myriad of lessons to be learned by the IC and recommendations for institutional reforms, mainly in terms of improving information-sharing within the IC, following the attacks (National Commission on Terrorist Attacks Upon the United States, 2002; Reveron, 2006). Intense negotiations to reconcile the differences over proposed changes to the *National Security Act of 1947*, resulted in the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) (AFIO, 2011b). Today, the IC comprises of 17 organizations, or *elements*, and one central coordinating entity, the Office of the Director of National Intelligence (ODNI), which was created as a result of IRTPA and the DCI subsequently lost its Cabinet rank (AFIO, 2011a; DNI, 2011a). However, much of the power and influence of U.S. strategic intelligence belongs to the Secretary of Defense (SecDef), who not only controls the intelligence budget but the majority of the intelligence agencies. Most IC elements have dual management lines extending to both the SecDef and DCI – and, since 2004, the ODNI. The CIA is an independent

agency and the remaining elements are located within policy departments, e.g. Department of Justice, etc. (Johnson, 2003: 642). There are three IC elements responsible for strategic intelligence: the CIA, the Defense Intelligence Agency (DIA), and the Bureau of Intelligence and Research (INR) (Informant 31).

Under the *Homeland Security Act of 2002,* the recently established Department of Homeland Security (DHS) was tasked with the coordination of national security-related communications between all levels of government (federal, state, local and tribal), private sector, and the public. To achieve this mandate, DHS implemented the *Homeland Security Information Network* (HSIN). However, it has not been used to its full potential as users resort back to pre-9/11 communication means, i.e. related systems and telephone calls to share information, which "only perpetuates the ad hoc, stove-piped information-sharing environment that HSIN was intended to replace. Resources, legislative constraints, privacy, and cultural challenges – often beyond the control of HSIN program management – also pose obstacles to HSIN's success" (DHS, 2006: 3-4).

Shelfer and Verner (2002: 56) advocated for merging military and civilian lessons-learned databases to extract new insights. They highlighted that while there are several lessons-learned databases with experiential knowledge, these lessons are often not applied to promote active learning across the IC and, thus, these integrated information systems do not reach their full potential. In fact, these databases could be used more proactively to identify and enable decision-makers to avoid mistakes that might cause devastating chain reactions. A decade after 9/11, Builta and Heller (2011) argued there is still a need to institutionalize the positive changes made as well as best practices. During the 111th Congress of the Select Committee on Intelligence, they commended the CIA for establishing its *Lessons Learned Program*. The Committee emphasized the need for the IC to institutionalize the lessons learned process and develop a

common policy supporting that effort. They recommended that the IC should create web-based lesson-sharing environments, encourage more research within the area of active learning, and support a modernization of its oral history programs as well as component-based lessons learned-activities throughout the IC (Select Committee on Intelligence, 2011: 30).

During the decade following 9/11, the U.S. funded more than 80 new collaborative technologies and initiatives aimed at improving inter-agency cooperation and information-sharing through the ODNI's Rapid Technology Transition Initiative (RTTI). The IC has developed infrastructure to integrate threat information and improved community-wide database searching capabilities as well as the development of a *CT Data Layer* that aids analysts' in finding links between known and potential terrorists (DNI, 2011b). Nevertheless, following the averted "Christmas Day Bomber" in 2009, it became evident that the multiple "no-fly lists" and watchlists had still not been consolidated (Schmitt and Lipton, 2009). This vulnerability has been addressed with additional resources dedicated to enhance watch-listing criteria. Subsequent successes include the prompt disruption of the national security threat posed by alleged extremists including Najibullah Zazi, David Headley, and Abdulhakim Mujahid Muhammad – along with the fusion of domestic and foreign intelligence enabling a more collective intelligence cycle. To ensure the collection of actionable intelligence and eliminate duplication of efforts, the ODNI has created the community-wide senior *Intelligence Community Executive Committee* (EXCOM). In addition, the ODNI established an analytic *Pursuit Group* within the NCTC to focus exclusively on discovering threats aimed at the U.S. and American interests (DNI, 2011b).

Reveron (2006: 1), an associate professor at the Naval War College and long-time intelligence analyst, argued that critical intelligence can be obtained by improving bilateral information-sharing with foreign intelligence agencies.

Kaplan (2011) cautioned, however, that it is counter-productive to put equal value on maintaining personal relationships and allegiances with despotic regimes such as Saudi Arabia while combating terrorism. Following 9/11, the U.S. maximized its use of foreign intelligence relationships both for defensive and offensive purposes (Lefebvre, 2004: 529). There are as many ways to share intelligence as there are intelligence services around the world. For instance, the U.S. (patron) can identify a foreign intelligence agency (client) with comparative advantages, e.g. access to targets, and offer them training or support in exchange for language translation or other services rendered. This is often referred to as a strategic *cliency-patron relationship* (Tétreault, 1991). Alternatively, a foreign country can allow the U.S. to use its territory to collect intelligence in return for sharing that information. The U.S. might even opt to combine intelligence collection or other operations with a foreign intelligence agency (Reveron, 2006). For instance, the U.S. increased its intelligence support to neighboring Mexico to aid collaborative efforts, particularly in regards to border security (DNI, 2011b).

According to Jack Devine (2009: 17), a career CIA clandestine services officer who also served as the acting Deputy Director of Operations, the future IC should consist of consolidated elements centralized under an appointed *Secretary of Intelligence* (SecInt), i.e. a Cabinet-level authority. Tomorrow's IC will, according to Devine, be somewhat free of bureaucracy, turf wars, and political restraints. It will, thus, be better equipped to protect U.S. interests. While there is resistance, particularly from the military, to placing all elements (including the FBI's intelligence division) under civilian control, Devine argued that "a powerful [SecInt] will be needed to provide leadership and authority of the new entity," a *Department of Intelligence* that is separate from the DoD (Devine, 2009: 23). Additionally, it is important, according to Bobbitt (2008: 289), "to solve the problem of how to develop rules that will effectively

empower the secret state that protects without compromising our commitment to the rule of law."

Paul Pillar (2002: 26), the National Intelligence Officer for the near East and South Asia and former Deputy Chief of the Counterterrorism Center at the CIA, cautioned: "If history is a guide, even the current enthusiasm for counterterrorism, great though it is because of the enormity of what happened in September [2001], will slacken over time." While enormous resources were initially poured into expanding intelligence and counterterrorism efforts, interest has already subsided. DoD is downsizing and the ODNI announced (a decade after 9/11) that the intelligence budget will be reduced over the following decade with "cuts in the double-digit range" (DNI James R. Clapper cited in Iannotta, 2011). Informant 43 warned: "The reduced budgets mean we need to be able to do more with less."

SURVEY FINDINGS

A large majority (70%) of the informants believe the IC has learned the lessons from 9/11, but a third of them added that there is more to be done. In comparison, 30% do not believe any lessons have been learned at all. Overall, more than half of all informants believe the IC has not sufficiently applied the lessons learned to improve its capabilities to avert another major terrorist attack on the U.S. One of the informants even added: "Unfortunately, I fear it will take another 9/11 for the most important lessons to be learned."

One of the lessons presented in the 9/11 Commission Report was the "failure of imagination" (National Commission on Terrorist Attacks Upon the United States, 2002). According to 17% of informants, the most important lesson learned from 9/11 was that the system of thought at the time was insufficient to assess, forecast or even imagine the potential threat of 19 hijackers turning four airliners into guided missiles (see Table 2). It became evident that both civilian and military elements as well as domestic and foreign

agencies must collaborate to combat contemporary terrorism. In fact, the majority of informants agree that the most important lesson learned by the IC from 9/11 was what devastating effects could be caused by the lack of inter-agency cooperation and information-sharing. Rustmann (2012) stated that while progress has been made, there are still fundamental obstacles in terms of organizational culture. "The CIA cannot be part of the FBI's 'trail of evidence' as they cannot be called to testify." In addition, the main objectives of the FBI are arrests and convictions, as that is how their employees are promoted. CIA agents, on the other hand, get promoted based on number and usefulness of the sources they recruit. Acting upon certain information can compromise a source's cover, which is why the CIA often is reluctant to share information with the FBI, as they are "more interested in a trial than the bigger picture" (Rustmann 2012).

Table 2: Lessons Learned

Insufficient interagency cooperation	25	20%
Underestimated the threat of terrorism	22	18%
Need to be proactive rather than reactive	18	15%
Insufficient system of thought	17	13%
Need to prioritize security	13	10%
Insufficient intra-agency cooperation	7	6%
Need to train policymakers/decision-makers	6	5%
Overreliance on technical solutions	5	4%
Pre-9/11 legislation/policy obsolete	4	3%
Insufficient domestic intelligence collection	4	3%
Insufficient bilateral cooperation	2	2%
Need to engage public more	1	1%
TOTAL:	124	100%

A couple of the informants remarked that 9/11 made it evident that having separate agencies for managing domestic and foreign threats can be a

vulnerability – unless these agencies cooperate (Miceli, 2011; Ruth, 2012). Lisa M. Ruth (2012), a former intelligence analyst at the CIA, stated: "Our whole paradigm for intelligence was wrong. We thought we could categorize everything neatly in domestic and foreign threats." The FBI has come to this same realization and increased its counterterrorism activities domestically and extended its reach overseas; working comparatively closer with the CIA following 9/11. Furthermore, there is much less competition within the IC post-9/11 and less need for the individual elements to take credit in order to protect their "rice bowl," i.e. less risk of decreased funding due to poor results as the credit and accountability is spread across the IC (Poteat, 2012).

Seven percent of informants stated the lack of intra-agency cooperation was another important lesson learned. The failure to coordinate and share information is not limited to between but within elements and, according to two percent of informants, there was also insufficient cooperation with foreign intelligence services prior to 9/11. A handful of informants mentioned that cooperating with more partners – e.g. local law enforcement, places of worship and civil society – became a higher priority for the IC following 9/11. Several other informants stated; while agencies are coordinating much better, the "stove-pipes" that hampered the information flow prior to the attacks still exist. One of the informants emphasized the need to engage the public to be vigilant and realize that they too have a role to play in counterterrorism.

More than a fifth of the informants believed the threat of terrorism had been underestimated pre-9/11 and one of them stated there was a need to refocus existing targets, e.g. major sources (risk areas) of terrorism. As mentioned, targeting had been very diffuse, as a result of the bipolar Cold War-world changing and the hazard constructs within the IC were too wide-ranging to get a comprehensive view of from where the next threat would originate. According to four percent of informants, there was an inflated confidence and

reliance on "hard" intelligence sources (e.g. TECHINT, SIGINT and GEOINT) leading up to 9/11. While more "soft" intelligence sources (HUMINT) are, according to them, needed to determine target intentions. "Satellites leave black holes about our enemies' plans and intentions. These black holes can only be filled by HUMINT, i.e., spies, to get the complete picture" (Poteat, 2012). Most informants agreed that the lack of proper targeting and sufficient HUMINT collection efforts contributed to the intelligence failure that failed to prevent 9/11.

Eighteen percent of the informants stated that after 9/11 the IC recognized the need to be proactive rather than reactive. Collectors must approach more potential sources. Analysts must promptly assess threats, produce actionable intelligence and disseminate it to the consumers (decision-makers). The consumer must then make a decision based on all available intelligence, e.g. elevate the threat level. Five percent of informants argued that 9/11 was evidence of the need to train the consumer in the role of intelligence, including its benefits and limitations. It is not the responsibility of the IC to make policy decisions, but to provide as much timely, accurate and above all actionable intelligence to ensure the consumer can make informed decisions.

When asked whether the IC has sufficiently improved its counterterrorism capabilities to prevent a terrorist attack of similar magnitude, 56% of the informants believe that the IC has but only to a limited degree, while 35% believe they have to a large degree. The remaining 8% believe that the IC has not sufficiently improved its counterterrorism capabilities. Several of the informants referenced to the fact that there has not been a successful terrorist attack since 9/11, as evidence that the lessons have been learned.

The informants were asked what the most significant differences are between U.S. strategic intelligence before compared to after 9/11 (see Table 3). The majority (22%) indicated that cooperation within and between agencies

increased as well as with relevant partners, and 17% stated that information-sharing improved between and within agencies. Two percent mentioned that rotational assignments have considerably increased during this past decade thanks to orders from the ODNI. "The IC community now works as a team on collection and targeting of terrorists targets since 9/11. New methods, technology, and rotational assignments between personnel of different agencies are greater now than ever before" (Informant 13). However, many common information management systems (databases) and other collaborative technology lack adequate functions to delegate or clarify who is in charge of what pieces of intelligence. While, in theory, this is already possible, it does not appear to function properly according to local and state-level collectors and analysts. It is unclear where the entered information goes and whether it is acted upon (Informant 29). Accountability and follow-through continue to be obstacles.

Table 3: Pre-9/**11 versus Post-9/11 Strategic Intelligence**

Increased cooperation between intelligence agencies	22	22%
Creation of new elements within the IC	18	18%
Improved information-sharing	17	17%
Increased joint civil-military missions	11	11%
Improved system of thought	9	9%
More appropriate legislation and policies post-9/11	8	8%
IC drastically downsized pre-9/11, now additional resources	8	8%
Increased collection	3	3%
More rotational assignments within the IC post-9/11	2	2%
More proactive and dynamic post-9/11	2	2%
TOTAL:	100	100%

Eighteen percent of informants highlighted the creation of new IC elements – such as the ODNI, DHS and National Counterterrorism Center (NCTC) – as

systemic reforms derived from the lessons learned from 9/11. A quarter of these informants believe this merely added another layer of bureaucracy to an already over-bureaucratized system. "If building an effective agency was the intent – then one should have merged FBI, the Bureau for Alcohol, Tobacco, Firearms and Explosives (ATF) into DHS, away from the Department of Justice, so that DHS can become more proactive" (Marquise, 2012). According to Informant 1, a retired Technical Collection Officer at the CIA: the establishment of the ODNI and NCTC initially blurred the chain of command in tasking (operational direction) and made it more difficult to act quickly and decisively on actionable intelligence. "For example, there were short delays in implementing tactical actions while deciding who was in charge and the composition of teams. However, most of those difficulties have now been resolved." Furthermore, Informant 25 argued: "the National Security Council and National Security Advisor initially filled the void left by the DCI. However, their roles should now be eliminated as redundant, and a replacement structure manned by civilian contractors accountable only to the U.S. Congress should be established."

In contrast, a handful argued that the post-9/11 established "fusion centers"[1] have *de facto* helped integrate agencies and promoted a culture of cooperation. According to Informant 20, a retired Chief of Intelligence of the U.S. Coast Guard, the "fusion centers are the closest thing to what collaboration was meant to be. The IRTPA outlined this as a direction to follow."

Eight percent of the informants believe that 9/11 prompted more appropriate legislation and policies for the IC to combat terrorism. Immediately following the attacks, there was general support for the implementation of the *Patriot Act,*

[1] Fusion Centers are state-owned and operated offices that serve as focal points for collecting and sharing of threat-related information between government agencies as well as between public and private sector partners (DHS, 2019).

which granted the military and the IC extended powers, particularly in terms of data collection. This support is diminishing now that there has not been another major attack since 9/11 (Informant 25). "The *Patriot Act* revised the legal framework, which traded some loss off individual rights for increased security. The miscalculation of our risk of terrorism moved public opinion to rebalance the equation" (Miceli, 2011). Partially due to increased funding and elimination of legal barriers, among other things, FBI and CIA have increased their success rate exponentially in terms of disrupting terrorist plots and making prosecutions during this last decade (Poteat, 2011).

According to eight percent of the informants, after decades of downsizing, the IC was finally allocated additional resources. Half of them mentioned that a considerable amount of funding was invested in developing employees' language skills. Nine percent of the informants believe that the IC's system of thought improved due to 9/11 and that this has benefited greatly from the additional resources and training allocated to counterterrorism. In reference to this, 3% mentioned that intelligence collection has increased since 2001. Unfortunately, the downsizing appears to have resumed now that it has been a couple of decades since attacks.

Eleven percent stated the number of joint operations between the military and CIA – including the capture of al-Qaeda leader Osama bin Laden (Mazzetti, 2011) – but also other civilian agencies has increased since 9/11. The bond forged between the CIA and DoD in the wake of the attacks has been referred to as "intelligence integration," i.e. the improved communication and collaboration between intelligence and defense. This bond has strengthened and, according to Gene Poteat (2011: 3), former President of Association of Former Intelligence Officers (AFIO) and retired CIA executive, already resulted in "the most effective covert ops capability the world has seen." Even local law enforcement, New York Police Department (NYPD) in particular,

greatly improved their counterterrorism capability and averted several terror plots during the decade following the attacks (Poteat, 2012).

According to Stan Miller (2012), Chairman of the Tennessee Valley Chapter of the National Military Intelligence Association: "approximately 65-75 percent of civilian intelligence officers are former military". The survey found that there are still differences between civilian and military elements not only in terms of mandate but also in organizational culture. The informants were asked whether there are any significant differences between civilian and military strategic intelligence in terms of counterterrorism; 40% stated there are significant differences, 33% stated there are differences but only to a limited degree, and 27% did not believe there are any significant differences. The major differences highlighted by informants were: military intelligence focuses on local, tactical threats (33%) while civilian agencies have a more global, strategic focus (29%). Others stated that the military collects raw intelligence to be used to plan for war (14%), while civilian agencies collect intelligence to analyze a shorter-term threat (10%). Prior to 9/11, the DoD often accused the CIA of "not being on the same side of the hill" (Rustmann, 2012). Fourteen percent agree with the statement that civilian and military elements will never be able to fully cooperate, as the military defines terrorism as an act of war, while civilian agencies define it as a crime. The FBI, in particular, define terrorism as a crime and the objective is, therefore, to arrest and convict terrorists. From a military perspective, the objective is to defeat the enemy – the terrorists – by use of military means.

When asked specifically whether inter-agency cooperation and information-sharing has increased since 9/11, 47% of the informants believe it has but only to a limited degree, 37% responded it definitely has, and 16% believe that inter-agency cooperation had not increased to a level they would consider acceptable. A handful of them added that compartmentalization and

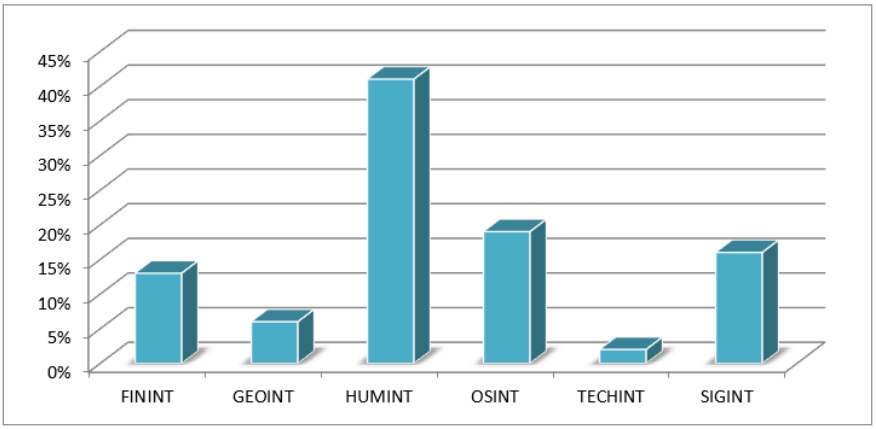
competition between agencies for funding are still major issues (Miceli, 2011). The "trusted networks" required as part of the 9/11 Commission Report have still not been developed (Informant 29). Even within agencies, employees are divided between departments constrained by the "need-to-know" principle, which makes it difficult to see the bigger picture. "Separate buildings, separate mind-sets" (Ruth, 2012).

When asked whether bilateral cooperation had increased between IC elements and foreign intelligence services, 40% answered that bilateral cooperation had increased significantly, more than half (53%) also answered that the cooperation had increased slightly, and seven percent did not believe there was any difference since 9/11. Most informants did, however, note that this increase mainly involves cooperation with existing allies, e.g. the U.K., and not necessarily expanding partnerships with other foreign intelligence services. For example, a few of the informants stated that there are prevalent trust issues between the IC and Chinese and Russian intelligence services. According to Konstantin Preobrazhensky (2011), a former senior member of the KGB (Soviet intelligence service): "Russians will never tell Americans the truth about anything. In Russia, terrorism is a good word – *subversion* – because the Russian Communist Party evolved from a terrorist organization (*Organ of Red Terror*). This is why the U.S. and Russia cannot combat terrorism together." Furthermore, many post-colonial governments are ruled by former liberation parties, i.e. formerly labeled as terrorists, and may thus sympathize with contemporary terrorist factions. Bilateral counterterrorism cooperation can, thus, require a delicate process of negotiations.

The informants were questioned if there was any intelligence discipline that the U.S. needs to improve to combat the current threat of terrorism. A considerably majority (41%) believe that HUMINT is severely lacking (see Figure 1), and the remaining informants indicated that all areas of intelligence

gathering require further improvements. It is crucial to collect what is needed, not only what is accessible (Ruth 2012). The informants indicated that the following categories need better direction on what and how to collect: open source intelligence (OSINT, 19%), SIGINT (19%), financial intelligence (FININT, 13%), GEOINT (6%), and TECHINT (2%).

Figure 1: Areas in Need of Improvement



The informants were asked if there was any stage of the intelligence cycle – planning (targeting), collection, analysis (processing) and dissemination – that was in need of further improvements (see Table 4). The survey found that the analysis stage was in greatest need of improvement and, other than the issue mentioned above in terms of collection, the planning stage only has minor needs for improvements. The collection and dissemination stages have some need for improvement, but were functioning overall. The problem is not lack of collection. In fact, many of the informants believe that the IC is collecting "too much" information. However, better targeting and more synthesizing is necessary. Analysts must know what intelligence is required and promptly disseminate it to consumers (Rustmann, 2012). Informant 27 added that it is still difficult to share the finished products with the consumer, especially executive-level management, without changing the message to fit the agenda.

Table 4: Areas in Need of Improvement

Stage of Intelligence Cycle	Individual Responses	Average	Attribute
Planning and Direction	2, 4, 4, 2, 2, 4, 4, 1, 1, 1, 2, 2, 2, 1, 2, 2, 2, 1, 1, 1, 1, 2, 2, 2, 1, 1, 4, 1	55/18=3	Little need
Collection	2, 4, 4, 1, 1, 2, 2, 4, 2, 2, 4, 4, 4, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 1, 1, 4, 1	39/16=2	Some need
Processing	1, 1, 1, 3, 3, 1, 1, 1, 2, 2, 1, 1, 1, 1, 1, 1, 2, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1	22/16=1	Greatest need
Analysis and Production	2, 4, 4, 2, 2, 2, 2, 1, 4, 4, 1, 1, 1, 1, 2, 2, 2, 1, 1, 1, 1, 2, 2, 3, 1, 1, 1	35/16=2	Some need
Dissemination	1, 2, 2, 2, 2, 2, 4, 2, 2, 2, 1, 2, 2, 2, 2, 2, 1, 1, 3, 3, 1, 1, 1, 1, 1, 1	27/13=2	Some need

As a concluding part of the survey, the informants were prompted to provide at least one practical recommendation on how to improve U.S. strategic intelligence to prevent future terrorist attacks. Their responses varied from reducing the bureaucracy to the creation of a Department of Intelligence with a separate budget (see Table 5). According to 8% of informants, there is still a need to develop a community-wide system of thought. Three informants added that the nature and scope of the threat must be clearly identified. Another responded that there has to be uniformity in every stage of the intelligence cycle that transcends across the IC. Ten percent of the informants recommended the appointment of Liaison Officers from each IC element to, at least, the CIA, FBI and NSA.

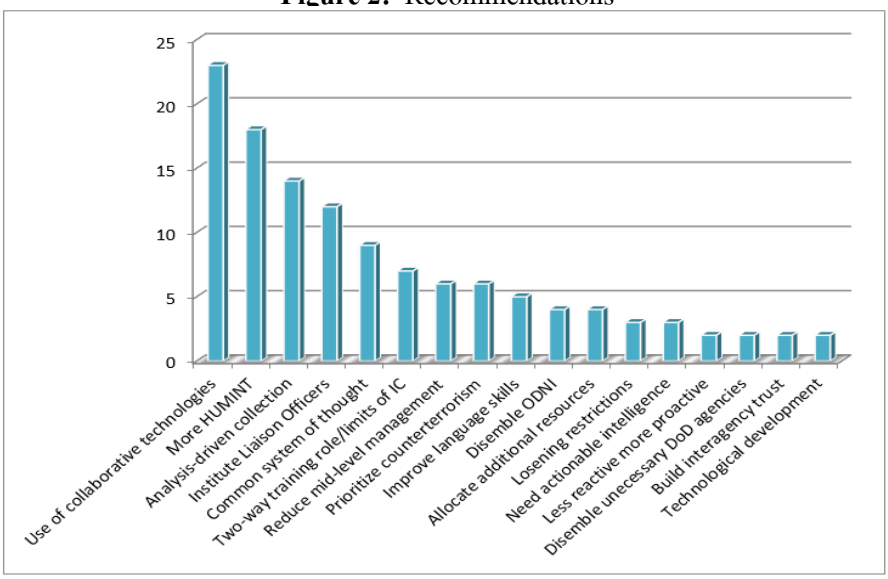
Table 5: Recommendations

Developing/increasing the use of collaborative technologies	23	20%
Less focus on technical collection, and more on HUMINT	18	16%
Need for analysis-driven collection	14	12%
Institute Liaison Officers in FBI, CIA and NSA from each IC element	12	10%
Further develop a common system of thought	9	8%
Two-way training to policymakers/decision-makers and analysts on the role and limits of intelligence services can/cannot provide	7	6%
Reduce middle level management	6	5%
Keep counterterrorism a priority	6	5%
Improve language skills within key defense languages	5	4%
Dissemble ODNI and reassign responsibilities to the DCI to include fiscal oversight over the DoD intelligence agencies	4	3%
Allocate additional resources to the IC	4	3%
Loosening restrictions	3	2%
Greater emphasis on actionable intelligence as military is down-sizing	3	2%
Less reactive more proactive	2	1%
Dissemble unnecessary DoD intelligence agencies	2	1%
Need to build interagency trust	2	1%
Continued input/emphasis on technological development	2	1%
TOTAL:	122	100%

A fifth of the informants recommended the development and/or increased use of collaborative technologies (see Figure 2). The new IC agencies have increased the risk of duplication. Hence, it is important to continue to improve inter-agency cooperation and information-sharing. Several informants recommended the continued development of cloud computing, where information is shared between civilian, military and law enforcement partners. A couple of the informants emphasized the need to build inter-agency trust. One of them added that too much is classified, which often excludes state and

local law enforcement from the information-sharing. More rotational assignments may contribute to strengthening partnerships and build trust across the IC.

Figure 2: Recommendations



Several informants warned that some IC elements continue to fail to collect, analyze and disseminate actionable intelligence in a timely manner. The value of intelligence is directly correlated with the speed it can be processed and shared with decision-makers (Informant 22). According to 16% of informants, focus should be transferred from technical (GEOINT, SIGINT, and TECHINT) to increased HUMINT collection. Furthermore, 2% of informants recommended loosening the legal restrictions placed on the IC, especially in terms of prohibiting the recruitment of sources with a criminal record, as this poses a significant challenge in terms of recruiting valuable sources inside terror cells. Twelve percent of informants, many of whom were collectors themselves, emphasized the need for analysis-driven collection to ensure

collectors are clear on consumer needs. Four percent of informants recommended additional training for collectors and analysts, particularly in developing important language skills like Arabic, Farsi and Mandarin. Informant 36 recommended analysts receive more training in analyzing anomalies while Informant 3 added that analysts must learn that not all questions require classified answers. OSINT is often sufficient and more cost-effective, rather than exhausting scarce HUMINT sources. Consumers, on the other hand, should never bypass the analysis stage of the intelligence cycle and make decisions based on raw information (Informant 34). Six percent of informants recommended training consumers but also analysts and collectors on the role and limitations of intelligence, to ensure there are no miscommunications or false expectations between the different actors.

A couple of informants stated that the IC is still more reactive than proactive, and that the reaction time must improve community-wide. In terms of human resources, 5% of informants recommended that mid-level management should be reduced to address unnecessary bureaucracy and "institutional slowness." Half of them added that these mid-level bureaucrats should return to the collection and production stages of the intelligence cycle.

Five percent of the informants emphasized the need to keep counterterrorism a priority to maintain momentum. A couple of them added that the media plays a major role in ensuring the public remains vigilant. Another reason to keep the media and public involved is that, generally, a lot of hard work within the IC otherwise goes unnoticed. This becomes an issue during budget negotiations. Three percent of the informants stated that the IC requires additional resources to be able to effectively combat terror. There is an urgent need to protect the IC's resources to avoid a repeat of 9/11. However, the relationship between the IC and media is complex, evolving and often tense (Dover and Goodman, 2009). The IC is still recovering from the WikiLeaks

and Edward Snowden scandals, which has had a negative effect on the individual agencies' willingness to share information. "My greatest concern is the continued dissemination of classified information to the media. Stiffer penalties should be sought and those who are convicted should have their clearances revoked and employment terminated" (Informant 13).

A handful of informants support Devine's recommendation to create Department of Intelligence led by a Cabinet-level SecInt. They proposed that, unlike the National Security Advisor, the SecInt should not be appointed by the President, but by Congress. Initially, the DNI could assume this position – pending congressional approval. The ODNI would be dismantled as redundant but merged into the new department. More specifically, Informant 43 proposed that the SecInt should not be an elected government official, but a politically unbiased individual, with their own committees to review the needs of the various elements. "It should be mandated that the SecInt's determination should be the sole voice that speaks on behalf of the community as a whole. After all, this SecInt would have far greater breadth and depth of the needs and priorities of the IC." The position of the National Security Advisor, and per default the National Security Council, would be eliminated. A replacement structure comprised of civilian contractors accountable only to Congress could be established instead (Informant 43). Three percent of informants appear to share this vision, at least to some degree, as they recommended dissembling the ODNI and reassigning these responsibilities to the DCI, but to include budgetary and resource control over both the civilian and military elements. A couple of the informants even recommended dissembling unnecessary military elements, or at least merging their responsibilities into more modern institutions. "Some DoD intelligence agencies are needlessly wasteful and these funds could be better spent" (Informant 1). In contrast, Poteat (2012) argued that the ODNI has succeeded in its primary mission to improve the

cooperation and information-sharing within the IC as well as with relevant partners. While he recognizes that the DNI, in some matters, lacks the subject matter expertise and often requests assistance from, for example, the CIA when briefing the White House on foreign intelligence matters; he does not believe that giving the ODNI control over the intelligence budget will increase the effectiveness of the IC. Poteat argued that it would only divert the DNI's time and attention away from national security and the IC towards the politics of Capitol Hill, i.e. an increased number of meetings with Congress and political lobbyists.

More than 90% of the informants interviewed believed that the IC has increased its counterterrorism capabilities. However, more than half of these – as well as the 8% who answered that the IC has not increased its counterterrorism capabilities – are not convinced that the IC will be able to thwart another major terrorist attack against the U.S., unless additional improvements are made – and soon. Past progress in terms of applying lessons learned do not rule out the possibility of future attacks – particularly considering the following areas of concern:

- Announced intelligence budget cuts;
- Downsizing of the military;
- Declining public vigilance; and
- The fact that a single-minded and resourceful enemy can identify and exploit a current, or future, blind spot of the American defenses and achieve another surprise attack.

In sum – while politicians, the media and the public have a major role to play – the IC must maintain their excellent track-record from the past two decades in preventing terrorist attacks against the U.S.

CONCLUSIONS

In the wake of 9/11, vast amounts of resources poured into the IC and allowed for extensive inquiries into the lessons to be learned from the intelligence failure to prevent the attacks and into making recommendations for systematic reforms. The need to learn from mistakes is the most pressing in times of intense political scrutiny. However, under such conditions, learning is often the most challenging.

With the exception of a series of sudden and, according to some of the informants, questionable reforms – including the establishment of the ODNI and DHS – it took nearly a decade to arrive at the relatively more effective intelligence system the U.S. has today. Evidence of this was the failure to consolidate the watchlists, the need for which was only realized following the 2009 Christmas Day Bomber-incident.

In response to the first research question, whether the IC has learned any lessons from the terrorist attack of 9/11 in terms of strategic intelligence and its role in counterterrorism, the answer is "yes, but only to a certain degree." The most important lessons learned were to:

1. Not underestimate the terrorism threat and the need for a more proactive counterterrorism approach and to have proper targeting of potential terrorist threats;
2. Improve cooperation and information-sharing, not only between and within agencies but with other domestic and foreign partners;
3. Utilize a variation of collection methods (HUMINT, OSINT, GEOINT, SIGINT, etc.) to derive timely, actionable intelligence for consumers to make informed decisions since insufficient HUMINT collection efforts contributed to the intelligence failure that led to 9/11; and
4. Reform and update policies, laws, and infrastructure to more effectively combat modern terrorism.

Significant strides have been made in terms of bridging the various organizational cultures that prior to 9/11 seemed nearly incompatible. The various IC elements, with their different mandates and procedures, have been generally willing to increase cooperation but still remain reluctant to share information because of a fear that it increases the risk of classified information being leaked. Remaining challenges range from limited resources and cooperation to insufficient communication between collectors, analysts and consumers in order to collect, process, and act upon intelligence more effectively. There needs to be an emphasis on the need for analysis-driven collection that clearly meets the needs of the consumers. While there has not been another large-scale terrorist attack in the U.S. since 9/11, the majority of informants are not convinced that the progress the IC has made in applying lessons learned is sufficient enough to prevent another major attack.

Based on the survey findings, the first recommendation is to promptly evaluate whether it is more appropriate to resolve these issues with the current organizational structure in place, or if this post-9/11 risk environment demands the establishment of a Department of Intelligence – separate from the DoD and the Department of State – and the appointment of a Cabinet-level SecInt to oversee, coordinate, determine priorities for intelligence matters, based on the input from all elements of the IC. The intelligence budget oversight procedures can remain, but the SecInt could be responsible for presenting a recommended budget as well as a justification based on a needs assessment to receive congressional approval.

The second recommendation is to not reduce the intelligence budget further, but rather allocate and utilize the resources more jointly and efficiently. A significant reduction of the intelligence budget, in combination of downsizing the military can prove counter-productive to the progress made since 9/11. The active learning, which has been aided by the inquiries and subsequent capacity

building efforts, has been instrumental to the positive reforms and increased effectiveness of the IC. Albeit tempting for a peacetime administration under enormous pressures due to the coronavirus pandemic and severe financial crisis, reducing the intelligence budget can jeopardize the momentum gained within the IC and risk a return to a pre-9/11 state where the U.S. once again is "flying blind" in a world of unknowns. The first two recommendations would facilitate a downsizing of the IC in terms of human and other resources. It would also streamline the individual elements of the IC and optimize the use of the scarce resources.

The third recommendation is to continue to invest in additional capacity building. Introducing new methods/technology, developing critical skills, and increasing the number of rotational assignments have yielded results and should continue. There needs to be improved communication between collectors, analysts and consumers in order to collect, process, and act upon intelligence more effectively.

Furthermore, to prevent future misuse of intelligence products to support politically-based decisions and prompt military action, increased check-and-balance systems should be implemented.

Finally, the IC should finish what it started. The survey findings suggest that the IC fully appreciates the benefits of active learning and has taken action to apply the lessons learned from 9/11 and other attacks to prevent history from repeating itself. Practical application of the lessons learned and institutionalization of best practices will develop the collective capability of active foresight, i.e. improving the ability of the IC to recognize early warning signs and implement proactive measures to prevent any future acts of terrorism against the U.S.

With active foresight as the ultimate, but constant, objective, the IC must continue to collect, analyze, and disseminate the lessons learned from past

attacks and thwarted plots. This will improve the IC's collective institutional memory and institutionalize the best practices that have been derived by learning from past successes and failures. *Never again.*

RESOURCES

- AFIO: Association of Former Intelligence Officers (2011) "Intelligence Communities," *The Guide to the Study of Intelligence, Intelligencer: Journal of U.S. Intelligence Studies,* Winter/Spring: 48.
- Anderson, W. and Poteat, G. (2010) "A New Paradigm for Intelligence Analysis," *Intelligencer: Journal of U.S. Intelligence Studies*, 17 (3): 113-114.
- Andrew, C., Aldrich, R. J. and Wark, W. K. (2009) *Secret Intelligence: A Reader*, New York: Routhledge.
- Bamford, J. (2001) *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency,* New York: Double Day, Random House, Inc.
- Bellantoni, C. (2010) "Obama Says Intelligence Nation's First Line Of Defense, But Notes Failings," *Talking Points Memo*, (Washington, DC), 7 January, available online at: https://talkingpointsmemo.com/news/obama-says-intelligence-nation-s-first-line-of-defense-but-notes-failings; accessed 10 September 2011.
- Bobbitt, P. (2008) *Terror and Consent: The Wars of the Twenty-First Century*, Penguin Books: London.
- Borch, F. (2003) "Comparing Pearl Harbor and 9/11: Intelligence failure? American unpreparedness? Military responsibility?," *The Journal of Military History,* 67 (3): 845–860.
- Bruneau, T. C. (2007), "Introduction: Challenges to Effectiveness in Intelligence due to the Need for Transparency and Accountability in Democracy," *Strategic Insights*, 6 (3).

- Builta, J. A. and Heller, E. N. (2011) "Reflections on 10 Years of Counterterrorism Analysis," *Studies in Intelligence,* 55(3): 1-12.
- Coleman, C. and Moynihan, J. (1996) *Understanding Crime Data: Haunted by the Dark Figure*, Buckingham: Open University Press.
- Davis, L., Wermuth, M., O'Cornell, K. and Treverton, G. (2005) "Terrorism and intelligence reform," in D. Aaron, (ed.) *Three Years After. Next Steps in the War on Terror*, RAND Corporation: 25-34; available online at: http://www.rand.org/publications/CF/CF212/; accessed 14 August 2011.
- Devine, J. (2009) "Tomorrow's Spygames," *Intelligencer: Journal of U.S. Intelligence Studies*, 17(2): 17-27.
- DHS: Department of Homeland Security (2006) "Homeland Security Information Network Could Support Information Sharing More Effectively," *Department of Homeland Security: Office of Inspector General*, OIG-06-38, June; available online at: http://www.hsdl.org/?view&did=464589; accessed 10 December 2011].
- DHS: Department of Homeland Security (2019) "Fusion Centers," *Intelligence & Analysis*, September; available online at: https://www.dhs.gov/fusion-centers; accessed 30 March 2020].
- DNI: Director of National Intelligence (2011a) "ODNI Fact Sheet," *Director of National Intelligence;* svailable online at: http://www.dni.gov/content/ODNI%20Fact%20Sheet_2011.pdf; accessed 12 November 2011.
- DNI: Director of National Intelligence (2011b) "History of the Office of the Director of National Intelligence," *Director of National Intelligence*, available online at: http://www.dni.gov/history.htm; accessed 25 September 2011.
- Dover, R. and Goodman, M. S. (2009) (eds.), *Spinning Intelligence; Why Intelligence Needs the Media, Why the Media Needs Intelligence,* New York: Columbia University Press.

- Eldridge, T. R., Ginsburg, S., Hempel II, W. T., Kephart, J. L., Moore, K., and Accolla, J.A. (2004) *9/11 and Terrorist Travel: Staff Report of the national commission on terrorist attacks upon the United States*, available online at: http://govinfo.library.unt.edu/911/staff_statements/ 911_TerrTrav_Monograph.pdf; accessed 10 September 2011.
- Elliot, M. (2002) "Could 9/11 have been prevented?," *Time,* 4 August, available online at: http://www.time.com/time/nation/printout/0,8816,333835,00.html; accessed 10 September 2011.
- Fielding, N. (2009). "Qualitative Interviewing and Ethnography," in N. Gilbert, (ed.) *Researching Social Life,* London: Sage.
- Gladwell, M. (2003) "Connecting the dots: The paradox of intelligence reform." *The New Yorker,* (New York), 10 March.
- Green, N. (2009) "Formulating and Refining a Research Question," in N. Gilbert, (ed.) *Researching Social Life,* London: Sage: 43-62.
Haberfeld, M. R. and von Hassell, A. (2009) (eds.) *A New Understanding of Terrorism: Case Studies, Trajectories and Lessons Learned*, London: Springer.
- Hart, C. (1999) *Doing a Literature Review: Releasing the Social Science Research Imagination.* London: Sage.
- Herman, M. (2002) *Intelligence Power in Peace and War,* Cambridge: Cambridge University Press.
- Iannotta, B. (2011) "U.S. Intel Director Outlines Budget Strategy," *Defense News*, (online), 17 October, available online at: http://www.defensenews.com/article/20111017/DEFSECT04/110170304/U-S-Intel-Director-Outlines-Budget-Strategy; accessed 12 November 2011.
- Johnson, L. K. (2003) "Preface to a Theory of Strategic Intelligence," *International Journal of Intelligence and Counterintelligence*, 16 (4): 638-663.
- Jones, J. L. (2002) "Confronting an Old Enemy: Terrorism and the Changing

Face of Military Intelligence," *Research Report NNN/2002-04*, Weston, FL: Florida International University.

- Kaplan, L. (2011) Private interview with author on 12 December.

- Keegan, J. (2004) *Intelligence in War: Knowledge of the Enemy from Napoleon till al-Qaeda*, London: Pimlico.

- Knodel, J. (1993) "The design and analysis of focus group studies: a practical approach," in

D. Morgan, (ed.) *Successful Focus Groups: Advancing the State of the Art,* Newbury Park, CA: Sage Publications.

- Kristol, W. (2005) "Victory in Spite of All Terror," *The Weekly Standard,* 10 (41), 18 July.

- Cole, D. and Lobel, J. (2007) "Why We're Losing the War on Terror," *The Nation,* 24 September: excerpt.

- Lefebvre, S. (2004) "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence*, 16 (4): 527-42.

- Likert, R. (1932) "A technique for the measurement of attitudes," *Archives of Psychology*, 140.

- Levitsky, M. (2002) "Fighting Terrorism: A New Kind of Enemy and a New Kind of War," *Defense Intelligence Journal,* 11 (1): 11-15.

- Marquise, R. A. (2012) Private interview with the author on 17 January.

- May, E. R. (1992) "Intelligence: Backing into the Future," *Foreign Affairs,* 71: 66.

- Mazzetti, M. (2011) "Detective Work on Courier Led to Breakthrough on Bin Laden," *The New York Times*, [Online], 2 May, available online at: http://www.nytimes.com/2011/05/02/world/asia/02reconstruct-capture-osama-bin-laden.html; accessed 12 September 2011.

- Miceli, S. (2011) Private interview with professional on 7 December.

- Miller, S. (2012) Private interview with professional on 14 January.
- Nachmias, D. and Nachmias, C. (1976) (2nd ed.) *Research Methods in the Social Sciences,* London: Edward Arnold.
- Napoleoni, L. and Carisch, R. (2005) "Terrorist finance," *The Club de Madrid Series on Democracy and Terrorism, Confronting Terrorism, Vol. II: International Summit on Democracy, Terrorism and Security*, 8-11 March, Madrid: 27-32; available online at: http://english.safe-democracy.org; accessed 3 September 2011.
National Commission on Terrorist Attacks Upon the United States. (2002). *The 9/11 commission report*. New York: W. W. Norton.
- Nordell, D. (2011) Private interview with founder and CEO of New Global Markets on 11 December.
- Perkel, W. (2004). "Money laundering and terrorism: Informal value transfer systems." *American Criminal Law Review,* 41: 183–213.
- Pillar, P. (2002) "Fighting International Terrorism: Beyond September 11th," *Defense Intelligence Journal,* 11 (1): 17-26.
- Poteat, G. (2011) "The Importance of Solid, Accurate, Actionable Strategic and Tactical Intelligence – and the Guts to Convey it to Leaders," *Intelligencer: Journal of U.S. Intelligence Studies*, 18 (2): 3-4.
- Poteat, G. (2012) Private interview with author on 11 February.
- Preobrazhensky, K. (2011) Private interview with public speaker and author on 12 December.
- Ranelagh, J. (1992). *CIA: A History,* London: BBC Books.
- Reid, T. (2003) "America's weapons evidence flawed, say spies," *The Times*, (London), May 7; available online at: http://www.commondreams.org/headlines03/0507-09.htm: accessed 3 September 2011.
- Reveron, D. S. (2006) "Old Allies, New Friends: Intelligence-Sharing in the

War on Terror," *Defense Intelligence Journal,* Summer 2006, [Online], available at: http://derekreveron.com/Documents/su04-reveron.pdf; accessed on 11 October 2011.

- Reveron, D. S. and Stevenson Murer, J. (2006) (eds.) *Flashpoints in the War on Terrorism,* New York: Routhledge.

- Roth, J., Greenburg, D. and Wille, S. (2004) *National Commission on Terrorist Attacks Upon the United States – Monograph on Terrorist Funding;* available online at: http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf; accessed 15 August 2011.

- Rustmann Jr., F. W. (2012) Private interview with author on 13 February 2012.

- Ruth, L. M. (2012) Private interview with professional on 17 January.

- Schmitt, E. and Lipton, E. (2009) "Officials Point to Suspect's Claim of Qaeda Ties in Yemen," *The New York Times,* (New York), 26 December, available online at: http://www.nytimes.com/2009/12/27/us/27terror.html?_r=1&scp=1&sq=bomber%20charged&st=cse; accessed 11 August 2011.

- Schultz, R. H., and Vogt, A. (2003). "It's war! Fighting post-11 September global terrorism through a doctrine of preemption." *Terrorism and Political Violence,* 15 (1): 1–30.

- Select Committee on Intelligence (2011) *Report of the Select Committe on Intelligence, United States Senate: Covering the period January 3, 2009 to January 4, 2011*. 17 March; available online at: http://www.intelligence.senate.gov/pdfs/1123.pdf; accessed 10 September 2011.

- Sellers, B. (2012) Private interview with author on 26 January.

- Selltiz, C. and Jahoda, M. (1962) *Research Methods in Social Relations,* New York: Holt, Rinehart and Winston.

- Shelfer, K. M. and J. M. Verner (2002) "Improving Counterterrorism Analysis: Using Scenarios to Support the Development and Use of Integrated Information Systems," *Defense Intelligence Journal,* 11 (1): 55-70.

- Steven, G. and Gunaratna, R. (2004) *Counterterrorism.* Santa Barbara, CA: ABC-CLIO, Inc.

- Storbeck, J. (2005) "Policing," *The Club de Madrid Series on Democracy and Terrorism, Confronting Terrorism, Vol. II: International Summit on Democracy, Terrorism and Security*, 8-11 March, Madrid: 7-12; available online at: http://english.safe-democracy.org; accessed 3 September 2011.

- Tétreault, M. A. (1991) "Autonomy, Necessity, and the Small State: Ruling Kuwait in the Twentieth Century," *International Organization,* 45 (4): 565-591.

- U.S. Congress (2002) *The House Intelligence Committee Report on Counter-Terrorism Intelligence Capabilities and Performance Prior to 9/11*, [Hearing], U.S. Congress. House. Committee on Armed Services. Special Oversight Panel on Terrorism. 107th Congress, 2nd Session, 5 September. Washington: U.S. Government Printing Office, 2003. 46p. [Hearing]. :SuDoc# Y 4. AR 5/2 A: 2001-2002/43.

- Warner, M, (1994) (ed.) *CIA Cold War Records: The CIA under Harry Truman,* Washington, D.C.: CIA History Staff, Center for the Study of Intelligence, CIA.

- White, J. (2002) (3rd ed.) *Terrorism: An introduction*, Belmont, CA: Wadsworth Publishing.

- Wright, L. (2006) *Looming Tower: Al-Qaeda and the Road to 9/11*, New York: Random House, Inc.