HOMELAND SECURITY AFFAIRS

NETWORK FUSION:
INFORMATION AND INTELLIGENCE SHARING FOR A NETWORKED WORLD

Joseph W. Pfeifer

THE JOURNAL OF THE NAVAL POSTGRADUATE SCHOOL
CENTER FOR HOMELAND DEFENSE AND SECURITY

http://www.hsaj.org

Network Fusion: Information and Intelligence Sharing for a Networked World

Joseph W. Pfeifer

ABSTRACT:

An innovative design for sharing information and intelligence is found in the form of network fusion, which encourages collaboration across multiple disciplines by leveraging technology to connect the unconnected at classified and unclassified levels. As terrorists move to new methods of attack, law enforcement and first responders must use comprehensive and timely information and intelligence to both anticipate potential threats and to ensure a high measure of adaptability in responses. This article defines network fusion along with other architectures for homeland security connectivity; explores the current information and intelligence sharing challenges; examines how network fusion can enhance fusion centers as well as assist emergency responders; and makes several recommendations for implementing network fusion. Network fusion provides an opportunity to bring many unique perspectives together for smarter, faster and cheaper intelligence sharing.

INTRODUCTION

In April of 2004, a surreal meeting took place in a small restaurant in Monterey, California between a Minneapolis FBI agent and a New York City fire chief. The FBI agent described his experience of the days leading up to 9/11 and wanting to obtain a search warrant for Zacarias Moussaoui under the Foreign Intelligence Surveillance Act. He became so frustrated with the system, which did not more aggressively pursue a search warrant and lacked any urgency for sharing information, that, at one point, he blurted out to his supervisors that he was "just trying to stop someone from taking a plane and crashing it into the World Trade Center." Little did he know how prophetic his statement would turn out to be. The 9/11 Commission Report *described the month before the attacks as a "system blinking red" with warnings. Then I told an equally distressing story of never being told on September 11 about police helicopters' observations that the top fifteen floors of the North Tower, which I was in, were "glowing red" with fire and that the corner of the building was starting to buckle. These historical eyewitness accounts illustrate that the systems for intelligence and information sharing were "blinking red" for 9/11. While there have been improvements in distributing information, some wonder if information sharing and collaborative systems are still blinking red in today's networked world.*[1]

Many in the intelligence and first-responder communities would like to believe that commissions, studies, new policies, and executive orders have solved the United States' information and intelligence sharing problems. Yet "the same enduring realities that prevented adaptation before 9/11 have stymied adaptation even in the aftermath of tragedy."[2] The problem is that organizations, by their command and control design, are not structured for collaboration. The struggle that ensues is how to achieve connectivity for sharing information, within a system inhibited by organizations determined to pursue disconnectedness as a means for power and control.[3]

The disconnect that exists between organizations creates information asymmetries, which produce two consequences. The first is the inability to prevent an attack from occurring. Without information, organizations are helpless to stop terrorism. The second focuses on an organization's powerlessness to adequately mitigate and respond to terrorist incidents, when there is a lack of understanding of the threat environment. Terrorism will continue to challenge society because it cannot be

totally prevented, which necessitates the expansion of our present information sharing and intelligence system to contain policies for resilience.

A new design for organizations to share information and intelligence may be found in the form of network fusion, which connects not only the law enforcement and intelligence communities for prevention and protection purposes, but also other key components of the emergency responder community – such as fire departments and health care systems – for mitigation, response, and recovery efforts. Together all organizations can benefit from and contribute to the critical mission areas of homeland security through the power of networks.

Finding new approaches for collaboration may be less a matter of innovation and more a matter of discovering what is already done by organizations. Stephen Cohen and William Eimicke from Columbia University observe that organizations are becoming increasingly connected through inter-organizational networks.[4] They argue that government is moving away from the traditional hierarchical model that dominated the twentieth century and toward a more fluid continuum of organizational collaboration.[5] This trend means that organizations now are more likely to be connected horizontally and look outward toward other organizations for necessary functions. The ultimate goal of networked government organizations is the production of public value greater than any one organization could accomplish alone.[6]

The fusing of information for intelligence sharing is the goal for some centrally controlled systems; however, sharing information is more likely to occur when organizations are arranged as members of an integrated network, which transcends traditional organizational boundaries for a faster and smarter understanding of the threat environment. This article defines network fusion along with other architectures for homeland security connectivity; explores the current information and intelligence sharing challenges; examines how network fusion, as well as competitive forces, will strategically shape fusion centers; and makes several recommendations for implementing network fusion.

DEFINING NETWORK FUSION

Network fusion is an information sharing system that fuses information and intelligence from multiple sources to allow decision makers to better adapt to a changing threat environment. It leverages technology to improve awareness and collaboration across different disciplines by connecting voice, video, and data communications at classified and unclassified levels. Networks bridge gaps, strengthen relationships, and allow for innovation, speed, and flexibility in exchanging critical information.[7] Through the use of collaborative technology, network fusion is a framework for linking multiple systems for pushing and pulling information and intelligence. It provides a platform for connecting disparate organizations and their unique viewpoints.

In a networked world, fusion centers, created for the sharing of information and intelligence, as well as other critical information nodes, will have to change their shape from a strictly hierarchical, linear, or unidirectional hub-and-spoke network to that of a network platform that can connect and fuse information from many different sources rather than only those co-located with them. Christopher Bellavita, who teaches at the Naval Postgraduate School, contends that fusion centers are examples of an emergent approach to homeland security. They were first started post 9/11 at the state level, to bring people together for better information sharing. However, "fusion" means more than simply putting people from different agencies in the same room; it requires the fusing of information, which represents continuing evolution of fusion centers.[8]

The future of fusion centers will depend on their ability to collaborate with other organizations for prevention and response as well as their capacity for information to be pushed and pulled in real time through networking. Successful network fusion has three distinct advantages:

- Faster to communicate directly with decision makers and those closest to the information;
- Smarter to understand the threat environment through multiple perspectives;

- Cheaper to collaborate virtually rather than co-locate.

Network fusion exploits technology to quickly connect various organizations that participate in homeland security to exchange critical information, insights into potential attacks, and real-time situational awareness reports. Its effectiveness lies in the speed with which it connects decision makers who are close to the information with others throughout the network. Secure video conferencing eliminates travel time, which speeds up the network of information exchange. "Fast information is better than slow," which is the core philosophy of major corporate information companies, like Google.[9] Failure to consider the speed of network fusion as part of the intelligence and information process will greatly retard the ability to prevent and respond to terrorist threats and disasters.

John Arquilla, associate professor at the Naval Postgraduate School, maintains that the fight against terrorism "depends to some extent on technological innovation, but mainly on a willingness to innovate organizationally and doctrinally, perhaps especially by building new mechanisms for inter-agency and multi-jurisdictional cooperation."[10] The Markle Foundation Task Force supports this conclusion by further arguing that traditional information sharing prior to September 11 contributed to a lack of terrorism prevention and preparedness and recommends "network architecture" as a corrective measure.[11]

As terrorists move to employ new methods of attack, law enforcement and first responders must use comprehensive and timely intelligence to anticipate potential threats and to ensure a high measure of adaptability in their responses. System adaptability occurs when multiple insights or a diversity of viewpoints "enables people to see different things when they view the same event."[12] The fusing of insights from the intelligence community – law enforcement, the fire service, health care organizations, transportation systems, environmental protection agencies, and other organizations – provides an opportunity to bring many unique perspectives together for smarter overall analysis.

While senior decision makers in these aforementioned organizations normally do not sit in fusion centers, or occupy seats in emergency operations centers, such decision makers would add valuable experience, analysis, and intuition to the interpretation of reports if they were part of the information-fusing process. By connecting to a sundry of perspectives, network fusion leverages the knowledge of senior executives to form a smarter understanding of the threat environment.

EXISTING NETWORKS

It is not enough to create faster and smarter ways of enhancing information sharing; such methods also must have sustainable price tags. The cost of physical co-location is $200,000 per year, per person.[13] If a position is to be covered twenty-four hours a day, seven days a week, the economic impact is one million dollars per year. Add to this several different operations centers, and the cost is staggering and unsustainable. In addition, having scores of agencies represented in one location imposes space constraints. It is impossible for every agency to have a seat at the table in a fusion center; the size of the facility would be enormous and cost for personnel would be prohibitive. The solution is one of network fusion, which utilizes new and existing networks to extend the reach of fusion centers to emergency responders.

The development of network fusion for faster, smarter, and cheaper information sharing and collaboration will require a sociotechnical approach that makes use of hard and soft systems. Technical or hard systems draw on technology to assist in connecting security partners to information and intelligence. For agencies working with the Department of Homeland Security (DHS), information is exchanged through e-mail, Web posts, phone calls, and video conferences. Unclassified methods for information exchange use the Homeland Security Information Network (HSIN) platform, while classified information moves primarily over the Homeland Security Data Network (HSDN). Working with the Department of Homeland Security, first

responders can utilize the technology of hard systems for voice, video, and data communications to exchange classified and unclassified intelligence in a timely manner over secure systems.

New York City has created an unclassified community-of-interest Web portal on HSIN called the New York Situational Awareness Program (NYSAP). More than forty-five agencies participate in this collaborative environment for organizations to post and receive information and share real-time situational awareness. When the East Coast was hit by Hurricane Irene in 2011, critical information on flooding, downed trees, and people in need of assistance was shared among agencies using NYSAP, which enabled New York City to take immediate steps to respond and recover from this natural disaster. Work is also under way to create better collaborative tools to illustrate information in graphic form.

Social or soft systems are often overlooked when developing networks. These are the functional skills and qualifications needed for collaboration when dealing with classified information. Major organizations that are at risk from terrorism and acting as critical network nodes, or are connected to fusion centers and the Joint Terrorism Task Force, need personnel to receive information within the security domains of top secret, secret, and sensitive but unclassified. DHS has made a commitment to work with first responders in providing clearances and training as part of a system for intelligence based on organizational need, risk, and capability.

Types of Networks

HIERARCHICAL Linear pushing of information	**CO-LOCATED LIAISONS** Multiple agencies are co-located
HUB-AND-SPOKE Pushing information from a central node	**NETWORK FUSION** Using technology to connect and collaboration

Table 1: Four types of information and intelligent sharing systems.

HIERARCHICAL LINEAR SYSTEMS

Linear information networks are illustrated by information moving from first the federal to state level, then to local and tribal entities, and then to individual agencies based on a priority list. This type of network should be evaluated for a single point of failure and for bias when the system is stressed. Too often the flow of information through many successive levels is slow. There are also occasions when organizations tend to hold information to flex their power. Asking first responders to respond to terrorist incidents without current information and intelligence is like asking a pilot to fly without instruments or weather reports. A lack of information places first responders at a huge disadvantage when performing lifesaving rescues at extreme events.

However, there are narrowly defined incidents in which only a small group of people is supplied with information. Navy Seal Team Six and limited government officials were the only people who knew about the raid on Osama Bin Laden's compound. In this case, a hierarchical, linear system was used to ensure security. But to

locate Bin Laden, it took a large network. Leaders should not be limited to one type of network. Rather, they should consider "how well [a network's] structure is adapted to the activities the organization carries out and the environment in which it carries it out."[14]

HUB-AND-SPOKE SYSTEMS

The DHS has plans for seventy-seven fusion centers around the United States. One center is designated for each state, with a number of metropolitan areas having their own regional centers. These centers are designed as hub-and-spoke networks, where each fusion center acts as a hub and connects to various security partners as though the spokes of a wheel. Information flows primarily out of the hub and connects directly to spoke agencies. Hub-and-spoke networks are effective in spreading information to the overall network by pushing information from a centralized location.

The potential drawback of these networks is their inability to handle the bidirectional exchange of information in a timely manner. Similar to an airport terminal, such networks have limited capacity during peak traffic times.[15] The convergence of information may cause the network to slow down during critical moments and become so overwhelmed that information does not get exchanged in a timely manner. To avoid such congestion, this type of system only pushes information to agencies, with little room for tailoring the information to the end user. It also may not recognize the need to disseminate information to others than law enforcement agencies. The real danger is for a hub-and-spoke network to become a modernized informational stovepipe, where information originates from a place of limited perspective and is pushed only when the originating agency deems it necessary to do so.

Another example of a hub-and-spoke network is the video surveillance systems that have proliferated around many cities. Cities such as Los Angeles, London, and Beijing currently provide thousands of camera feeds into fire, police, and city emergency operations centers. Video feeds are selected by these operation centers to assist in acquiring better situational awareness. However, the weakness of this type of network is seen when information cannot be pulled or is not provided by the controlling agency.

CO-LOCATED LIAISON SYSTEM

With grant money from DHS and working with the private sector, the New York City Police Department (NYPD) has as many as 2,000 cameras feeding into their Lower Manhattan Security Initiative (LMSI). These cameras can provide critical images to criminal investigators and could assist decision makers if multiple terrorist attacks (such as those seen in Mumbai) were to occur.

Requests by the Office of Emergency Management (OEM) and the Fire Department of New York (FDNY) to receive live-feed video from LMSI to their emergency operations centers were repeatedly turned down by the NYPD. Alternatively, OEM and FDNY were invited to send a liaison to LMSI. However, this does not provide direct viewing of live video by senior decision makers. Instead, information has to be relayed by a lower-ranking liaison, by voice only. A liaison system often fails to get the right information to the right people at the right time.

Yet, many local and federal government programs see a liaison system of co-location as the only collaborative structure available for information exchange. While there is value in face-to-face collaboration and analysis, at times these co-located liaison systems consist of individuals or groups who act in parallel and do not generate unique ideas to increase collective value. If groups are not designed with shared responsibility and accountability, the liaison system can underperform.[16]

NETWORK FUSION

The struggle for information sharing in a networked world is to provide not just a seat at the table, but to have real-time information provided directly to decision makers. It does not matter who controls the raw data but how organizations and individuals can connect to extract the information needed to make

critical decisions, "because all of us are better than any one of us at understanding what the data is saying."[17]

The lack of a robust multichannel system for information and intelligence sharing points to a system that is still "blinking red." To avoid such limitation, collectors and consumers of intelligence and information should enhance their current systems of co-locating people by having a network fusion mechanism for pulling and pushing information. However, as agencies adopt a network approach to information and intelligence sharing, they will face many challenges.

INFORMATION AND INTELLIGENCE SHARING CHALLENGES

The Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 were written in response to a need for improved information and intelligence sharing. These acts were later strengthened by the issuance of a 2005 presidential memorandum establishing guidelines and requirements for a new information-sharing environment.[18] Even with such initiatives, the United States Government Accountability Office (GAO) concluded: "the nation still lacks a government wide policy and processes needed to build an integrated terrorism-related, information-sharing road map, but small-scale sharing initiatives are under way."[19] The *National Strategy for Homeland Security* (2007), the *National Response Framework* (2008) and *National Preparedness Goals* (2011) continue to highlight the importance of creating a culture of preparedness and disseminating information to enable first responders to better manage incidents and minimize damage.[20] A dynamic and unpredictable threat environment requires leaders to constantly evaluate their organizational structure for better ways to collaborate.

Sharing of information and intelligence among different agencies through networks creates a system-wide understanding of the threat environment. If information sharing fails, the ability of some agencies to make sense of the threat environment also fails. Lacking the relevant information to form a system-wide analysis of a threat environment could mean that individual agencies make separate decisions that, although appropriate for that agency, may conflict with the system-wide goal and thus prove adverse to that agency as well as to other units within the system.[21] The fusion center model strives to provide a comprehensive picture of the threat environment to lessen potential system failure; yet organizations tend to self organize and share intelligence in functional areas of prevention and protection, ignoring the need for intelligence for mitigation, response, and recovery. Sharing intelligence for only prevention will surely lead to the next surprise attack if a plot cannot be disrupted. However, using intelligence to also mitigate and respond to potential attacks will lessen the consequences and avoid the element of surprise. Since there is no such thing as a perfect defense against terrorism, homeland security agencies must prepare for a range of potential terrorist attacks and work together to diminish the effects of uncertainty.

In *Bak's Sand Pile* and a similar article in *Homeland Security Affairs*, Ted Lewis describes complex adaptive systems as being self-organizing: as these systems become more efficient and connected they reach a state of self-organized criticality (SOC) or the point where they collapse unexpectedly.[22] Based on this argument, fusion centers that have self-organized into law enforcement-only centers with limited central hubs for information may be hitting the point of criticality. What was once a well-intentioned idea for sharing intelligence has mutated, for some, into tightly connected criminal investigation fiefdoms that exclude those outside of law enforcement. On a more positive note, lecturer Paul Cilliers argues that the edge of criticality is the point at which systems can change with the least amount of effort.[23] The challenge for adaptation is to bridge information gaps and overcome organizational biases.

INFORMATION GAPS AND HOLES

Examining how networks function provides clues for identifying gaps and reengineering

intelligence sharing in terms of network fusion. The key building blocks of networks are the connections between organizations, which are referred to as ties. Social network research literature focuses on ties and bridging gaps between organizations. Opportunities for information sharing are dependent on the formation of these ties as a fundamental first step for creating a network model.

Having a multiplicity of ties between organizations will increase the chances for finding new information. According to Ronald Burt, professor at Chicago University, these ties span structural holes or gaps when there are two or more nodes that do not communicate available information.[24] The structural hole argument describes the negotiation of connections that bridge gaps to join otherwise disconnected people and information systems.[25] Two design principles are involved for an optimized network to create efficiency and effectiveness.[26] The first principle is to connect different non-redundant nodes to maximize diversity of information. The second principle is to use these contacts as a portal to others in a cluster. Instead of maintaining relations with all contacts, an optimized network delegates the maintenance of clusters to the primary contacts.[27] In this way, one organization is able to connect with many organizations. Fusion is about connecting to individuals and organizational clusters to take full advantage of available information.

When the small plane of the Yankees pitcher Cory Lidel crashed into a Manhattan high-rise in October 2006, first responders needed critical information in order to respond appropriately. They needed to know if this plane crash had any nexus to terrorism, if it was an isolated accident or one in a series of attacks, and if the specific building was prone to fire or collapse. Homeland Security officials in Washington also needed to have situational awareness about the incident and the extent of the fire. During this incident there were structural holes between the National Operations Center and New York City's first responders. The formal system for information exchange was slow to react because of these holes in the network as well as inadequate technology. However, an informal and hastily formed information-sharing network bridged those gaps to quickly provide critical information from the scene. This incident illustrates the value of having many ties and the need to formally bridge holes between organizations.

Morton Hansen, professor of entrepreneurship, argues that social research has concentrated too much on the ability of ties to access novel information and not enough on the transfer of complex forms of knowledge.[28] He claims that complex knowledge is best transferred by strengthening ties among different groups. The lack of interagency cooperation between organizations responding to 9/11 seems to support the hypothesis that weak ties inhibited these agencies from exchanging information. Understanding why weak ties may not always span across groups during complex incidents is critical to building networks for information fusion.

ORGANIZATIONAL BIASES

The *9/11 Commission Report* warns that the biggest impediment to an all-source analysis of intelligence needed to connect the dots of a terrorist plot is the human or systemic resistance to information sharing.[29] This develops as the tendency to look inward toward members of the same organization and avoid looking outward to other groups, thus creating *organizational bias*.[30] People are naturally prone to gravitate towards and give more information to members of their own organization and less information to outsiders.

As the stress and complexity of a crisis increase, people tend to focus on aspects judged most important to themselves and their agency.[31] Daniel Kahneman describes this as a case of "what you see is all there is" (WYSIATI).[32] Often organizations fail to allow for other possibilities, by turning inward. They create a positive in-group bias in favor of those who are part of the same group and a negative out-group bias against those who are part of an alternate group.[33] The events of 9/11 illustrated that the CIA and FBI, as well as first responders, did not realize how little information they had nor did they understand how the information they had could have assisted other agencies.

When people suffer from organizational bias, they frequently feel little obligation to exchange valuable information with those outside their group, since responsibility for acting is diffused across the in-group. This phenomenon excludes the out-group from receiving information that may be vital to its operation. The intelligence community traditionally views first responders as the outsiders; this organizational bias must be overcome when creating an intelligence network model. In a networked world, it is critical to strengthen ties and connections to law enforcement and first responders by developing trust and eliminating biases for information sharing and collaboration. Overcoming organizational bias increases the flow of information, which contributes to overall prevention and preparedness by anticipating potential attacks and building resilient systems to reduce negative effects.

MITIGATION NEGLECT

Another form of bias is *mitigation neglect* – or neglecting to share relevant information with those who must respond to and mitigate the effects of an event. To optimize homeland security efforts, law enforcement agencies and first responders must comprehend threats, assess vulnerabilities, and determine the impact of possible terrorist incidents. They also must be willing to set aside the conventional mindset that believes intelligence is only for prevention. Information sharing through a network model can strengthen prevention and mitigation efforts by increasing understanding of the threat and working collaboratively to detect and lessen the consequences of an attack.

One tactic of terrorists is to conduct a *sequenced attack*, using a small explosion or fire to lure first responders and/or passersby to the scene of an incident, only to cause maximum injury and fatality with a secondary explosive device. In 2002 in Bali, Indonesia, a backpack explosive was used inside a nightclub to drive occupants outside, where a more powerful vehicle-borne improved explosive device (VBIED) was detonated and killed 202 people. While the intelligence community works hard to prevent such events from occurring, it has neglected the need for first responders to have intelligence to understand the potential threat environment.

On December 11, 2010, a car fire was used in a busy shopping area in Stockholm, Sweden, to attract first responders to a car where an improvised explosive device was to be set off remotely. Fortunately, this attack on first responders failed. However, it took more than six weeks for the FDNY to learn of the VBIED car fire in Stockholm that put firefighters at risk. This delay in information and intelligence sharing to first responders is an indication of mitigation neglect by those who are responsible for sharing intelligence. Mitigation, or the lessening of effects before, during, and after an event, validates first responders' critical "need to know" for intelligence sharing.

SHAPING INTELLIGENCE STRATEGY

Intelligence is the process by which raw data is collected and transformed into usable information, and then disseminated to end users at the strategic, operational, and tactical levels.[34] Mark Lowenthal describes the intelligence process of collecting information as meaningless unless analysts can turn information into reports and briefs, which are usable by consumers, thus creating value.[35] Creating true value for all consumers of intelligence requires a strategy that goes beyond just creating reports and incorporates network fusion.

Harvard Business School professor Michael Porter argues there are five competitive forces that shape strategy for business. These forces consist of the power of suppliers, consumers, rivals, new entries, and substitutes.[36] Understanding how the five forces shape strategy provides companies with a competitive advantage for profitability. In the government, the goal for understanding these forces is to generate greater public value. By applying Porter's competitive forces to intelligence sharing, we gain insight into how we might strategically structure fusion centers and use network fusion to create a stronger system for homeland security.

SUPPLIERS AND CONSUMERS

Suppliers and consumers have the power to influence what is being reported about terrorist plots, trends, critical infrastructure vulnerabilities, and the possible modality of attack. This information, in turn, will affect decisions made at the strategic, operational, and tactical levels. Too often suppliers of intelligence use their unintentional organizational bias and affiliation with law enforcement to tailor intelligence for prevention, which leaves the first responder community at a major disadvantage for reducing the consequences and the risk of responding to terrorist incidents. Non-traditional consumers of intelligence – those outside of law enforcement – are now requesting different forms of intelligence. Together, suppliers and consumers set new strategic requirements for intelligence.

Here are some examples of how information and intelligence for all hazards are influenced by suppliers and consumers to create public value.

- Policy makers use *strategic intelligence* to decide how best to equip first responders and systematically position resources. An example of such intelligence is the strategic response to a terrorist threat involving toxic industrial chemicals. In India and Iraq, terrorists have used chlorine gas in previous attacks. Understanding this threat on a strategic level and knowing the proximity of industrial chemical plants to Manhattan, the FDNY purchased two 140-foot fireboats, specially designed to protect their crews from chemical, biological, radiological, and nuclear (CBRN) exposure while applying large volumes of water to displace a toxic chemical cloud. These fireboats act as interagency command platforms and are positioned to protect the New York–New Jersey Harbor region from CBRN attacks and maritime threats.
- *Operational intelligence* is used for planning and training against dynamic scenarios for preparedness. The aim of intelligence for operations is to increase public safety by mitigating the effects of attacks. The advantage of multiple disciplines is to develop scenarios to help decision makers deal with uncertainty by considering alternate courses of action.[37] These scenarios are not predictions of the future; rather, they are vehicles that assist people in learning about alternative tactics.[38] Scenario building assists homeland security in identifying the blind spots in its planning process and developing adaptability to deal with uncertainty. One example of this advantage of information sharing involves the analysis of the plot to blow up the Buckeye Pipeline supplying fuel to JFK Airport in New York City. Working closely with multiple agencies in an intelligence briefing, the FDNY provided law enforcement with an alternate location for an attack, which had not been considered and was far more damaging to New York City airports. Maps, geospatial photographs, and a description of the pipeline were given to security partners, indicating the places of greater vulnerability. A competitive advantage over the terrorists was derived from the network interaction of first responders with intelligence experts to create dynamic scenarios that identify vulnerabilities in addition to the investigation.
- *Tactical Intelligence* is the timely and accurate exchange of information during an incident. The power of network fusion was seen on January 15, 2009, when US Airways Flight 1549 made an emergency landing in the icy waters of the Hudson River in New York. By pulling the list of passengers and crew from the control tower at LaGuardia, and tracking and cross-referencing it to the Emergency Medical System network of people taken off the plane, the FDNY was the first to know that all people on this flight were safe and immediately posted this on the HSIN portal, which connected to the emergency management cluster. This information was pulled by many security partners including the DHS National Operations Center, and was given to the secretary of intelligence and analysis to brief the Secretary of DHS and the situation room of the White House.

> Through a fusion of data points, information was shared in real time across a network of homeland security partners.

RIVALRIES

The federal government has invested a great deal of money in creating liaison models for sharing information and intelligence. In 1980, the Joint Terrorism Task Force (JTTF) was formed at the New York Office of the FBI with NYPD. Over the years this joint venture has proved its worth in unraveling terrorist plots and prosecuting cases. It represents the blending of law enforcement agencies for counterterrorism purposes. Similarly, High Intensity Drug Trafficking Area (HIDTA) task force was created to share information. The DHS fusion centers were designed to expand information sharing among unconnected law enforcement and non-traditional consumers of intelligence like the fire and health services. However, many of those overseeing funding are starting to wonder if fusion centers duplicate the function of the law enforcement model of JTTF.

For fusion centers to have a competitive advantage, they will need to develop a distinct core competency and improve their ability to share information faster, smarter, and cheaper. To achieve these goals, public sectors must strategically position their organization to perform different activities from rivals or perform similar activities in different ways.[39] The competitive advantage of fusion centers lies in their capacity to connect to a diverse group of agencies to share intelligence and information not only for prevention and protection, but also for mitigation, response, and recovery. Without such competitive advantage, fusion centers could become extinct with future budget cuts, by not being unique enough to have substantial value. Network fusion is the distinctive core competency of fusion centers, which allows them to connect to multiple disciplines in response to all threats and hazards. The advantage is in the ability to exchange critical information with a variety of senior executives in real time by not requiring them to be co-located. Through network fusion classified information is carried over HSDN and is utilized not only criminal investigations but also for all hazards.

NEW ENTRANTS AND SUBSTITUTES

It is broadly known that New York City is considered a prime terrorist target because of its iconic and economic status. Yet, there are no plans for a NYC fusion center. Analysis reveals several reasons for this lack. First is the rivalry that a fusion center would create between the Joint Terrorism Task Force and High Intensity Drug Trafficking Area task force. Second is the new entrance into intelligence by the robust intelligence and counterterrorism bureaus of the NYPD, which boast of more than one thousand NYPD officers assigned to this work, including officers in several international cities.

The third and most revealing reason is the emergence of network fusion as a substitute for a fusion center in New York City. Through the connectivity of HSDN the same type of classified intelligence that is shared with fusion centers is exchanged directly with NYPD. The police department is able to connect to DHS Intelligence and Analysis, the National Counterterrorism Center (NCTC), and bridge to the FBI and other sources of intelligence. FDNY also was provided with HSDN to connect to similar types of intelligence. In New York City, the police and fire departments that suffered great losses on 9/11 and will respond to the next terrorist event, can now share classified information with each other as well as the DHS, FBI, United States Coast Guard, state fusion center in Albany, NY, and centers and agencies in surrounding states as well. James Surowiecki describes this aggregated knowledge as the "wisdom of crowds," which is characterized by diversity of opinion from independent and decentralized sources.[40] Network fusion provides an alternative means for sharing intelligence with multiple agencies responsible for protecting and responding to terrorism in New York City.

The emergence of network fusion could have a similar effect on co-located models for intelligence (e.g., fusion centers) as Wikipedia had on encyclopedias. After 244

years, the printed copy of the *Encyclopedia Britannica* was replaced by a digital format.[41] Wikipedia, with its ability to leverage the "wisdom of crowds" and Internet availability, proved to be equally accurate, faster, cheaper, and more widely used than the traditional encyclopedia. Fusion centers have the opportunity to embrace the concept of diversity through network fusion and make it their distinctive core competency, thus avoiding irrelevancy.

PARADIGM SHIFT TO NETWORK FUSION

Network fusion is the next evolution in information and intelligence sharing. The objective of this approach is to blend technology with social interaction to understand threats and mitigate their effects. Such emergent systems connect organizations to each other; this alters their behavior in response to the behavior of other organizations in the network.[42] The network effect expands the capacity of organizations to interact with each other and to recognize threats. Collective collaboration represents the establishment of trust and personal relationships among clusters of police, fire, health, and others to exchange information. To create such a shift to a network structure, leaders must prod organizations to develop a new purpose, reengineer operations, build broad support, and restructure responsibility and accountability across organizations.[43]

PURPOSE

Information and intelligence sharing is defined in the *National Preparedness Goals* as "the ability to exchange intelligence, information, data, or knowledge among Federal, state, local or private-sector entities as appropriate."[44] The more connection there is, the greater the chance for discovering novel and critical pieces of information. Unfortunately, this document limits intelligence and information sharing as core goals of prevention and protection only. A new purpose should include a network fusion approach that exchanges information for collective collaboration across all five mission areas:[45]

- *Prevention*: Information/intelligence supports efforts to avoid, prevent, or stop terrorist attacks by connecting to different sources to discover novel elements of threats.
- *Protection*: Information/intelligence enhances homeland security effects against man-made or natural disasters by increasing awareness of vulnerabilities.
- *Mitigation*: Information/intelligence widens the understanding of the threat environment, which enables people to act in time to lessen the effects of a possible event.
- *Response*: Information/intelligence increases situational awareness to support an adaptive response to save life and property in a dynamic event. It also shapes preparedness efforts of training, equipping, and exercising.
- *Recovery*: Information/intelligence will shorten the time needed to restore a community to normal.

The purpose of sharing within a network framework is to facilitate the exchange of useful, relevant, and timely information among the entities that need it, ensuring that the right information will get to key decision makers in a timely manner. Instead of waiting for information to be pushed, network fusion also allows for information to be pulled and returned back to the network in the form of enhanced intelligence. As government agencies move toward a *sociotechnical network* approach for counterterrorism and crisis management, the effectiveness of such an approach will depend on how well they develop technology and collaborative channels of communication with their security partners.

REENGINEERING FOR NETWORK FUSION

In a networked world information moves quickly across a multichannel network that is engineered to connect individuals and groups to create a broad understanding of the threat environment. Without information, organizations cannot fully use their skills to mitigate the threat or the consequences of

terrorism. Fusion centers will only tap a small potential of information sharing by co-locating partners, unless they also connect to other partners through network fusion. New York City's experience with network fusion illustrates how key city agencies can connect with each other as well as to the Department of Homeland Security, state fusion centers, the FBI, and others in the intelligence community.

Reengineering for network fusion requires a sociotechnical approach that uses innovative technology to facilitate collaboration among those tasked with the function of protecting life and property. The following are some concrete steps that leaders can take to develop a system for network fusion and greater information sharing.

Leverage Technology: To participate in network fusion at a classified level, DHS will need to construct a secure room or Sensitive Compartmented Information Facility (SCIF) that is equipped with HSDN, secure computer, secure video conferencing, secure telephone (terminal) equipment (STE), safe, printer, and shredder. The room and the equipment will provide a secure means to receive classified material and briefings.

Identify Personnel: It is critical that organizations identify those in leadership positions who will benefit from classified reports and briefs. Organizations that participate in network fusion must also commit a team that will work together to analyze and produce intelligence products, thus adding value to the intelligence community.

Connect to Intelligence and Information: Having the equipment and personnel to receive classified information is useless, unless the equipment connects to usable intelligence and members have the tools to accomplish their work. Network fusion creates a web-like feature for fusion centers, which connects organizations to secure intelligence sites. To receive access to secure websites, agencies become an adjunct to their state or regional fusion center. In 2012, the New York City Fire Department became an adjunct to the New York State Intelligence Center (the NYSIC is New York's Fusion Center) and took full advantage of resources without having to travel to Albany. The NYSIC and New York City agencies are now partners. In addition, DHS created a Fire Service folder on HSDN for secure documents to be dropped or as a place to request Fire Service input and analysis.

Collaborate with Others: As a sociotechnical network, it is expected that members will interact with one another. By looking at intelligence from different perspectives, new pieces of information can be exchanged via email. However, one of the most valuable means of collaboration is the use of secure video teleconferencing (S-VTC). DHS can provide a bridge for a weekly (or when needed) brief among New York City police and fire departments, the FBI, NYSIC, New Jersey Fusion Center, and other security partners. Since there is no time lost in travel, senior executives are more likely to attend a short fifteen- to twenty-minute brief. Video conferencing not only produces a common operating picture, it also builds relationships and trust among security partners.

Support and Coach: Forming a network fusion team for intelligence sharing requires an additional element that is often overlooked. Richard Hackman, who researched collaborative intelligence at Harvard University, stresses the need for DHS support in terms of education and expert coaching.[46] DHS supports the need for members of an analytical team to receive analyst training to increase their skills. DHS has also provided each fusion center and those that are a part of network fusion with an intelligence and analysis analyst to assist in the information sharing process. Other expert coaching is also a good idea for creating a strong analytical team. At NYPD, highly regarded intelligence experts head the Intelligence Bureau and provide professional guidance. At FDNY, intelligence experts attached to the Terrorism Task Forces and Operations Center supply coaching to foster a higher-level competency.

Network Fusion is a sociotechnical information sharing system designed to encourage collaboration across multiple disciplines by utilizing technology to connect voice, video, and data communications at classified and unclassified levels.
▪ **Leverage Technology** With DHS, construct a secure room or Sensitive Compartmented Information Facility (SCIF) equipped with Homeland Security Data Network (HSDN), computer, S-VTC, STE, safe, printer and shredder.
▪ **Identify Personnel** Identify personnel who would receive classified information and train selected members to be part of an analytical team.
▪ **Connect to Intelligence and Information** Link to Fusion Centers, as an adjunct agency, for access to intelligence and abide by the rules and requirement for handling classified information.
▪ **Collaborate with Others** Partner with other agencies for exchanging information.
▪ **Support and Coach** Receive DHS support, acquire clearances, educate analysts and provide expert coaching for understanding intelligence context.

Table 2: Implementing Network Fusion for Practitioners

ACQUIRING LEGITIMACY AND SUPPORT

Designing networked intelligence not only requires operational capacity to connect networks, but also political support found by proving substantial value for national security.[47] Following the 1993 bombing of the World Trade Center, FDNY Fire Marshal Ronald Bucca (who had a security clearance due to his participation in Army Reserve Military Intelligence), tried to represent the fire department on the Joint Terrorism Task Force but was denied. Based on his access to military intelligence he feared that terrorists would again target the World Trade Center. This fear became a reality on September 11, 2001. Fire Marshal Bucca was killed as he took part in the rescue operation, but his vision for FDNY to be part of the intelligence sharing community was realized. Today, two fire marshals are assigned full-time to the JTTF and high-ranking fire chiefs are given clearances to attend classified intelligence briefings.

The efficacy of horizontal integration of intelligence has been proven in real-life situations. In 2003, there was a credible threat against the George Washington Bridge, which connects New York and New Jersey. A multiagency brief was held concerning the threat and law enforcement devised a plan to protect the bridge. The fire service, a weak tie to law enforcement, brought a perspective of consequence mitigation to the discussion and asked about the vulnerabilities of the structure. The Port Authority of New York and New Jersey sought out its engineers to brief the FDNY fire chief, who inquired about progressive bridge collapse. Once the answer to this serendipitous question was known, it led to an exchange of information, which in turn led to the creation of new preventive guidelines, the revision of preparedness plans, the relocation of special resources for mitigation, the issuance of new response protocols, and the purchase of new equipment.

This horizontal network approach enabled organizations to extend their expertise and presence into areas not traditionally associated with the intelligence community, thus filling a hole in security plans. Including

mitigation and response expanded the aperture of intelligence that previously focused on prevention and protection.

Information sharing does not stop with a single threat. New York City's Department of Transportation (DOT), aware of this threat against the bridges, conducted a study with the US Army Corps of Engineers and private consultants to understand the vulnerability of its major bridges. The study produced thousands of pages of information and was shared with a network of emergency responders including law enforcement. Unfortunately, connecting to volumes of technical engineering reports was useless to emergency responders.

The FDNY asked DOT to support the development of a *First Responder's Bridge Guide*. This was a secure document developed for high-ranking incident commanders to assist in their making critical decisions on the stability of the bridges. Incident commanders were now armed with the knowledge of what would cause a bridge to collapse. This information could be moved wirelessly across an encrypted network to the decision makers in real time. The result of this project demonstrates the power of multi-agency support for reengineering information structures to connect different perspectives about the same threat and collaborate to produce a fusion-supported decision making document for first responders.

In 2006, the DHS chief intelligence officer, Charles Allen, testified in front of Congress: "to prevent and counter potential terrorist attacks and other threats to the homeland, first responders and frontline law enforcement officers must be armed with the information that will enable them first to recognize and then defeat the threat."[48] This testimony publicly recognized first responders as a legitimate part of the intelligence networks, which will enable them to better fulfill their role in homeland security.

THE FIRE SERVICE AND NETWORK FUSION

On the West Coast, California's Terrorism Early Warning Group, which was the predecessor to fusion centers, invited the Los Angeles County Fire Department to place battalion chiefs as members of this team. In Washington, DC, the Metropolitan Police Department refused to attend a security briefing at the Capitol unless a fire chief from DC Fire Department was invited to attend. These efforts by a few forward looking individuals paved the way to recognizing the fire service as a security partner.

Under the direction of Charles Allen, the Office of Intelligence and Analysis (I&A) started working directly with the FDNY to form an information and intelligence-sharing environment for the fire service.[49] By aligning the FDNY with DHS efforts to improve information flow, the Fire Service Intelligence Enterprise (FSIE) was created, which provided a template for DHS to share information among major city fire departments.[50] This initiative adheres to the mandate articulated in the Intelligence and Terrorism Reform Act and the presidential directives to create an information-sharing environment across the country.[51]

In April 2010, the DHS integrated the fire service into fusion centers and added an annex for the fire service into the baseline capabilities for Major Urban and State Fusion Centers.[52] The purpose was to establish a direct information conduit between the United States Department of Homeland Security and the fire service. Through the sharing of pre-incident intelligence and real-time incident updates, information support for both the first responders and DHS is enhanced.

In 2011, I&A, with Caryn Wagner's leadership, provided FDNY with HSDN for greater intelligence sharing, which was the foundation for network fusion. In addition, the FDNY furthered the legitimacy of the fire service within the Department of Homeland Security by setting a series of intelligence requirements. Fearful that terrorists might continue to use fire as a tactic, the FDNY set detailed requirements for the intelligence community to search for possible chatter on this topic. Discovery of such information would indicate advancements in the use of fire as a weapon.

In 2012, a memorandum of understanding for network fusion was signed between FDNY and the New York State Intelligence Center (NYSIC) making FDNY an adjunct member of

New York State's fusion center. Legitimacy is now attained by connecting to a platform for exchanging classified and unclassified information in real time with senior officials to prevent, mitigate, and respond to a range of threats. The benefit of network fusion is that information is not only pushed through briefings, but now can be pulled for a greater understanding of the threat environment. Connecting to additional fusion centers and other first responder groups within those fusion centers attains further benefits of network fusion.

Rodrigo Nieto-Gómez argues that when faced with new combinations of technologies for terrorism, homeland security must take a different approach to security. He recommends bringing small groups together for a specific purpose, which forms "ad-hocratic" organizations.[53] Just such an ad hoc committee was assembled with FDNY in response to a detailed article in the ninth issue of *Inspire Magazine* (2012) that describes how to use improvised incendiary devices to set wildland fires. Taking advantage of network fusion, DHS Intelligence and Analysis asked FDNY, New York State's fusion center, and others to collaborate in writing an awareness document of a potential terrorist tactic that uses "fire as a weapon." Collaborative analysis discovered that such tactics might also be used against large populations in high-rise buildings. The fusing of information and network collaboration of ad hoc committees illustrates the fire service's contribution to the intelligence process and the adaptability of an emergent intelligence network for understanding the threat environment.

RESPONSIBILITY AND ACCOUNTABILITY

The emergence of networks prompts organizations to redefine their core responsibilities, from managing only their own people and programs to coordinating resources and information with other agencies for producing public value.[54] The focus now is on the mission outcome of public safety and not simply on an agency's outputs. Integrating the concept of network fusion for information and intelligence sharing into organizations requires a management system capable of dealing with "multiple locations, several different cultures, often different and incompatible information technology systems, and sometimes deliberate withholding of important information when partners perceive they are in competition with one another, or simply to protect bureaucratic turf."[55] The goal of network fusion is to connect agencies as a force multiplier for gathering, analyzing, and disseminating information into the core mission of homeland security.

Homeland security's use of network fusion represents a balance between anticipation and resiliency. A strategy of anticipation is the creation of ties among first responders, law enforcement, and the intelligence community to better understand the threat environment for prevention and protection before an event occurs. A strategy of resilience is the strengthening of those ties for mitigation, effective consequences management, and quicker recovery if attacks were to take place.

The FDNY has pushed to enhance information and intelligence sharing capabilities by forming networks, strengthening ties, and using technologies to educate and train its members and to work with other agencies. The results of these efforts were evident on May 1, 2010, when a vendor alerted police to a possible vehicle fire in New York's Times Square. As police directed them to the car, the firefighters noticed, "something did not look right."[56] The owner of the SUV was nowhere to be found; there was white smoke rather than black; a handheld thermal camera showed no sign of fire; and an odor of fireworks emanated from the rear of the vehicle. Firefighters asked police to run the license plates. When the plates came back unregistered, the fire lieutenants concluded that the fire could be a car bomb. The police and fire officers overcame their organizational biases and collaborated with each other, which led to a decision to evacuate people from the area. This decentralized approach worked because it allowed organizations to deal with uncertainty by having multiple agents (street vendors, firefighters, and police officers) fuse information to find the best solution.[57] Later reports determined that the SUV had the

potential of being a powerful terrorist bomb with lethal consequences. Organizations and individuals were accountable to one another to share information and collaborate.

POLICY FOR NETWORK FUSION

Network fusion is composed of flexible and innovative systems capable of adapting to the complexity of today's threat environment. Organizations that can rapidly exchange intelligence and critical information will operate more effectively than less prepared organizations at complex incidents.[58] Failure to develop network fusion will leave first responders and fusion centers to combat terrorism with limited information. Overcoming organizational bias and consequence mitigation neglect will foster a synergistic network that combines the knowledge of law enforcement and the intelligence community with first responder organizations to form a robust information and intelligence-sharing platform. Network fusion does not replace fusion centers, but enhances their capability to share information and intelligence. The stirring images of 9/11 and a system still blinking red with stovepipes that failed to share information illustrate the need for better information and intelligence sharing among agencies before and during a crisis.

Network fusion is an emergent process that connects the unconnected by bridging gaps in information and intelligence sharing. The challenge is to get those who control information to see that hoarding information is not a way of attaining power; sharing information with the unconnected attains that power in a networked world. Network fusion extended to other at-risk cities and organizations will enhance homeland security and fusion centers' efforts by making them faster, smarter, and more cost-effective in exchanging information and intelligence. Network fusion is faster because information and intelligence can be exchanged directly with many; smarter because there is a pull and push of different perspectives; and more cost-effective because DHS does not have to pay for representatives to be co-located. The question we must face today is whether we have taken sufficient steps to ensure a policy of network fusion to repair an information sharing system that was "blinking red."

ABOUT THE AUTHOR

Joseph Pfeifer *is an assistant chief for the New York City Fire Department. During his career, he has commanded some of the largest fires and disasters in the department's history and was the first chief at the World Trade Center on the morning of September 11, 2001. He founded and directs the FDNY Center for Terrorism and Disaster Preparedness and responds to major incidents. He is also a visiting instructor for the Center of Homeland Defense and Security at the Naval Postgraduates School, a senior fellow at the Combating Terrorism Center at West Point, and a fellow at the Ash Center for Democratic Governance and Innovation at Harvard University, where he speaks on crisis leadership and information sharing networks. He holds master degrees from the Harvard Kennedy School, Naval Postgraduate School and Immaculate Conception. He is published in various books and journals and can be contacted at: joe_pfeifer@hks.harvard.edu.*

[1] Additionally supported by *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W. W. Norton & Company, 2004), 275, 309.

[2] Amy B. Zegart, *Spying Blind: The CIA, the FBI and the Origins of 9/11* (Princeton: Princeton University Press, 2007), 13.

[3] T. P. M. Barnet, *The Pentagon's New Map: War and Peace in the Twenty-first Century* (New York: Berkley Press, 2005).

[4] Stephen Cohen and William Eimicke, *The Responsible Contractor Manager: Protecting the Public Interest in an Outsourced World*. Washington, DC: Georgetown University Press, 2008. 42.

[5] Ibid., 40.

[6] Stephen Goldsmith and William D. Eggers, *Governing by Networks: A The New Shape of the Public Sector (*Washington, DC: Brooking Institution Press, 2004), 8.

[7] Ibid., 28.

[8] Christopher Bellavita, "Changing Homeland Security: Shape Patterns, Not Programs," *Homeland Security Affairs* II, no. 3 (October 2006): 16, http://www.hsaj.org/?fullarticle+2.3.5

[9] Jeff Jarvis, *What Would Google Do?* (New York: HarperCollins Publisher, 2009), 103.

[10] John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica, CA: Rand Corporation. 2001), 15.

[11] Markle Foundation Task Force, *Mobilizing Information to Prevent Terrorism* and *Creating a Trusted Information Sharing Network for Homeland Security* (New York: Markle Foundation, 2006 and 2003).

[12] Karl E. Weick and Kathleen M. Sutcliff, *Managing the Unexpected: Assuring High Performance in an Age of Complexity* (San Francisco: Jossey-Bass, 2001), 60.

[13] An FDNY lieutenant's annual salary (without overtime) is $98,078. This figure plus 101 percent fringe equals $202,028. Five people are needed to cover 24 hours a day, seven days a week, which equals a million dollars for one position. Higher ranks would cost hundreds thousands more.

[14] David Tucker, "Terrorism, Networks, and Strategy: Why the Conventional Wisdom is Wrong," *Homeland Security Affairs* IV, no. 2 (June 2008): 7.

[15] D. Lazer and M.C. Binz-Scharf, "It Takes a Network to Build a Network" In V. Mayer Schonberger and D. Lazer, eds., *Governance and Information Technology: From Electronic Government to Information Government* (Cambridge, MA: The MIT Press, 2007), 267.

[16] J. Richard Hackman, *Collaborative Intelligence: Using Teams to Solve Hard Problems* (San Francisco: Bernett-Koehler, 2011), 32.

[17] Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-first Century* (New York: Picador, 2007), 210.

[18] Presidential Memorandum, *Guidelines and Requirements in Support of the Information Sharing Environment* (Washington, DC: The White House, December 16, 2005), http://www.whitehouse.gov/news/releases/2005/12/20051216-10.html.

[19] United States Government Accountability Office, GAO-06-385, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information* (Washington, DC: Government Printing Office, 2006), 14.

[20] Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Government Printing Office, 2007), 41; Department of Homeland Security, *National Response Framework* (Washington, DC: Government Printing Office, 2008); Department of Homeland Security, *National Preparedness Goals* (Washington, DC: Government Printing Office, 2011).

[21] Louise K. Comfort, "Rethinking Security: Organizational Fragility in Extreme Events," *Public Administration Review* (September 2002), 98–107.

[22] Ted Lewis, *Bak's Sand Pole: Strategies for a Catastropic World*, (Williams, CA: Agile Press), 2011.

[23] Paul Cilliers, Complexity and Postmodernism: Understanding Complex Systems, (New York: Rouledge, Taylor and Francis Group, 1998), p.97.

[24] Ronald Burt, *Structural Holes: The Social Structure of Competition,* (Cambridge: Harvard University Press, 1992), 28.

[25] Ronald Burt, "Structural Holes versus Network Closures as Social Capital" in Nan Lin, Karen Cook, and Ronald Burt, eds., *Social Capital: Theory and Research* (New Brunswick: Aldine Transaction, 1 June 2001), 35.

[26] Burt, *Structural Holes*, 20–21.

[27] Ibid.

[28] Morten T. Hansen, "The Search-Transfer Problem: The Role of Weak Ties in Sharing Knowledge Across Organizational Subunits," *Administrative Science Quarterly* 44, no. 1 (March 1999): 82–111.

[29] *9/11 Commission Report*, 416.

[30] Joseph Pfeifer, "Understanding How Organizational Bias Influenced First Responders at the World Trade Center," in Bruce Bongar, Lisa M. Brown, Larry E. Beutler, James N. Breckenridge and Philip G. Zimbardo, eds., *Psychology of Terrorism* (New York: Oxford University Press, 2007), 207–215.

[31] Karl Wieck, *Sensemaking in Organizations* (London: Sage Publications, 1995), 102.

[32] Ibid.

[33] A summary of the research and theoretical perspectives regarding social biases focused around social identity and intergroup biases can be found in the overview chapter by the social psychologist Kay Deaux, "Social Identification," in E. T. Higgins and A. W. Kruglanski, eds., *Social Psychology: Handbook of Basic Principles*, (New York: Guilford Press, 1996), 777–798; and Philip Zimbardo, "A Situationist Perspective on the Psychology of Evil," in A. Miller, ed., *The Social Psychology of Good and Evil* (New York: Guilford, 2004).

[34] New Jersey State Police, *Practical Guide to Intelligence-Led Policing* (New York: The Manhattan Institute, 2006), 6.

[35] Mark M. Lowenthal, *Intelligence from Secret to Policy* (Washington, DC: CQ Press, 2003), 42.

[36] Michael M. Porter, *On Competition* (Boston: A Harvard Review Book, 2008.), 3-33.

[37] Peter Schwartz, *The Art of the Long View* (New York: Doubleday Dell Publishing Group, Inc., 1991), 4.

[38] Ibid., 6.

[39] Porter, *On Competition,* 38.

[40] James Surowiecki, *The Wisdom of Crowds* (New York: Doubleday Publishing, 2004).

[41] Julie Bosman, "After 244 Years, Encyclopedia Britannica is Going Out of Print," *The New York Times*, March 13, 2012, http://mediadecoder.blogs.nytimes.com/2012/03/13/after-244-years-encyclopaedia-britannica-stops-the-presses/?pagemode=

[42] Steven Johnson, *Emergence: The Connected Lives of Ants, Brains, Cities, and Software* (New York: Scribner, 2001), 88.

[43] Mark H. Moore, *Creating Public Value: Strategic Management in Government* (Cambridge, MA: Harvard University Press, 1995), 239.

[44] Department of Homeland Security, *National Preparedness Goals* (Washington, DC : Government Printing Office 2011), 6.

[45] Adapted from drafts of Department of Homeland Security, *National Prevention Framework* (Washington, DC: Government Printing Office, 2012).

[46] Hackman, *Collaborative Intelligence,* 52.

[47] Moore, *Creating Public Value*.

[48] Charles Allen, "The Homeland Security Information Network: An Update on DHS's Information Sharing Efforts," at the Subcommittee of the House of Representatives Testimony on the Hearing of the Intelligence, Information Sharing and Terrorist Risk Assessment, Washington, DC, September 13, 2006; Statement red into the records and retrieved on Nov.20, 2011 from http://www.fas.org/irp/congress/2006_hr/091306allen.pdf .

[49] In the fall of 2006, Deputy Assistant Chief Joseph Pfeifer, FDNY's chief of counterterrorism, met with Mr. Allen and guided a team from FDNY's Center for Terrorism and Disaster Preparedness to work with I&A in developing the FSIE initiative.

[50] A special DHS-FSIE conference was held in New York, on September 6-7, with major city fire chiefs. Then chief of the FDNY, Salvatore J. Cassano, invited fire chiefs from Baltimore; Boston; Chicago; Denver; Houston; Las Vegas; Los Angeles City; Los Angeles County; Miami; Miami-Dade County; Philadelphia; Phoenix; Seattle; and Washington, DC, to attend a conference on intelligence sharing.

[51] George Bush, Presidential Memorandum, *Guidelines and Requirements in Support of the Information Sharing Environment* (Washington DC: The White House, 2005).

[52] Department of Homeland Security, *Fire Service Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Fusion Centers* (Washington, DC: Government Printing Office, 2010).

[53] Rodrigo Nieto-Gómez, "The Power of 'the Few': A Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment," *Homeland Security Affairs* 7, Article 18 (December 2011): 13. http://www.hsaj.org/?article=7.1.18

[54] Goldsmith and Eggers, *Governing by Networks,* 24.

[55] Cohen and Eimicke, *The Responsible Contractor Manager,* 39.

[56] Interview with Lieutenant John Kazans from Ladder Company 4, about his response to the attempted Times Square Bombing Incident of Faisal Shahzad on May, 1, 2010.

[57] Raphael Sagarin, "Natural Security for a Variable and Risk-filled World," *Homeland Security Affairs* 6, no. 3 (September 2010), http://www.hsaj.org/?article=6.3.4

[58] Mica R. Endsley, Leonard D. Hollder, Bruce C. Leibrecht, Daniel J Garland, Richard L. Wampler, and Michael D. Matthews, *Modeling and Measuring Situational Awareness in the Infantry Operational Environment* (U.S. Army Research Institute for the Behavioral and Social Sciences, 2000), 17.