COMMUNICATION GAPS IN THE INTERAGENCY: LET'S CHATTER BETTER

ARTICLE

*Col. (Ret.) Arnaldo Claudio**

The lack of an efficient and viable communications strategy across the Interagency was identified as a key issue within the top intelligence agencies in the United States during the events of 9/11. Intelligence, Law Enforcement, and First Responders were unable of filtering information that could have possibly prevented the terrorist attack of 9/11. The way this radical operation took place came as a total surprise for many, especially to the Intelligence community.[1]

As a responsible American I care much about the safety and security of this nation. Therefore, it is my hope that this paper will help illustrate the operational gaps of communications that exist within our Interagency; particularly those that directly affect coordination. From a personal perspective, I define the concept of Interagency as the establishment and development of intergovernmental contacts to reinforce operational relationships and procedures, increase situational awareness and improve coordination in dealing with issues and actions of common interest and responsibility. The latter, promotes efforts to advance the synchronization of activities with intergovernmental partners, to ensure mutual understanding and unity of effort during special events and emergency operations such as 911.

As we now know, prior to September 11, 2011, the United States had only limited engagements with terrorists in our national territory and very minimum in Washington DC. As Americans, we became very complacent with our security. During the mid-70s and early 80's the United States experienced several airline hijackings and bombings—however, nothing to the scale or unpredictability as 9/11.

---

* Retired U.S. Army Colonel, Inter-agency Program Director of the Joint Force Headquarters National Capital Region and U.S. Army Military District of Washington. Was the military police officer with the highest rank in Iraq from 2005-2006. I would like to thank the Law Review of the Inter American University, School of Law for giving me the opportunity to publish this paper.

[1] Michael Chertoff, *The 9/11 Essays: 9/11 Before and After*, Homeland Security Affairs, vol. 7, num. 2 (Sept. 2011).

In 1993, the World Trade Center was bombed, causing a large number of casualties, including six (6) deaths.[2] A close examination at the next decade shows an increase of terrorist activities against the United States, most of them abroad. The Intelligence community was able to foil some attacks to the homeland. The latter, gave the impression that the intelligence communication systems and information sharing and dissemination were working well. Obviously 9/11 was going to prove them wrong. During this decade terrorists were able to inflict most of their damage against the United States oversees. They were successful in conducting several large-scale operations in which many Americans lost their lives: Khobar Towers, bombings of two US embassies, Kenya and Tanzania [3] and the attack on the USS Cole in Yemen. [4] As part of the overall effort of this paper, I will attempt to emphasize and explain how the Interagency's lack of intelligence communications, synchronization efforts, and mitigation processes account for terrorists' capacity to avoid early detection. As described by the *9/11 Commission Report* –we need to uncover how ill-prepared our nation was in addressing and preventing another attack.[5]

Several years ago, the government started re-evaluating its security arrangements across the United States and abroad, with the Department of Homeland Security ("DHS") as the lead federal agency. One of the main goals of the DHS was to look at its communications systems and their capacity to provide the Interagency with a common operating picture. It is important to note that the success of the DHS in providing adequate communications also depends on its ability to properly coordinate and synchronize security efforts with state and local government representatives (a major undertaking, especially in Washington DC, where hundreds of local, state, and federal partners operate within close proximity). Therefore, the need to work jointly is vital in providing and implementing a successful homeland security communications strategy.[6]

---

[2] FBI, FBI 100: First Strike: Global Terror in America, http://www.fbi.gov/news/stories/2008/february/tradebom_022608 (accessed Feb. 26, 2013).

[3] OJP, Message from the Director, http://www.ojp.usdoj.gov/ovc/publications/infores/respterrorism/message.html (accessed Feb. 24, 2013).

[4] Betty Burnett, *The Attack on the U. S. S. Cole in Yemen on October 12, 2000* (1st ed., Rosen Pub Group, 2003).

[5] To specifically illustrate the magnitude of the failure of communications amongst the Interagency see 911 Commission Report Preface, page 2, released on July 22, 2004: "We learned that the institutions charged with protecting our borders, civil aviation, and national security did not understand how grave this threat could be, and did not adjust their policies, plans, and practices to deter or defeat it. We learned of fault lines within our government—between foreign and domestic intelligence, and between and within agencies. We learned of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers."

[6] Kevin Strom & Joe Eyerman, *Interagency Coordination in Response to Terrorism: Promising Practices and Barriers Identified,* Four Countries Criminal Justice Studies: A Critical Journal of Crime, Law and Society vol. 20, num. 2, 131-147 (2007).

Today major efforts have been taken to ensure our systems are ready and able to confront the many threats of terrorism to our country.[7] The major reasons why any large-scale agency can operate in an efficient and innovative manner is directly related to the way it is lead and organized, and its capacity to gather and circulate information (communications). In my opinion, the U.S. Government was judicious in creating the Department of Homeland Security, as it provides a source of leadership that enables the Government to respond to crisis at all levels. As described by professor Agranoff in his book Collaborative Management, the re-engineering process with respect to local governments is always necessary.[8] When studying the evolution of our Government's response to crisis and the role of the Interagency, the need for change has made us look internally to ensure we continue to do what is necessary so the evil of 9/11 or similar attacks never return to our shores. This will guarantee that our country is ready to react to the unpleasant acts of terrorism and other crisis response scenarios.

Agranoff's concepts are very appropriate when describing the DHS' role regarding the need for actionable communications. Advancing the way our Government secures the United States cyber domain is one of the most critical aspects of the Homeland Security communication process. The key in making steady progress lies in the way we manage information security. Therefore, it is important that cyber managers (civilian and military) fully tackle the issues associated with the Homeland Security web, specifically those issues associated with authorities, dollars, and intelligence resources. One could argue that a fundamental problem lies in the method in which our Government is safeguarding the access of our sensitive data and the issues related with internal dissemination of the information we gather.

Exactly eleven (11) days after the terrorist attacks on September 11, 2001, the former President of the United States, George W. Bush, ordered the creation of a new federal department to manage, coordinate, and provide strategic direction for the United States Federal Government concerning all aspects related with Homeland Security. This new organization was to be called the DHS. President Bush appointed Pennsylvania's Governor Tom Ridge as the first director of the organization. It is important to note that prior to the establishment of the Department of Homeland Security, all homeland safety and security events in the United States (domestic) were carried out by as much as forty (40) agencies and supported by more than two thousand (2,000) split congressional financial appropriations. Two years later, on March 2003, several security organizations in the Federal Government, including the Secret Service, Coast Guard, Customs Service, Federal Emergency

---

[7] Lester Moore, *Interagency Cooperation: It's As Hard as You Think It Is Naval War College* (A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations, Oct. 2006).

[8] Robert Agranoff & Michael McGuire, *Collaborative Public Management: New Strategies for Local Governments* (Georgetown University Press 2003).

Management Agency (FEMA), and the Transportation Security Administration, were transferred to the command and control of the Department of Homeland Security. [9] Since its creation in 2001, the Department of Homeland Security has continued to expand as an institution. Today, the Department is the third largest cabinet in the Federal Government with more than 240,000 employees. [10]

The present Homeland Security Secretary, Janet Napolitano, has a more positive view concerning our current security posture. In an article titled "*Progress Toward a More Secure and Resilient Nation*",[11] the Secretary states that the past ten years have "made us smarter about the kind of threats we face, and how best to deal with them," focusing on the strategy of local hometown security as a key to making our communities and our nation safer in the future. She argues that, "more and more often, state, local, and tribal law enforcement officers – and their community partners – are best positioned to uncover the first signs of terrorist activity".[12] Her statement speaks to the establishment of better lines of communication among the many Interagency partners and suggests that our Nation is much more prepared to handle crisis, as a result of the use of effective communication strategies.

Any responsible reaction to a crisis should include at a minimum a well-coordinated Interagency approach. In today's national security environment the answer comes in the form of the National Response Framework (communications via training). This National Response Framework ("NRF") is a directive that "communicates" the way our Interagency will conduct an "all-hazards response". The National Response Plan (NRP) was the Government's plan to respond to emergencies such as natural disasters or terrorist attacks. It came into effect on December 2004, and was superseded by the NRF on March 22, 2008. This document, just as many publications associated with the failures of 9/11, provided a new sense of direction for the Interagency to respond to crisis and also served as a great source for research. In Washington D.C., this document is well known and widely utilized.[13] The NRF provides key details as to how the Interagency will align itself regarding the roles, responsibilities, communications, chain of command priorities, and other aspects inherent to the crisis management response strategies. The NRF links all levels of government, non-governmental organizations and the private sector as well. In reviewing this document, I see one important main objective: To capture and

---

[9] Elizabeth C. Borja, *Brief Documentary History of the Department of Homeland Security 2001-2008*, https://www.hsdl.org/?view&did=37027 (accessed Feb. 25, 2013).

[10] DHS, *About the Department of Homeland Security*, http://www.dhs.gov/about-dhs (accessed Feb. 25, 2013).

[11] Janet Napolitano, *10 Years After, The 9/11 Essays: Progress Toward a More Secure and Resilient Nation*, Homeland Security Affairs vol. 7 (2011).

[12] *Id*.

[13] NCR, *NCR Homeland Security Strategic Plan Appendices,* http://www.mwcog.org/uploads/pub-documents/o15fXFc20101001065908.pdf (accessed Feb. 26, 2013).

document lessons learned (best practices) for the management of incidents across the entire spectrum of operations (local, regional, terrorist or natural disasters), so they can serve as a guide to success in future crisis management operations. As stated by Professor Eyerman, prior multi-agency training and high-level operational and strategic coordination efforts among the multiple agencies will define failure or success during responses to crisis and their eventual solutions.[14]

Any response to an emergency such as 9-11 or the 2005 London bombing requires a well-coordinated, multi-agency approach.[15] This is a delicate undertaking as most of the crisis management situations these governments face are mainly related to law enforcement (prevent, and/or resolve a threat or act of terrorism). Consequence management is predominantly an emergency management occupation and includes actions to safeguard public health, reestablish essential government functions, and provide emergency relief to governments, businesses and individuals affected by the consequences of terrorism. Communications play a vital role in the success or failure of these operations. The operational response to a terrorist threat will have to be fully coordinated and organized prior to the employment of forces. The effectiveness (or deficiency) of these response efforts, as well as their solutions, will also depend on the prior multi-agency training and the high-level operational and strategic coordination among the multiple agencies. Lieutanant Christopher Bertram of the Salt Lake County Sheriff's Office, emphasizes how critical collaboration and communications are when conducting homeland security operations among the Interagency.[16] During this event (categorized as a National Security Special Event by DHS) over ten thousand (10,000) law enforcement officers representing federal, state and local agencies helped secure the games. This collaboration and well-synchronized communications efforts culminated in providing approximately 4 million people with a safe and secured venue. As I see it, this event and the manner in which the Interagency came together was an indication that the 9/11 terrorist attacks had forever changed the way in which our Government would collaborate in all aspects of security operations, just as it had been suggested by the references cited in this paper.

There are many examples concerning the importance of partnering and communicating with federal, state and local authorities for defense support to civil authorities. [17] This partnering is fundamental to the Interagency as many of the local authorities provide communication capabilities that support the way we effectively respond to crisis and demonstrate that their adequate organization has enabled them

---

[14] Storm & Eyerman, *supra* n. 6.

[15] Alan Cowell, *London Finds Linked Bombs, a Qaeda Tactic,* N.Y. Times, http://www.nytimes.com/2007/06/30/world/europe/30britain.html?pagewanted=all&_r=0 (accessed Feb. 25, 2013).

[16] *Factors that effect Interagency collaboration: lessons during and following the 2002 Winter Olympics* (Master thesis, Naval Postgraduate School, 2008).

[17] Christopher Ford, *Twitter, Facebook, and Ten Red Balloons: Social Network Problem Solving and Homeland Security*, Homeland Security Affairs vol. 7, art. 3 (2011).

to properly execute their roles and duties. From a commander's viewpoint, the way in which support operations are prioritized is highly critical.

The key in making steady progress lies in the way we manage information security. Therefore, it is important that cyber managers (civilians and military alike) fully tackle the issues associated with the Homeland Security web, specifically those issues associated with authorities, dollars, or intelligence resources. A fundamental problem lies in the method in which our Government is safeguarding the access of our sensitive data and the issues related with the internal dissemination of the information we gather.[18] Case-in-point is the Wikileaks incident, where an Army Private First Class is accused of giving hundreds of thousands of classified documents to the anti-secrecy organization Wiki Leaks.[19] The article "*Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness*",[20] illustrates many of the challenges I believe are associated with information sharing among federal, state, and local agencies—all critical elements of U.S. Homeland Security tactical and operational strategy. The article proposes that few researchers have examined the relationship between the use of Homeland Security information-sharing systems and perceived levels of emergency preparedness.

After reading the article "*What Do We Know and Where Do We Go From Here?"*[21] concerning Virtual Teams ("VT"), the concept of Information Technology ("IT") modernization and globalization is evidently critical. This article, just like the one titled "*Evaluating the Impact of Contextual Background Fusion on Unclassified Homeland Security Intelligence*",[22] poses exceptional information concerning communications within a specific community and clearly supports the arguments presented in this paper. These articles also provide information concerning the use of unclassified products and their application by non-traditional recipients ("NTR"). Particularly interesting to me, in the second article, is the explanation of the impact of intelligence contextual background fusion through the use of hyperlink technology and the evaluation of the NTR concerning the use of technology. The latter provided qualitative information concerning communications usage, assessment, and information value that contributed to the development of my analysis.

---

[18] Alex Wagner, *U.S. Vulnerable to Terrorism, Especially Cyber Attacks, Intelligence Chiefs Say,* http://www.politicsdaily.com/2011/02/10/u-s-vulnerable-to-terrorism-especially-cyber-attacks-intellig (accessed Feb. 25, 2013).

[19] Mathew Hay Brown, *Bradley Manning charged in Wikileaks case*, The Baltimore Sun (2012).

[20] Hamilton Bean, *Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness*, Homeland Security Affairs vol. 5, num. 2 (2009).

[21] Luis L. Martins, Lucy L. Gilson & M. Travis Maynard, *Virtual Teams: What Do We Know and Where Do We Go From Here*, Journal of Management vol. 30, num. 6, 805-835 (2004).

[22] Charles Eaneff, *Evaluating the Impact of Contextual Background Fusion on Unclassified Homeland Security Intelligence,* Homeland Security Affairs vol. 4, num. 1 (2008).

For me, recognizing the threats posed by the enemies of the U.S. in the post 9-11 world is vital to our National Security Strategy. In the report titled "*9/11: Before and After*", [23] former HLS Director, Michael Chertoff, explains the massive breakdown concerning our ability to coordinate information gathering and integration amongst the multiple agencies. These failures led to the collapse of our intelligence system in identifying patterns of conduct that could have easily prevented the attacks. The latter only illustrates a small portion of the issues associated with our Government's ability to properly and securely communicate and coordinate vital national security information among the Interagency. In another report, author Eric Jorgensen illustrates an alternative example of poor communication and coordination among the Interagency concluding that —"[g]enuine interagency coordination and collaboration remain merely aspirational".[24]

In sum, the interaction and contact amongst federal, state and local agencies, organizations and jurisdictions support and facilitate the United States Government's missions of Homeland Defense (HLD) and Homeland Security (HLS). The Interagency day-to-day links could easily provide more accurate, timely and relevant information in support of planning and operational requirements for HLS and HLD. In addition, robust interagency relationships promote the participation of civilian agencies and organizations in federal, state, and local sponsored training exercises. In turn, their participation also contributes to the overall situational awareness of interagency roles, responsibilities, policies and practices that may impact our national security posture. As a result, the Interagency's coordination obtains greater visibility of potential capabilities and limitations of each of its agency partners. This insight is helpful during normal operations, but is even more significant during emergency situations such as 911.

The sum of any individual interagency relationship provides the foundation for the institutional relationships within organizations. These relationships aim to build and facilitate organizational cooperation based on trust and mutual benefits. In this regard, a mature institutional relationship is a two-way street. Each partner must perceive that the relationship fulfills an organizational or operational need that would be more difficult or costly to achieve by other methods. These needs and benefits may be asymmetrical. Consequently, everyone should avoid assuming that the benefit calculation by any agency and organizations of cooperating and interacting together will contain the same set of variables and produce the same results as our analysis. Asymmetrical needs may also indicate differing levels of input and contribution to the institutional relationship on a day-to-day basis. This may lead to situations in which it may seem that the relationship is lopsided in terms of investment and support. This underscores the importance of trust in maintaining

---

[23] Chertoff, *supra* n. 1.

[24] Eric A. Jorgensen, *Greater Than the Sum of Its Parts: Putting the Inter into the Interagency*, Prism vol. 2, num. 2 (2011).

an effective institutional relationship. Such asymmetries are more easily understood and accommodated when there is a high level of trust.

As I learned during my extensive military career, good communication is essential to building a cohesive and effective team, as well as for managing its performance. By knowing how to communicate and synchronize efforts, one can minimize risks, especially during critical and sensitive operations when accurate and timely information is vital. As I reviewed the literature used for this article, I found that overall the Interagency has enabled our security systems, both classified and unclassified, to communicate well among agencies and has instituted plans to adequately respond to national emergencies. However, 9/11 highlighted the critical need for an enhanced command and control and communications capability from which to sustain situational awareness and conduct operations across the Interagency. Clearly, the threats to our country are not going to be much different than they were in the past, and to manage these threats, the strategy must be different, proactive and responsive to the needs of our Nation. Thus the coordination needed among the many local, state, federal, civil, and military authorities to execute highly visible and sensitive events is absolutely critical.