AIR UNIVERSITY

AIR WAR COLLEGE

Defending the Homeland

The Case for Integrating National Guard Intelligence Personnel into the State Fusion Centers

BRENT W. GUGLIELMINO
Lieutenant Colonel
Air National Guard of the United States

Air War College
Maxwell Paper No. 67
Maxwell Air Force Base, Alabama

October 2012

Defending the Homeland: The Case for Integrating National Guard Intelligence Personnel into the State Fusion Centers

Lt Col Brent W. Guglielmino
Air National Guard of the United States (ANGUS)

> *It's clear that collectively, many in the homeland security business have lost sight of key intelligence lessons from 9/11. Because of their actions, we may well be destined to helplessly watch the unfolding of another 9/11-style incident, all the time knowing that the next post-disaster commission will rediscover the same core intelligence mistakes and suicidal bureaucratic processes/resistance.*
>
> —Maj Gen Todd Bunting, ANGUS
> Kansas Adjutant General

In the fall of 2009, five al-Qaeda operatives were arrested by federal authorities while in the final stages of separate operational plans to conduct attacks within the United States.[1] Clearly, law enforcement was aware of their activities. Others within the US intelligence community were aware of the identity of some of the individuals and their relationships with al-Qaeda but had no knowledge of the specific plots that were underway.[2] Alarmingly, the adjutants general (TAG) of the states where the plots unfolded were unaware of these activities until the individuals were arrested and the stories hit the press.[3] This is significant because the National Guard plays a key role in the American homeland security (HLS) enterprise, principally in response to a chemical, biological, radiological, nuclear, or explosive (CBRNE) event. Yet, they typically lack sufficient access to potentially vital information

that is available via other channels until after it hits the press or has become operationally irrelevant.

These events highlight a major flaw in the current information and intelligence sharing paradigm, particularly as it pertains to the National Guard. What if these men hadn't been arrested? What if they had successfully executed their attacks? The Guard would have been one of the last to know despite being one of the principle first responders to a potential terrorist event. How many lives would have been lost in the name of maintaining the stovepipes and firewalls between the intelligence and law enforcement worlds? More importantly, how can this flaw be corrected?

The National Guard lacks a fundamental understanding of the role of intelligence as a result of the historical security paradigm within the United States. This paradigm created a culture so averse to domestic intelligence operations and so deferential to the civil liberties and personal freedoms of Americans that in some instances, it imperils them. An oft-asked question since 9/11 is, how many civil liberties are Americans willing to forgo in order to secure their freedoms? For most Americans, the obvious answer to that question, as the flurry of post-9/11 legislation and vast changes to America's HLS landscape clearly shows, is more than what they currently are.

Through nearly its entire history, the Guard has been a domestic force with a mission that could best be described as a strategic reserve

primarily operating within the borders of the United States. The longstanding sensitivities of the American public regarding domestic intelligence operations and the Guard's citizen-soldier history, understandably, led the Guard to minimize its intelligence footprint as much as possible.

In 2004 the 9/11 Commission recommended several changes to the dominant information sharing and homeland security paradigm in its final report to Congress. It identified 41 recommendations to help prevent another terrorist attack on the United States; of those 41, six pertain specifically to information sharing—more than any other single topic.[4] Since 9/11, a number of significant foundational documents and key organizations have stood up in the United States to enable the fusion of information and intelligence urged by the 9/11 Commission. John Rollins of the Congressional Research Service (CRS) emphasizes the relative weight assigned to these intelligence and information fusion concepts noting, "All major post 9/11 government reorganizations, legislation, and programs have emphasized the importance of intelligence in preventing, mitigating, and responding to future terrorist attacks."[5]

Concurrently, operational adaptations have occurred with significant implications for the military, law enforcement, and the overarching HLS paradigm. One of the key developments involves the role of the National Guard, specifically the creation of the National Guard Joint Staff, represented in the states by the Joint Force Headquarters

(JFHQ). The JFHQs are the National Guards' operational coordinating entity and, consequently, would be responsible for coordinating any Guard response to a terrorist event. Unfortunately, the intelligence officer, or J2, is not a high priority in most JFHQs and in many cases is not even a full-time position. In other instances, the J2 is not a trained and certified intelligence officer. Despite the many reforms since 9/11, the Guard intelligence enterprise remains alarmingly detached from the rest of the HLS community, jeopardizing its ability to achieve sufficient situational awareness and adequately posture Guard HLS assets to respond to a potential terrorist act within the United States.

This paper first addresses the current homeland security landscape as it pertains to the National Guard, detailing the role the Guard has been directed to play and the legal landscape undergirding what the National Guard can and cannot do in terms of HLS operations. Second, it proposes a potential solution to the problem of better connecting the National Guard into the larger HLS community by integrating National Guard intelligence personnel into the existing state fusion center (SFC) enterprise. Finally, an assessment of the objectives, advantages, and second-order effects of this action is included.

Research Process

This paper uses standard archival research citing a broad array of publically available sources. Additionally, a number of personal e-mail interviews were conducted by the author with various state adjutants

general and members of the National Guard Bureau (NGB) staff. Efforts were made to contact individual JFHQ-State J2s, but most were unavailable or unable to respond within the timelines provided. The author relies heavily on personal experiences while serving as chief of current intelligence within the NGB Joint Staff as well as serving as the principal intelligence analyst for the chief of the NGB from 2008 to 2010.

The Role of the National Guard

The 2010 Quadrennial Defense Review recommended that the National Guard plays a prominent role in the CBRNE consequence management and response plans of US Northern Command (USNORTHCOM). In coordination with the Department of Homeland Security (DHS) and the Federal Emergency Management Agency, the plan calls for the Guard to develop 10 new units known as homeland response forces (HRF). The HRFs would join an already robust lineup of 57 National Guard combat support teams (CST) and 17 CBRNE enhanced response force packages (CERFP) to increase the existing Department of Defense (DOD) CBRNE consequence management enterprise from 18,000 personnel to approximately 24,000 by the end of fiscal year 2010.[6]

This tremendous growth in the Guard's homeland role, approximately 33 percent in terms of CBRNE response force structure, is a reflection of the words of former secretary of Homeland Security Tom Ridge who stated that the military's role in HLS would be significant and

would be "played predominantly by the National Guard."[7] Moreover, in 2008 the Commission on the National Guard and Reserves, in their final report to the Congress and the secretary of defense on National Guard transformation, recommended that "Congress should mandate that the National Guard and Reserves have the lead role in and *form the backbone* of DOD operations in the homeland."[8] While a legal mandate for this has not yet materialized, momentum in the HLS community in recent years emphasizes increased Guard involvement in HLS operations.

While no formal tasking has appeared, the National Guard Joint Staff is already heavily invested in, and tasked to be, an integral player in the United States' HLS paradigm. Moreover, recent emphasis by DOD on the total force as a result of the global economic crisis likely translates into an extended period of fiscal austerity for regular DOD assets leading to more substantive efforts to integrate reserve component and regular forces. This will result in even more prominent roles for the National Guard in certain missions.

The Need for Situational Awareness

USNORTHCOM commander, Adm James Winnefeld Jr., recently called the National Guard "NORTHCOM's indispensible partner" stating that "the Guard is the key connective tissue, the tie between the first responders in the states and the federal team."[9] NORTHCOM depends more than ever on the Guard to provide effective, local, on-scene leadership in response to domestic disasters, as well as in monitoring US

borders, and in HLS operations in general. From an operational perspective, Guard forces tasked with key response and force protection missions in the homeland must be as knowledgeable of their operating environment as possible. They must share a common, well-developed picture of the domestic threat environment with their HLS partners and establish a capability in the two regimes that monitor, report on, and predict the likely future of the threat environment: law enforcement and intelligence. This was the intent undergirding the concept of SFCs.

The Rise of the State Fusion Centers

SFCs are state owned and operated facilities housing law enforcement and intelligence specialists from across a broad spectrum of local, state, and federal government in one common facility. Intended to be the first line of defense against homeland terror threats, they ensure effective fusion of law enforcement and intelligence information at all levels of government. At present there are 72 SFCs within the United States, each with unique capabilities and manning and each with a slightly different perspective of their mandate.[10]

In August 2006, recognizing a disparity of capabilities, policies, and procedures across the SFC enterprise, the Department of Justice and DHS collaborated in developing a set of fusion center guidelines "to assist in the establishment and operation of centers."[11] The guidelines did not correct the substantial differences from one center to the next, and there remains no standard requirement for what a fusion center

should look like or do. According to John Rollins of CRS, "Although many of the centers initially had purely counterterrorism goals, they have increasingly gravitated toward an all-crimes and even broader all-hazards approach."[12] This ongoing variation between centers perpetuates the stove-piped architecture the 9/11 Commission hoped to avoid. The commission implied that to effectively achieve fusion of intelligence and law enforcement information, it is necessary to have representation from all principle stakeholders working side by side on a daily basis. However, according to a 2008 CRS report, "While many of the centers have prevention of attacks as a high priority, little 'true fusion,' or analysis of disparate data sources, identification of intelligence gaps, and proactive collection of intelligence against those gaps which could contribute to prevention is occurring."[13]

The Legal Landscape and Intelligence Oversight Policy

Historically, there has been significant opposition within the military to conducting intelligence operations within the United States, despite the provisions afforded under intelligence oversight (IO) policy. Within the Guard, leadership tended to defer to the judicial guidance of their respective staff judge advocates general (JAG), often suggesting that the Guard should not be involved in domestic intelligence activity in any way—the ultimate stovepipe. This extremely conservative approach has been the prevailing mentality over the years and has protected TAGs from potential legal difficulties stemming from possible IO policy

breaches or civil liberties violations. Conversely, it undermined IO policy, eliminated intelligence as a situational awareness tool, and destroyed fusion initiatives in the SFCs. To be clear, provided it is properly followed, there is no directive or legal impediment in current IO policy preventing integration of National Guard intelligence personnel into the SFCs.[14] According to the NGB JAG, there is no legal reason why DOD intelligence personnel, including Guardsmen operating in Title 10 or Title 32 status, who follow IO rules regarding retention and methods and have a legal mission to do so, cannot conduct intelligence activities pertaining to foreign intelligence threats within the United States.[15] DOD Regulation 5240.1-R, *Intelligence Oversight Policy*, procedure 12 states, "DOD intelligence components *are* authorized to cooperate with law enforcement authorities for the purpose of investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or *international terrorist activities*."[16]

IO policy is governed by Executive Order (EO) 12333, *United States Intelligence Activities*, and supplemented by DOD Regulation 5240.1-R and the various service-specific IO regulations and instructions. In a very broad sense, EO 12333 outlines the legal boundaries for the intelligence community. It states that foreign intelligence operations fall under the purview of the intelligence community; whereas, domestic intelligence operations are the purview of the law enforcement community—specifically, the Federal Bureau of Investigation (FBI). However, DOD

5240.1-R provides more guidance on the proper execution of EO 12333 and offers specificity on circumstances and procedures under which it is acceptable for US military intelligence personnel to engage in intelligence activities within the United States against US persons (USPERS).

Guard intelligence personnel are required to comply with all federal IO rules without exception. However, before one can understand how IO policy affects the National Guard, there are a number of issues that must be understood regarding the duty status of Guardsmen, the concept of "intelligence activities," and the latitude that IO policy actually provides, enabling intelligence personnel to do their jobs legally in a domestic environment.

Title 10 vs. Title 32, State vs. Federal

Guardsmen operate under one of three provisions of the US Code: Title 10 status (T10), Title 32 status (T32), or state active duty (SAD) status. The distinction between these statuses is significant with a tremendous impact on what Guard intelligence personnel can and cannot legally do. T10 and T32 are federal statuses, and each carries certain permissions and restrictions. While in T10 status, individuals are activated by the federal government to serve on active duty and must operate under the same restrictions as their regular Army or Air Force brethren. T32 Guardsmen are also mobilized into federal service but specifically for the purposes of conducting training in support of their T10 mission. T10 and T32 personnel are allowed to conduct intelligence

activities within the United States and to access federal intelligence databases and computer systems as long as they have been given a legal mission and they operate within the confines of IO policy.

IO policy is complex, but for the purposes of this paper, there are two key elements of note. First, properly authorized intelligence personnel engaged in intelligence activities on a USPERS must conduct their activities using the least intrusive means.[17] Second, intelligence personnel have 90 days to determine whether intelligence on a USPERS they may have collected or used is germane to the mission. If so, they may proceed in accordance with their mission; otherwise, they must destroy the information and cease any further operations against that USPERS. Short of these two considerations, there is no legal impediment to Guard intelligence personnel working in an SFC and fusing intelligence and law enforcement information.

Current State of Affairs

Interestingly, in 2006 the Guard explored the possibility of integrating intelligence personnel into the SFCs but decided not to proceed with the initiative. At the time, there was a great deal of debate as to the extent to which the Guard should be involved in HLS operations. The NGB J2 had even drafted a concept of operations (CONOP) for integrating National Guard intelligence personnel into the SFCs. Col Timothy Keasling, author of the draft, noted:

> "DHS took immediate offense to the document since they were the lead for sharing information with state and local officials. They saw this [CONOP] not as help from the Guard but as disrupting their rice bowl . . . this after six months of discussion within the [DOD working] group [of which DHS was a part]. DHS then provided a copy to DOD HD [assistant secretary of defense-homeland defense]. HD did not see this as a DOD mission, voiced IO concerns, and asked the Guard to shut down the effort. All guidance [to shut down the initiative] was verbal. Just prior, the National Information Strategy was released by the White House stating that the National Guard did have a role. Additionally, the program manager-information sharing environment had recently published their plan discussing the National Guard's role. Despite these overarching documents, OSD [Office of the Secretary of Defense] ignored the Guard's role and the senior leadership of the Guard had no desire to engage. The National Guard's role in information sharing [subsequently] died on the vine."[18]

Consequently, in a number of instances since March 2008, JFHQ-State J2s and their respective TAGs were found to be unaware of key intelligence pertaining to homeland threats affecting their respective states.[19] Moreover, many key Guard personnel either did not have

adequate clearances or lacked regular access to appropriately classified facilities and/or equipment.

The issue is not whether the Guard should be involved with the details of ongoing terrorism investigations within the United States. However, as the designated DOD first responder to CBRNE contingencies and a potential source of security and force protection in the region, they should be made aware that there are investigations underway and who the principals are. To be prepared to respond to or avoid a terrorist attack, the Guard needs some basic facts and general situational awareness of potential trouble spots. In most cases, the law enforcement community is fully aware and often actively engaged in thwarting plans of potential terrorists. What happens if they miss one, as in the recent case of Mohammed Abdul Mutallab, the Christmas Day bomber who attempted to blow up a civilian airliner over the United States? National Guard leadership cannot properly posture and/or position assets to deal with the potential aftermath of a successful attack without access to information on the current operating environment. The fact is, in most cases that access is lacking.

Several TAGs share these concerns. When asked whether they felt they had sufficient access to intelligence, particularly intelligence regarding homeland threats, there was a general sense of agreement amongst TAGs.[20] General Bunting, TAG of Kansas, responded with an emphatic "no." "This is true in regards to both tactical and strategic

intelligence, fully understanding that intelligence products are never absolute. The majority of [intelligence] reports raise your blood pressure and stress levels but lack anything actionable, or many times even relevant, to the states."[21]

Maj Gen William Wofford, the Arkansas TAG, shared the same opinion, mentioning that while he did receive intelligence of this sort, it was generally not very useful. "The problem is that the intel we receive is not always timely and many times has not been analyzed properly to show important trends if there are any. If the info is not timely it is as bad as not receiving info at all."[22] Conversely, in Maryland the situation appears to be much better from the perspective of the Maryland TAG, Brig Gen James Adkins. General Adkins relates that Maryland is getting very good intelligence support on homeland and state threats, and he attributes this success largely to the full-time presence of Maryland Army and Air Guard inside the Maryland SFC "that maintain good information sharing networks with various Homeland Security officials both at federal and state level."[23]

Colonel Keasling, former deputy director of the NGB J2 at a time when the National Guard was initially considering integrating Guard intelligence folks into the fusion centers, has a very clear perspective:

> No, I do not [believe the states are receiving adequate intelligence of homeland threats]. Too few states have qualified J2s and too little communications capability in the

> right places. Most of a states' [intelligence] capabilities rest with their organic component intelligence structures, the Army or Air Guard respectively, who are generally focused on their overseas missions. To make matters worse, some states have no organic intelligence structures. Compounding this problem, most TAGs lack the will and understanding to leverage the intelligence capability they do have.[24]

Two Distinct Worlds: Intelligence and Law Enforcement

Currently, given the role the Guard has in the HLS and the Defense Security Cooperation Agency mission areas, the lack of access to critical intelligence becomes increasingly problematic for the National Guard as well as the rest of the HLS community and the people they are tasked to protect. It positions the Guard as the weakest link in the HLS chain in terms of situational awareness. That often translates into being the weakest link operationally as well.

The Guard has tried to kill two birds with one stone by maintaining a footprint inside many of the fusion centers in the form of counterdrug intelligence analysts. To be clear, many counterdrug intelligence analysts are not intelligence analysts at all. According to the NGB's counterdrug office, at best about half of the counterdrug intelligence analysts are actually intelligence qualified personnel.[25] Many are actually law enforcement personnel having served as a member of a provost marshall's staff or as field investigative officers. Most have not

attended one of the service intelligence schools (Fort Huachuca, Arizona, for the Army or Goodfellow AFB, Texas, for the Air Force), nor have they served as intelligence officers in the field at any time during their careers.

Law enforcement and intelligence represent two separate career fields and hence two different skill sets. Fundamentally, law enforcement is forensic in nature, looking backward from the point of the crime in an effort to determine what happened and prosecute the guilty. Conversely, intelligence inherently assumes a predictive, forward-looking posture, being tasked to provide the current threat picture and assess likely future enemy actions. This is not to debate the merits of either. Indeed, the 9/11 Commission states both are needed to develop the best possible picture of the threat. The 9/11 Commission's intent behind the SFCs was to collocate law enforcement and intelligence personnel. The Guard responded by collocating military and civilian law enforcement personnel, forgoing the intelligence piece, thus missing the whole point.

A Possible Solution

A possible solution to this problem is to integrate National Guard JFHQ-State J2s into the SFCs, affording them regular and systematic access to relevant intelligence and law enforcement derived data pertaining to potential terrorist threats to the individual states as well as the larger homeland in general. Moreover, it affords them the opportunity to participate in the interagency analysis that goes on within the HLS

community, bringing more fidelity to the federal threat picture via additional inputs from the state and local level.

Such a move could provide not only National Guard leadership but also leadership across the whole of government, with a substantially improved view of the threat landscape and a better opportunity to coordinate response options with partners and stakeholders at all levels—the stated intent of the 9/11 Commission. This is a solution TAGs could enact on their own accord; there is nothing stopping them. The Guard must be willing to shift priorities within the JFHQ-State staffs. If they ever hope to have the situational awareness necessary to posture and/or respond to a terror attack, it is an absolute imperative that the Guard appropriately man the JFHQ-J2 positions with trained, qualified, experienced, full-time intelligence professionals and imbed them inside the SFCs.

Impediments to Integration

The Guard has yet to make intelligence a priority. Most of the JFHQ-J2s do not have access to top secret intelligence specific to homeland threats either due to lack of equipment or lack of adequate clearances.[26] This is reflected in the fact that only 30 of the 54 JFHQ-State J2s are full-time personnel.[27] Of those 30, it is unknown at the national level how many state J2s are actually intelligence qualified. This information is likely available at the state level; however, the NGB has not conducted a data call to date to determine those numbers. According

to the NGB J2, 22 of the 54 JFHQ-State J2s have access to the communications architecture and equipment capable of accessing top secret information on a daily basis. Of those 22, three rely on using someone else's top secret facilities while the remaining 19 have, or are building, their own dedicated JFHQ sensitive compartmented information facility.

In the summer of 2009, the NGB J2 developed a top secret intelligence portal addressing a number of National Guard interest areas specifically related to the intelligence the chief of the NGB receives during intelligence briefings. This was done to help better focus the Guard on the threat environment domestically and overseas. The portal required the highest levels of security clearance and handling caveats. Subsequently the NGB J2 notified the state JFHQs of this new source of intelligence. Over the course of the past year, only 10 of the 30 full-time JFHQ-State J2s accessed the products and information on that portal and still fewer did so regularly. In other words, of the 54 total J2 positions, less than 20 percent had accessed the key intelligence available and potentially relevant to them.[28]

Unfortunately, manpower in the National Guard is a zero-sum game. Should leadership decide to increase intelligence manning, another staff element would suffer. Failing a dramatic change in funding or a lifting of the congressional cap on active Guard reservists,[29] there is at present no way around this hurdle. The real question is whether TAGs

and NGB leadership are prepared to go before Congress in the aftermath of another 9/11 and explain why they still haven't developed their intelligence and information sharing capabilities to the point urged by the 9/11 Commission. If not, serious work faces the National Guard in reprioritizing its manpower to address deficiencies in its intelligence capacity and capability.

Operationally, the Guard has been proactive in adapting to the post-9/11 world with the creation of HRFs, CSTs and CERFPs as well as the JFHQ-State construct, but the necessary changes to develop an intelligence infrastructure capable of supporting the new missions and force structure have not yet materialized. Many TAGs do not have the requisite security clearances to see most of the vital homeland security related intelligence that is available and which often affects them.[30] When coupled with the fact that their respective JFHQ-J2s may be equally constrained, it becomes extremely problematic to expect TAGs to have a suitable level of situational awareness to properly posture and/or position their forces for the purpose of either force protection or disaster response. In short, they are being asked to make decisions without the benefit of much of the key information needed.

Despite overwhelming evidence that the Guard requires access to key HLS related intelligence, it is the only organization with a sizeable role in HLS lacking the vital intelligence it needs. For a number of reasons—some self-inflicted, some bureaucratic, and some technical—

the National Guard lacks day-to-day access to and is denied the daily collaborative analytical exchange on the vast stores of homeland security-related information/intelligence currently available within the intelligence community (IC).

Conclusions

The National Security Strategy (NSS) of the United States is very clear and unambiguous regarding how the United States intends to combat terrorism and foster a more secure homeland:

> To prevent acts of terrorism on American soil, we must enlist *all of our intelligence, law enforcement, and homeland security capabilities*. *We will continue to integrate and leverage state and major urban area fusion centers* that have the capability to share classified information; establish a nationwide framework for reporting suspicious activity; and implement an integrated approach to our counterterrorism information *systems to ensure that the analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government*. We are improving information sharing and cooperation by linking networks to facilitate Federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate.[31]

Consistent with all post-9/11 US counterterrorism (CT) policy guidance, the NSS advocates sharing all relevant CT information across all levels of government. The IC, DOD, and DHS have made tremendous strides in moving towards this goal. The development of a robust community of SFCs, coupled with ongoing efforts to develop policy that supports sharing, is merely the first step. Short of the technological hurdles currently impeding a robust and efficient HLS enterprise, the next step in meeting the objectives of the 9/11 Commission is to ensure that those who are tasked with defending the homeland—the citizen soldiers of our nation—have appropriate access to the same information that is already being shared by other parts of the HLS enterprise.

Part of the solution is for TAGs to seize the initiative and act by reprioritizing their manpower and properly resourcing their intelligence capabilities. There are no legal constraints; though there may be some funding constraints, but ultimately, where there's a will, there's a way. The Guard is assuming more and more of the DOD's HLS responsibilities, and USNORTHCOM has reached out to them to work more closely. Now is the time for National Guard intelligence personnel to be integrated into SFCs. It will enable a better preventive posture against possible terrorist operations in the homeland and, in response to those operations, ensure a better coordinated response across the spectrum of government by first responders. Additionally, it further minimizes the

traditional stovepipes that have represented the operational norm between and within the intelligence and law enforcement communities.

Failing any new policy directives, the issues highlighted in this paper will continue to pose a risk to our nation's defense. The fear is that rather than correcting the problem, we will continue to march forward with our stovepipes, once again finding ourselves a nation enthralled with the televised activities of yet another congressionally mandated post-disaster commission. We will once again hear testimony telling how we failed to connect the dots and fuse the intelligence. We will hear how we lacked the imagination to consider that the enemy might attack us in some new way. Perhaps we'll even see an IC reorganization. At what cost? To be sure, integrating Guard intelligence personnel into the SFCs would have far-reaching implications on not just the National Guard but the DOD, DHS, and the entire US HLS paradigm. It remains as one of the final pieces of the fusion and integration puzzle and represents the most expedient and cost-effective means of achieving the necessary level of situational awareness our homeland defenders need.

Notes

1. In September 2009, Najibullah Zazi, a Pakistani national and permanent resident of the United States was arrested for attempting to build and detonate explosive devices in the New York City subway. The attacks were ordered by al-Qaeda regional leader and facilitator Saleh al-Somali and orchestrated between Zazi and two associates across state

lines between Colorado and New York. In October 2009 David Coleman Headley, a Pakistani-American citizen, and Tawahar Rana, a Pakistani-Canadian, were arrested, accused of conspiring with al-Qaeda, the Pakistan-based terrorist organization Lashkar-e Tayiba, the Pakistani Interservices Intelligence directorate, and a number of former Pakistani military officers. Headley reportedly played a prominent role in the planning and execution of the 2008 Mumbai attacks killing 168, as well as the 2010 bakery attack in Pune, Germany, which killed 15 and injured 54. In fact, he was deeply involved with various international terrorist cells; Judith Crosson, Rocco Parascandola, Alison Gendar, Jake Pearson, Tina Moore, and Larry Mcshane, "Reputed Al Qaeda Terror Cell Operative Najibullah Zazi Arrested by FBI," *New York Daily News*, 19 September 2009, http://www.nydailynews.com/news/world/2009/09/19/2009-09-19_zazi_cuffed_after_qaeda_canary_sings_li_secret_code_used_to_inform_plotters_li.html; Annie Sweeney and Hal Dardick, "Chicago: Front Line in War on Terror: Officer Spotted Mumbai Terrorist Running His Children through Military Drills in Park," *Chicago Tribune*, 11 November 2010, http://www.chicagotribune.com/news/elections/ct-met-terrorism-chicago-police-1114-20101111,0,391867.story; and Antonio Olivo, "Chicago Agency a Front for Terror Plot, Probers Allege Federal Officials Target Operations of First World Immigration," *Chicago Tribune*, 3

January 2010, http://www.chicagotribune.com/news/chi-terror-rana-immigrationjan03,0,6207893.story.

2. Personal knowledge of the author who served as the principal briefer to the chief, National Guard Bureau (CNGB) at the time of the activities in question and who regularly corresponded with other intelligence agencies on current intelligence issues.

3. TAG is a major general in a given state who commands that state's National Guard forces. In many states, the TAG is tasked with the additional responsibilities of being the state emergency manager and/or the state director of homeland security. TAGs with these additional responsibilities are sometimes referred to as "super TAGs;" and author's personal experience as chief of the NGBs current intelligence division and principal intelligence analyst to the CNGB. Between 2008 and June 2010, I had the opportunity to present either face-to-face briefings or to telephonically notify various TAGs on certain specific terrorism issues. In almost every case, the TAGs were unaware of the information presented to them.

4. National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, 1st ed. (Washington, DC: W. W. Norton & Company, 2004), 416–19.

5. John Rollins, *Fusion Centers: Issues and Options for Congress*, Congressional Research Service (CRS) Report for Congress (Washington, DC: CRS, 18 January 2008), 5.

6. Department of Defense (DOD), "Homeland Response Force Fact Sheet," http://www.defense.gov/news/HRFCERFP.pdf (accessed 15 October 2010).

7. Tom Ridge, director of the Office of Homeland Security (address, Fletcher Conference, Washington, DC, 14 November 2001), http://www.vodium.com/mediapod/ifpa/ (accessed 15 September 2010).

8. Commission on the National Guard and Reserves, *Transforming the National Guard and Reserves into a 21st Century Operational Force*, Final Report to the Congress and the Secretary of Defense (Washington, DC: Government Printing Office, 31 January 2008), 15, emphasis added.

9. SSgt Jim Greenhill, "'You Can Count on Me,' NORTHCOM Commander Tells National Guard," http://www.ang.af.mil/news/story.asp?id=123219170.

10. Department of Homeland Security, "State and Local Urban Fusion Centers," http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

11. Ibid., 1.

12. Ibid.

13 Rollins, *Fusion Centers,* 1.

14. Maj Erin McMahon (Office of the NGB Judge Advocate), e-mail interview with author, 15 October 2010.

15. Ibid. Key to this discussion was the idea that any form of communication (e.g., e-mails, chat room correspondence, etc.) between US persons and a terrorist entity would suffice to establish a foreign nexus sufficient for intelligence personnel to handle information pertaining to the individuals in question. Intelligence personnel would still be bound by all other aspects of IO policy including proper mission, authorization, handling caveats, etc.

16. Ibid., emphasis added.

17. DOD Regulation 5240.1-R, *Intelligence Oversight Policy*, December 1982.

18. Col Timothy Keasling (former deputy director of the NGB Joint Intelligence Directorate), e-mail interview with author, 30 September 2010.

19. The author had over 20 opportunities to brief several state TAGs and JFHQ-State J2s, either face-to-face or via other means, while a member of the CNGBs current intelligence team. A common response at the end of said briefings, with very few exceptions, was stunned disbelief. In particular, we presented intelligence regarding three specific terrorist threats to the homeland that had been developing for several weeks to the TAGs of the affected states. Two of the three threats were ultimately foiled and received significant attention in the national media. We had

been briefing this information to the chief of the National Guard for weeks, but when we briefed the TAGs of the affected states, they were shocked to hear that this was going on in their respective states. Additionally, in most cases, it was necessary to arrange for classified read-ons for the TAGs and their staffs prior to briefing them so they would have authorization to receive the information. No doubt realizing the limitations inherent to the National Guard Joint Staff and its limited connectivity into the intelligence community, it is a tremendous credit to the CNGB that he emphasized we notify the TAGs directly upon receiving this type of intelligence.

20. TAGs from Kansas, Arkansas, Alabama, and Maryland, e-mail interviews with author, as well as personal phone conversations held in the course of regular duties with chiefs of staff with nearly 20 different states between 2009 and 2010.

21. Bunting, e-mail interview with author, 29 September 2010.

22. Maj Gen William Wofford (TAG of Arkansas), e-mail interview with author, 23 September 2010.

23. Brig Gen James Adkins (TAG of Maryland), e-mail interview with author, 12 October 2010.

24. Keasling, e-mail interview with author, 1 October 2010.

25. Capt Mesha Cichon (counterdrug division, NGB [NGB-J32]), e-mail interview with author, 27 October 2010.

26. Personal experience in working with many of the JFHQ-State J2s while serving as chief of the current intelligence division within the NGB-J2.

27. "NGB J2 Contact Roster," 9 September 2010, https://gkoportal.ngb.army.mil/sites/J2/Lists/J2%20State%20Contact%20List2/AllItems.aspx (accessed 18 October 2010).

28. NGB J2 Top Secret Intelligence Portal Statistics, current as of October 2010.

29. Active Guard Reserve (AGR) refers to a federal military program which places Army National Guard and Army Reserve Soldiers and Air National Guard and Air Force Reserve Airmen on federal active duty status to provide full-time support to National Guard and Reserve organizations for the purpose of organizing, administering, recruiting, instructing, or training the Reserve components. Soldiers and Airmen in such status are commonly referred to as AGRs. There is a congressionally mandated cap on the total number of AGRs allowed at any given time.

30. Personal experience in working with many of the JFHQ-State J2s while serving as chief of the current intelligence division within the NGB-J2.

31. Barack H. Obama, II, *National Security Strategy of the United States* (Washington, DC: The White House, May 2010), emphasis added.