Chapter 16
Geospatial Resource Integration in Support of Homeland Defense and Security

David Foster
Cherokee Nation Technology Solutions (CNTS), USA

Christopher Mayfield
NORAD-NORTHCOM Command and Control, USA & Space and Naval Warfare Systems Command, USA

ABSTRACT

The U.S. Department of Defense (DoD) has faced numerous challenges within the realm of Geospatial Information Systems and Science in fostering a Common Operational Picture suitable to homeland defense and security. This paper details the challenges and successes since September 11th, 2001 to build common ground for all federal, state, local governments, and non-government organizations that depend on geospatial data to provide for the safety and security of the Nation. An analysis of the protracted integration of commercial GIS technologies within the DoD and the speed, openness, and scale this expertise can bring is discussed as an issue for the Federal response to disasters. Finally, distinct successes of collaboration and integration of common standards and data currently in use at military commands is discussed as a robust path to improve future geospatial efforts.

INTRODUCTION

The security and defense of a nation is the primary responsibility of its government. Success in protecting the Homeland is the only acceptable result. Information sharing and integration efforts of federal organizations aligned with a focus on defense, such as the Department of Homeland Security (DHS), United States Northern Command (NORTHCOM), National Geospatial Intelligence Agency (NGA), and United States Army Corps of Engineers (USACE) provide valuable data, tools, and processes that mitigate risk, increase situational awareness, improve decision making, and secure information dominance. Leaders within the Department of Defense (DoD) understand that decision making within a crisis

DOI: 10.4018/978-1-5225-8054-6.ch016

requires the most current and complete information available. Simply, they "need quantified, explicit information which will really let you determine if this is bad or if this is *really* bad so we don't over respond and we don't ignore our real problem." (Brown 2011). Developing processes and relationships to obtain and share actionable information in response to domestic disasters is at the forefront of emergency response preparations. The evolution of spatial data sharing within official government channels has been a lengthy process that is still exploring a balance in the speed of commercial collaboration and innovation with the necessity to provide secure, vetted solutions that meet government standards. This paper demonstrates the significant gains made by government institutions in geospatial information capabilities, data sharing, and collaboration to protect the Homeland.

BACKGROUND AND EVOLUTION

The origins of contemporary use of geospatial technologies by more than a handful of specialists during crisis response can be traced to a small number of disasters as milestones. The main catalyst for the current United States Government geospatial cooperation, organization, capabilities and concepts was September 11th, 2001. Prior to this date, Federal and State organizations responsible for security of the country and disaster response insulated themselves from extensive collaboration and sharing with other agencies in order to protect information. Infamous domestic examples of poor collaboration as a contributor to pre and post event failures identified in the 9/11 Commission report include the 1993 World Trade Center and 1995 Oklahoma City bombings.

Geospatial technologies, although no longer in their infancy, were an expensive set of tools that a few specially trained employees used to create products at the discretion of their leadership. Sharing these geospatial products and data was not a compelling priority for many organizations. The 9/11 Commission Report identified the following as limited collaboration capacities within Federal agencies: Sharing information both internally and externally, insufficient training, inadequate resources, and perceived legal barriers to sharing data were issues that hindered the government's response to disasters. Specifically, the 9/11 commission declared in 2004: "breaking the older mold of organization stovepipes within purely executive agencies, we propose a National Counterterrorism Center (NCTC) that would borrow the joint, unified command concept adopted by the American military in a civilian agency, combining the joint intelligence function alongside the operations work." Furthermore, the Commission proclaimed: "Secrecy stifles oversight, accountability and information sharing. Unfortunately, all the current organizational incentives encourage over classification. This balance should change…..The President should lead a government-wide effort to bring the major national security institutions into the information revolution, turning a mainframe into a decentralized network. "The obstacles are not technological." (Brown 2011).

From the unforgettable tragedy of 9/11, the Incident Command System (ICS) and Department of Homeland Security were born to facilitate a change in the way government shares information and responds to crises. In 2004, the year the 9/11 Commission Report was published, Lieutenant General (LTG) Russel Honore took command of the U.S. Army First Army at Fort Gillem, Georgia. At that time First Army's primary mission was supporting civil authorities responding to domestic disasters. One of LTG Honore's first actions as commander was changing the way his operations center received, analyzed, processed and shared information. Having called together key staff into the First Army operations center LTG Honore gestured to a paper map on the wall and stated that the days of having paper maps in his operations center were over. He directed a US Navy Lieutenant Commander to turn on the Nuclear Power