June 2012

Counterterrorism Intelligence:

Fusion Center Perspectives

The George Washington University Homeland Security Policy Institute

CTISR

Counterterrorism Intelligence Survey Research

Parati! Be Ready!

Frank J. Cilluffo

Joseph R. Clark

Michael P. Downing

Keith D. Squires

THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY POLICY INSTITUTE

Frank J. Cilluffo has served as Director of the Homeland Security Policy Institute since joining The George Washington University in April 2003. He is also an Associate Vice President and leads GW's homeland security efforts on policy, research, education, and training. The Institute's recent policy and research agenda covers a wide range of national and homeland security matters, including counterterrorism, counter-radicalization & counter-narrative efforts, cyber threats & deterrence, transportation security, CBRN terrorism, intelligence, national resilience, emergency management, and the nexus of crime and terrorism. Prior to founding HSPI, Cilluffo served as Special Assistant to the President for Homeland Security at the White House.

Dr. **Joseph R. Clark** is a policy analyst at HSPI. His primary research interests include military doctrine, national security strategy, counterterrorism policy, and organizational learning. He serves as the research director for HSPI's Counterterrorism and Intelligence Task Force. In addition, he leads HSPI's Counterterrorism Intelligence Survey Research (CTISR) program. Clark has written on counterinsurgency doctrine, the need to engage moderate members of the Taliban in political dialogue, piracy, and the US Army's ability to innovate doctrine in the face of strategic failure in Vietnam and Iraq.

Deputy Chief **Michael P. Downing** is the Commanding Officer of the Los Angeles Police Department's Counter-Terrorism and Special Operations Bureau where he leads five operational divisions: Major Crimes Division, Emergency Services Division, Metropolitan Division, Air Support Division, and Emergency Operations Division. These divisions include the Anti-Terrorism Intelligence Section, Criminal Investigative Section, Organized Crime, Surveillance Section, Hazardous Devices Section, Operation Archangel, LAX Bomb K-9 Section, Special Weapons and Tactics (SWAT), Mounted Unit, Underwater Dive Team, and Emergency Preparedness and Response. Downing is also a member of the Executive Board of the Los Angeles Joint Regional Intelligence Center (JRIC) and a Senior Fellow at HSPI.

Colonel **Keith D. Squires** is the Deputy Commissioner of the Utah Department of Public Safety. He also serves as the Governor's Homeland Security Advisor responsible for Utah's Homeland Security and Emergency Management Division. He provides additional oversight for the State Bureau of Investigation, the Statewide Information and Analysis Center and the State Crime Lab. In 2007, he was tasked with designing and establishing Utah's fusion center. Col. Squires began his career with the Utah Department of Public Safety in November of 1989 as a Utah Highway Patrol trooper and promoted through all ranks of the agency. He has previously served as the director of the State Bureau of Investigation, deputy director of the Utah Division of Homeland Security and assistant superintendent of the Utah Highway Patrol.

The authors would like to thank the National Fusion Centers Association for its help with this survey, especially Ross Ashley and Mike Sena for their advice and feedback. They would also like to thank HSPI intern Anna Mae Gibson for her exceptional editing and support.

This research was made possible by the generous support of
The George Washington University and the Ahmanson Foundation.

Founded in 2003, ***The George Washington University Homeland Security Policy Institute (HSPI)*** *is a nonpartisan "think and do" tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation.*

Research Brief Volume 2, Number 1. Washington, DC; Homeland Security Policy Institute.

ISBN: 978-0-9839904-4-4

2001

On September 9th, shortly after midnight, Maryland State Police Trooper Joseph Catalano pulls over a red Mitsubishi. The car was traveling 90 miles per hour in a 65 mile per hour northbound stretch of Interstate 95. The trooper's dashboard mounted camera and microphone record the eight minute traffic stop.

Trooper Catalano takes the driver's Virginia license and the rental car's registration information and walks back to his cruiser. He asks dispatchers to check whether the car has been reported as stolen. It has not. There is no reason to hold the driver. The incident appears to be nothing but a routine traffic stop. The driver is calm and polite.

Trooper Catalano walks back to the red Mitsubishi. He hands the driver a ticket for $270 and tells him he needs to sign it. The driver signs the ticket and hands it back. "You're free to go" Catalano tells the driver before returning to his patrol car.

As he returns to his cruiser, Catalano is unaware that the driver, Ziad Jarrah, is on a Central Intelligence Agency watchlist. Fifteen seconds later he watches the red car and its driver disappear into the night.

Two days later, Ziad Jarrah boards United Flight 93 and takes his position in seat 1B — the closest to the cockpit.[1]

2011

On June 25th, around 6:00pm, officers from the Colorado State Patrol arrest the driver of a green Toyota pickup truck who had been driving erratically. When the police attempted to pull him over the driver fled. He eventually crashes his truck on Highway 103 in Clear Creek County.

Colorado State Police arrest the driver for reckless driving, driving drunk, having an open alcohol container in the vehicle, and felony menacing. As they process the driver, and input information about his pickup, they learn from the Colorado Information Analysis Center that the green Toyota matches one used in the attempted bombing of a bookstore in Lakewood, Colorado.

A week later, federal authorities charge the driver — David Lawless — with planting a series of explosives around the Colorado Mills Mall in Lakewood.

The arrest and prosecution of Lawless for the attempted bombings has been directly supported by the Colorado Information Analysis Center. The fusion center successfully gathered and disseminated information from private businesses, local police, state authorities, and the Federal Bureau of Investigation.

Lawless is scheduled to stand trial in 2012.[2]

Preface

In marking the tenth anniversary of the 9/11 attacks, the US Department of Homeland Security noted that: "Fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities."[3] We agree, this is the promise behind the concept of the fusion centers. Yet, the research contained in this report indicates that the promise has yet to be fulfilled.

A decade after 9/11, the US increasingly faces blended threats. Our homeland security structures must be prepared to address foreign directed or inspired attacks, homegrown jihadi plots, or hybrid threats that mix these elements with new technological resources — including those in cyberspace, where computer network attacks and computer network exploits can be leveraged by our adversaries. Meeting the challenges of this evolving threat environment requires a robust national intelligence enterprise. It requires that the fusion centers act as more than hubs for the circulating of information. It requires that those who work in the centers be invested with the analytical capabilities and skill-craft necessary to fuse disparate pieces of information into risk-based threat assessments, explicit warnings, and actionable intelligence. Data from those working in the fusion centers suggests such investments have yet to be made. From the perspective of those in the centers, our fusion centers excel at the dissemination of information, yet lack the analytical capabilities needed to fulfill their mandate to assess the local implications of threats.

The US' national network of fusion centers are an important part of our national intelligence enterprise. With an increased investment in the analytical training afforded to those in the centers, and with a retooling of the professional incentive structures used to evaluate and manage their performance, the fusion centers can fulfill their promise and become true assets to homeland security. Although we are suggesting that additional resources be allocated, we recognize the reality of existing budgetary constraints. The arguments presented here are not ones for spending blindly. Investments in the capabilities of the fusion centers could (and should) build on existing successful efforts within the intelligence and law enforcement communities. Outside the fusion center network, the Interagency Threat Assessment and Coordination Group (ITACG) provides a concomitant example. By working to support the development of analysts, supplying guidance in the construction of tailored intelligence products, and facilitating access to classified information, ITACG provides one model and set of resources for moving the fusion centers forward. Future efforts should follow a similar pattern and provide concrete support to specific centers in an effort to help grow and expand their endogenous analytical capabilities.

Those working in the fusion centers have important and valuable insights. They are to be commended for their dedication and hard work in both the service of their communities and this country. Furthermore, using the perspective of those working in our national network of fusion centers it is possible to get a

practitioner level view of existing threats, emergent risks, and our level of preparedness in addressing them. It is also possible to evaluate how well the fusion centers are fulfilling their mandate to overcome the information sharing and intelligence shortcomings of our pre-9/11 homeland security structures. These last two points get to the primary objective of the research contained in this report — to extract and build upon the lessons and insights of practitioners.

It is impossible to meet those objectives with a single survey or report. What is possible, however, is to begin to focus attention on the value of practitioner level perspectives and to begin to draw lessons from what they have to teach us. This report is a step in the Homeland Security Policy Institute's commitment to doing just that.

In support of efforts to construct and continuously improve our national intelligence enterprise, the Homeland Security Policy Institute at The George Washington University has begun the **Counterterrorism Intelligence Survey Research (CTISR)** program as a long-term endeavor. This program represents an attempt to systematically collect data from counterterrorism professionals at all levels of government. CTISR will measure *practitioner* perceptions of the threat and the systems by which they gather and evaluate information about it. With such practitioner-level data, it will be possible to reach an empirically derived understanding of the evolving threat posed by terrorism, its relationship to criminal activities and other societal dangers, and the status of collaborative and cooperative efforts to combat it. In short, with such data it will be possible to bring a little science to the art of counterterrorism intelligence. Only then, can the limited resources available for targeted programs and projects be utilized in a fashion that can yield the greatest benefits to American security.

CTISR is, at its core, interested in the national counterterrorism intelligence enterprise of the United States — by which, is meant the processes and mechanisms through which counterterrorism relevant information is collected and analyzed by government entities and practitioners at the local, state, tribal, regional, and federal levels. Such processes and mechanisms, as well as the individual and organizational behaviors that develop and sustain them, represent a network of activities that attempt to determine threat domains by detecting and evaluating risks to the safety and security of the people of the United States — while at the same time protecting the civil rights and civil liberties that Americans cherish and that define the political culture of the United States.

Frank J. Cilluffo

Joseph R. Clark

Michael P. Downing

Keith D. Squires

Bottom Line Up Front

A February 2012 HSPI poll of individuals working in the (then) seventy-two state and major urban area fusion centers found the following:

- On a scale of 1 to 10, in which 10 equals "high threat," slightly more than forty-nine percent of respondents stated that terrorism posed a threat of 6 or greater in their region.
- A majority of respondents, slightly more than seventy-eight percent, expect the threat of terrorism to persist. No one indicated that they expect it to diminish.
- When asked who posed the greatest terror threat, a majority of respondents, more than sixty-five percent, answered homegrown jihadi individuals or organizations.
- A minority of respondents, slightly more than twenty-nine percent, reported that their center conducted regional threat assessments on a yearly basis.
- Small majorities, slightly more than fifty-two percent and slightly more than fifty percent, stated that their centers had effective strategies for gathering information about the capabilities and intentions of those they identified as posing the greatest threat in their region.
- When asked who they believe to be the most important source for counterterrorism information, law enforcement was the most common answer (given by forty-eight percent of respondents). The FBI's Joint Terrorism Task Forces (JTTFs) were the second most common answer (given by twenty-six percent of respondents.)
- A majority of respondents, slightly more than sixty-nine percent, reported that they send information to the major law enforcement entities in their jurisdiction every day.
- A majority of respondents, slightly more than fifty-three percent, stated that the owners of critical infrastructure in their region were not part of their fusion center.
- A majority of respondents, slightly more than fifty-one percent, listed analytical capabilities as the functional area in which their center needs the most improvement.
- A minority of respondents, slightly less than forty-six percent, stated that the US' homeland warning system was adequate.
- A majority of respondents, slightly more than sixty-five percent, believe their center has relatively weak capabilities in regard to the gathering, receiving, and analyzing of cyber threats.
- Law enforcement remains the operational focus of most fusion centers. Sixty-three percent of respondents listed law enforcement as their center's most important function. (Approximately twenty-eight percent identified counterterrorism as their center's most important function — which naturally includes law enforcement functions.)

Results from HSPI's survey suggest that the fusion center system is defined by the professional backgrounds of the individuals that staff them — not the events that triggered their creation. Those working in the fusion centers appear to recognize this and openly express a need for the personnel investments that would allow them to fulfill the promise and mandate under which their centers were established. Given these last two points, questions naturally arise about the quality and quantity of the local, state, and federal support being provided to the centers.

Background

According to guidelines published by the Department of Homeland Security (DHS) and Department of Justice (DoJ), "A *fusion center* is defined as a 'collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.'"[4]

DHS recognizes seventy-seven state-designated and major urban area fusion centers. This number represents a recent (March 2012) increase from the seventy-two recognized centers that existed at the time this research was conducted.[5]

Fusion centers are primarily staffed by state and local personnel, although they may occasionally have representatives from DoJ or DHS entities — including the Federal Bureau of Investigations (FBI), the Drug Enforcement Agency (DEA), Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP).

Fusion center staffs range in size from four individuals to more than one hundred. Regardless of any federal presence or funding, fusion centers are owned and operated by state and local jurisdictions — each of whom tailors the mission focus and activities of their center to the specific needs of their jurisdiction.[6]

Each fusion center is not, however, a *sui generis* expression of purely local needs. Individually and collectively they are the product of the terror attacks of September 11, 2001 — and the resulting investigations that identified the lack of information sharing and environmental awareness as key factors that allowed a growing threat to go undetected.[7] The fusion centers are, in fact, intended to be a local, state, regional, and national assets. A point illustrated by the fact that the 2010 National Security Strategy continues to highlight the role of fusion centers in preventing acts of terrorism and the importance of leveraging intelligence, law enforcement, and homeland security capabilities.[8]

Each fusion center was established to "receive, analyze, gather, and share threat-related information." Individually and collectively, the fusion centers exist to provide early warning of threats from criminal and terror activities, to support emergency management, and facilitate the identification, assessment, and protection of critical infrastructure.[9] To summarize, the fusion centers exist as a network for detecting threats, sharing information, providing warning, and coordinating responses.

> ***"The ultimate goal is to provide a mechanism where law enforcement, public safety, and private sector partners can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. The fusion center is this mechanism; it is key to ensuring the flow of threat- and crime-related information between local, state, regional, and federal partners."***
>
> **— "Fusion Center Guidelines"[10]**

Fulfillment of the fusion center mandate is predicated on the collection of information by public and private sector entities at the local, state, regional, and federal levels. This information, in either raw or processed forms must be gathered from disparate sources and merged, correlated, extracted, deconflicted, and refined. This is the fusion process. From it, the development of a rich picture of various threat domains becomes possible.[11]

Data fusion increases the likelihood of seeing trends and patterns that may not be observable from any single perspective, source, or organization. Although the integration of data from entities at the local, state, and federal levels is a necessary step in the fulfillment of each fusion center's mission — it is not a sufficient step for doing so.

Ultimately the fulfillment of the mandate and promise of fusion centers rests on skilled analysis. Without collection there would be nothing to analyze — yet, it is analysis that turns information into actionable intelligence. The guidelines issued by DoJ and DHS state that fusion centers will provide four key benefits. They are as follows.

- "Allow local and state entities to better forecast and identify emerging crime and public health trends."
- "Support multidisciplinary, proactive, risk-based, and community-focused problem solving."
- "Provide a continuous flow of intelligence to officials to assist in developing a depiction of evolving threats."
- "Improve the delivery of emergency and nonemergency services."

To be completed successfully, each of these tasks requires substantial analytical skill. Analysts digesting new information must place such data within the context of existing beliefs about the relevant subject matter. Analysts must also use fused data to identify and prioritize risks within their center's jurisdiction.

Such prioritization has always been important — it drives resource allocation and operational deployments. It helps answer questions in regard to where, when, and with what private and public sector actors observe emerging or existing threats. In a period of increasingly limited budgets, however, data based prioritization also provides insights for making the most informed spending choices possible.[12]

Collection and analysis, however, are still not enough. Even the most prescient intelligence is worthless if it stays locked in a drawer. Collection and analysis must eventually lead to the production and dissemination of intelligence products. Information from the fusion centers only becomes actionable intelligence if it gets to the right people at the right time. This requires each center achieve the following.

First, once intelligence has been developed, center personnel must identify the appropriate consumer audience or audiences. This can be done by asking who are the individual and organizational consumers, public and private, who are responsible for prevention, response, and consequence management for the given threat.

Second, with the consumer in mind, center personnel must format the intelligence in such a manner as to increase the likelihood that the consumer audience(s) will receive, digest, and act on it. Lack of relevancy (in regard to a specific consumer's needs) is often a complaint associated with dismissing the overall value of a fusion center's intelligence products. Careful consideration must be given in identifying how information may impact a specific jurisdiction. Thought must be given to the mode of delivery (as a warning of new developments, raw information, the fulfillment of a specific request, or a full report, etc.) as well as the means of delivery (as an email attachment, posting to a secure server or shared database, the sending of a hard copy, or even an alert delivered via telephone, etc.). Each of these factors affect who sees what, when, and whether they digest the information.

Third and finally, center personnel must decide when to send intelligence — they must balance between

ripeness and timeliness. Two interrelated questions help decide this balance. How likely is it the information would affect the consumers' behavior, operations, or posture? How likely is it the information would affect the consumers' window of opportunity for action?

These primary functions — collection (be it by the gathering or reception of information), analysis, production, and dissemination — represent the *raison d'êtra* of each fusion center. They are the foundation of each center's operational capabilities. In 2010 at the National Fusion Center Conference in New Orleans, fusion center directors and federal partners encapsulated these primary functions in four Critical Operational Capabilities (see the box below). These critical capabilities were to be prioritized by each center.[13]

Critical Operational Capabilities (COCs)

COC 1: Receive — Ability to receive classified and unclassified information from federal partners.

COC 2: Analyze — Ability to assess local implications of threat information through the use of a formal risk assessment process.

COC 3: Disseminate — Ability to further disseminate threat information to other state, local, tribal, and territorial entities and private sector entities within their jurisdictions.

COC 4: Gather — Ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners as appropriate.

With the death of Osama Bin Laden, and according to some estimates the weakening of the al-Qaeda organization, it might be tempting to question the utility or necessity of a national network of fusion centers. That would be a mistake, for the threat domains faced by local, state, and federal authorities continue to evolve. Even if the specific threats that precipitated the creation of the fusion centers disappears, others including threats from drug cartels, homegrown jihadists, state sponsors of terror, cyber threats, and others will take their place. The fusion function will continue to be necessary.[14]

The last few years have seen a dramatic increase in homegrown terrorism. Today, questions regarding cyber threats loom. Over the horizon there are increased concerns about state-sponsored threats from countries like Iran.[15] Each of these potential threat domains illustrate the interconnected and mutual dependence issues that define the intelligence enterprise of the 21st century. Local, state, and federal officials cannot be fully aware of the threats faced within their jurisdictions without information about events and actors that lie within other jurisdictions. The role of the fusion centers as intelligence hubs continues to be an important one.

The fusion centers were created to develop a better understanding of domestic threat domains. When they fulfill their potential, the fusion centers can deliver anticipatory intelligence that greatly reduces the level of risk faced by Americans at all levels of governance.

A decade after the precipitating events that led to the creation of the fusion centers, two interrelated questions present themselves. To what degree are the fusion centers fulfilling their potential? To what degree are they operating in such a manner as to provide actionable intelligence to the appropriate public and private consumers? To answer such questions, HSPI turned to those working in the

fusion centers to capture their perspectives and leverage their insights.

The perceptions of those working in the fusion centers are vitally important in addressing fusion center operations and the status of the US' national intelligence enterprise. Fusion center workers are best located to evaluate the degree to which their centers can gather information, analyze it, and disseminate intelligence. They have the ability to provide insights into the levels of access they have to local, state, and federal sources of information. They also have the ability to evaluate the degree to which they have the analytical tools they need. Furthermore, they are well positioned to evaluate the mechanisms by which intelligence is disseminated and warnings are issued.

There is one additional reason why the perceptions and insights of those working in the fusion centers are critically important — if the fusion centers are operating as envisioned, fusion center workers ought to have the most well informed understanding of the threats faced in their region. Their perceptions of the threat domain provide insights into their center's ability to detect and warn of emerging threats against the safety and security of the United States.

Methods

In January and February 2012, a seventy-eight question self-completion survey was administered by the Homeland Security Policy Institute (HSPI) to individuals working in the (then) seventy-two state and urban area fusion centers. Seventy-one individuals voluntarily took the survey.

Through a partnership with the National Fusion Center Association (NFCA), an invitation to participate in the survey was extended to every individual working in a fusion center. The NFCA is a private non-profit professional organization made up of and representing those working in the fusion centers. The NFCA's mission is: "To represent the interests of state and major urban area fusion centers, as well as associated interests of states, tribal nations, and units of local government, in order to promote the development and sustainment of fusion centers to enhance public safety; encourage effective, efficient, ethical, lawful, and professional intelligence and information sharing; and prevent and reduce the harmful effects of crime and terrorism on victims, individuals, and communities."[16]

To protect those who chose to participate in the survey and allow them the freedom to answer honestly and completely — neither their individual identities nor the location of their fusion centers was recorded as part of this research.

Not every individual answered every survey question. There are two reasons for this. First, some individuals chose not to answer a given question. It can be assumed that they lacked either a strong opinion regarding the question, felt the question did not pertain to their particular function within their fusion center, or felt themselves unqualified to answer. Second, individuals were not presented with every question. The survey employed skip logic — meaning that depending on a respondent's answer they may or may not have been presented with a related follow-up question. Response rates varied from a high of seventy-one to a low of two. On average, forty-eight to forty-nine individuals answered any given question.[17]

The survey was open from January 23, 2012 until February 16, 2012. During that period there were no external events or shocks that might have altered the perceptions of respondents who answered the questions at one period of time as compared with those answering at another period. Additionally,

until the survey was closed, respondents were able to re-enter the survey and modify or delete their responses.

The survey was administered via SurveyMonkey (a web based survey service). Data generated by the survey was downloaded and analyzed using IBM's SPSS statistical software package.[18]

Before presenting HSPI's findings, two methodological points need to be made — both of which affect the interpretation of this survey.

First, the sample size and number of responses for each question comprise a *small-N* dataset. The results discussed below represent the perspectives of a relatively small number of individuals — as noted earlier, seventy-one people participated in this survey. That said, the total number of staff working in the fusion centers is not large. In 2010, a quarter of all fusion centers reported having fewer than ten people working in them. Three-quarters reported that they had fewer than fifty individuals working in the center.[19] The population of individuals working in the fusion centers is itself small. Given the 2010 statistics concerning staffing, seventy-one respondents likely represents approximately one-fifth of all those working in the fusion centers.[20] Given this small universe of potential respondents, and the focus of this survey (a description of the perspectives of those working in the fusion centers) — the *small-N* nature of the dataset does not constitute a significant methodological flaw.

Second, the data collected represents the perceptions of those working in the US' national network of fusion centers. As such, it represents a valuable tool for evaluating how well the fusion centers are fulfilling their mandate, the role they play in the US' national intelligence enterprise, the potential of the centers, the level of support the centers are being given, and the current nature of the threat domain. However, the data cannot be taken "as is." It must be placed into context and interpreted with care. The data and this brief provide a description from the perspectives of the fusion centers, not a causal argument nor a normative judgement.

Results

The results of HSPI's survey of those working in the US' (then) seventy-two state and urban area fusion centers provide important insights into their perceptions of the terror threat and the status of the US' national intelligence enterprise and fusion process. In addition, the survey results yield key information about the composition of fusion center staffs and their capabilities.

"Lone offenders and other small groups inspired by writing, web blogs, websites and other social media." — **Survey Respondent's answer to the question: Who Poses the Greatest Threat in Your Jurisdiction?**

The Terror Threat

HSPI's CTISR data indicates that those working in the US' nation network of fusion centers see terrorism as both an existent and persistent threat.

When asked to rate the risk terrorism poses to *their region* on a scale from 1 to 10, where 1 equalled "no threat" and 10 equalled "high threat" — thirty-four of sixty-nine respondents (some 49.3% of those who answered) rated the threat as 6 or higher. (FIGURE 1) A majority of respondents, 72.5%, indicated that terrorism posed a threat of 5 or higher.

HSPI then asked how those working in the fusion centers expect the terror threat to change over the course of the next year. (FIGURE 2) Of the sixty-nine

people who answered this question, 78.3% said they expected the level of threat they face in their jurisdiction to remain the same. The remaining 21.7% said they expected the level of threat posed by terrorism to increase. No one reported that they expected the terror threat to decline.

FIGURE 1: Risk Terrorism Poses to Your Region

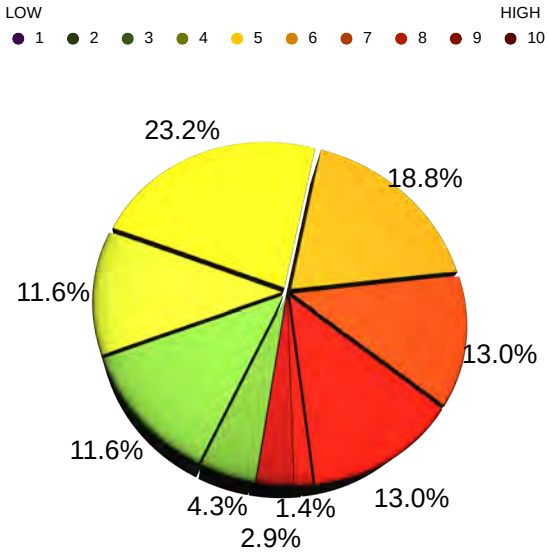
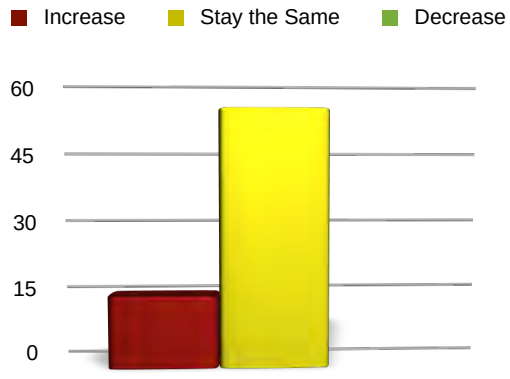


FIGURE 2: Terror Threat Level Over the Next Year



When asked who poses the greatest threat to their jurisdiction, forty-six out of sixty respondents cited homegrown terrorist groups or individuals.[21] (FIGURE 3) This question was followed by one that asked about whether they made judgements regarding what constitutes the "greatest threat" on the basis of the *likelihood* of a given outcome *or* the *consequences* of a given outcome — forty-two of sixty-respondents answered likelihood. (FIGURE 4)

FIGURE 3: Who Poses Greatest Threat

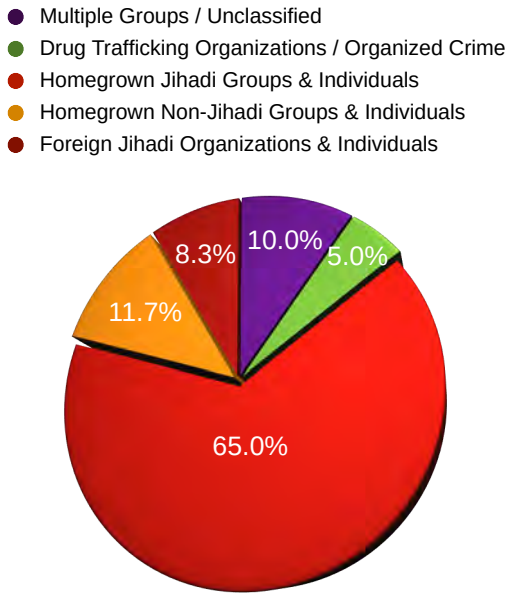
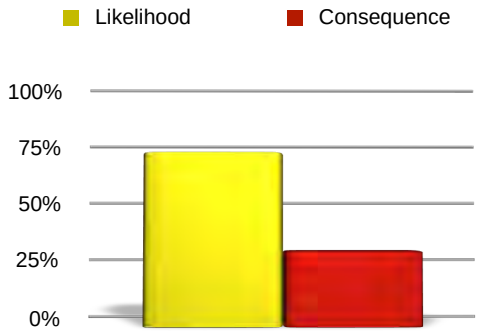
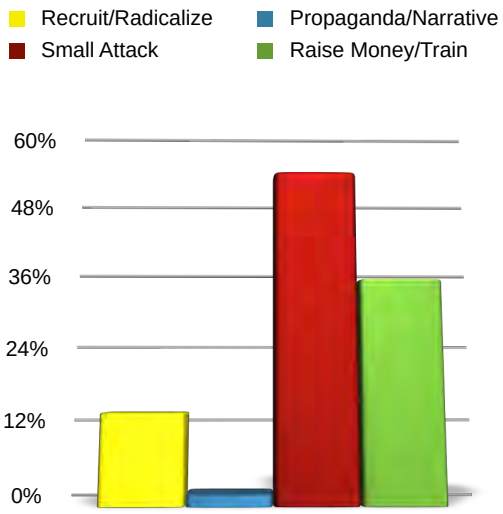


FIGURE 4: Basis for Judging "Greatest Threat"



When asked about the capabilities of the group or individuals they identified as posing the greatest threat in their jurisdiction, respondents cited small scale attacks (including the use of improvised explosive devices), fundraising, and/or recruitment and radicalization. (FIGURE 5) Fifty-two individuals responded to this open question, several identified multiple capabilities. Based on their answers four categories were created: Conduct Small Attack (against either individuals or property), Promotion of Violent Narrative or Spread Propaganda, Recruit or Radicalize Individuals, and Raise Money or Train.[22]

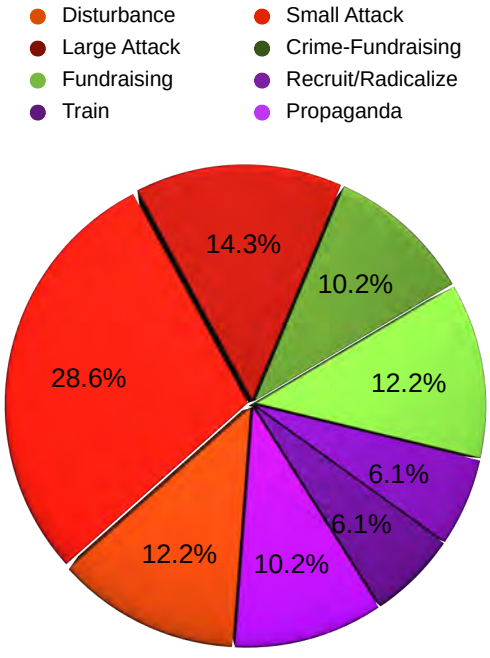
FIGURE 5: Capabilities of Group/Individuals Who Pose the Greatest Threat in Your Jurisdiction



When those in the fusion centers were asked about the intentions of the group or individuals they believed pose the greatest threat in their jurisdiction, respondents again provided answers that could be categorized as "to attack," "to fundraise," or "to radicalize." Using just those three categories, however, would mask much of the diversity and information contained in the respondents' answers. For example, in regard to attacks, respondents listed a range of intentions — from small scale attacks targeting uniformed military personal (like the attack against the recruiting station in Little Rock, Arkansas), to mass casualty attacks, to attacks meant to seriously disrupt or bring down the US government. One individual even listed cyber-terrorism as the chief intention of the group they contend poses the greatest threat in their jurisdiction.

To capture the richness of the responses of the fifty-one individuals who answered this question, the following categories were created: Civil-Disobedience Disturbance, Small Attack, Large Attack, Crime-based Fundraising, Fundraising, Recruit/Radicalize, Train, Disseminate Propaganda.[23] (FIGURE 6)

FIGURE 6: Intentions of Group/Individuals Who Pose the Greatest Threat in Your Jurisdiction



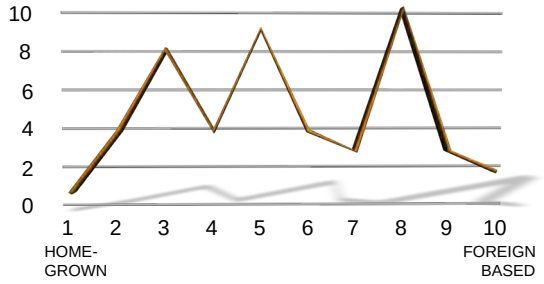
"A Mumbai-style attack is always of high concern." — **Survey Respondent**

Insights from those working in the fusion centers paint an interesting picture of the current terror threat domain. The data suggests they see a complex, rather than monolithic threat. The overall image is that of a moderate, persistent threat more likely to be realized by small, yet still potentially deadly, attacks executed by homegrown terrorists. The data also suggests, however, that those in the fusion centers continue to worry about the aspirations of terrorists and ability of terrorists to expand their capabilities. Responses to an HSPI question about terror planning illustrates the perceived complexity of the threat and why vigilance against foreign directed plots is still warranted.

When asked on a scale of 1 to 10, where 1 equals "homegrown individuals or organizations" and 10 equals "foreign based individuals or organizations," who do you think plans the specific jihadi terror plots of today — the aggregate data from the forty-eight individuals who answered the question provides three peaks (at 3, 5, and 8). (FIGURE 7)

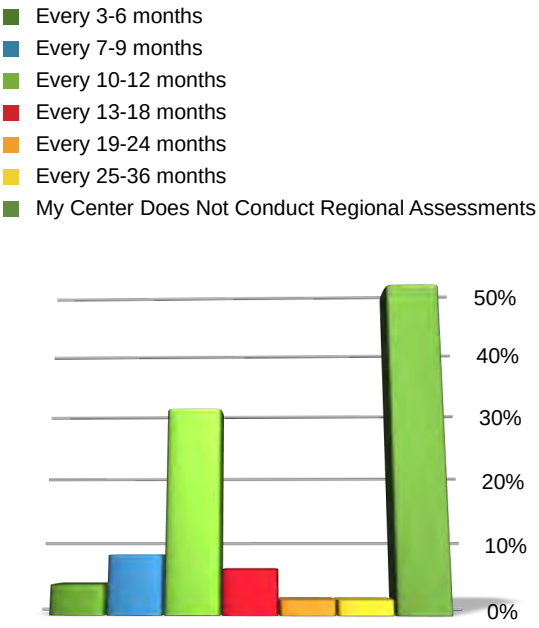
At least two interpretations of the data are possible. One interpretation is that there is disagreement within the fusion center network about who is planning the bulk of today's plots. The second interpretation is that the range of opinion that HSPI's survey captures within the fusion center network represents a new reality in terror planning. The fusion center network could be detecting a change in the terror ecosystem. The development of plots may be increasingly occurring at home, abroad, as well as being jointly planned by actors within and outside the United States.

FIGURE 7: Who Plans the Specific Jihadi Plots of Today — Homegrown or Foreign Based Actors



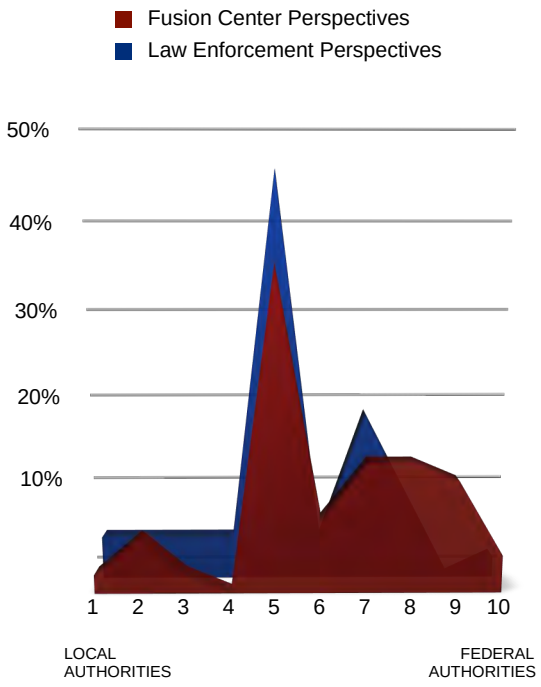
When asked how often their fusion center conducts regional threat assessments, nearly half of the forty-eight individuals who answered the question indicated that their center did not conduct regional threat assessments. (FIGURE 8) This represents a somewhat surprising result, given an expressed recognition of an existent and active threat.

FIGURE 8: How Often Does Your Center Conduct Regional Threat Assessments?



Based on HSPI's survey data, it appears that many of the individuals working in the fusion centers view counterterrorism as a shared responsibility between federal and local authorities. When asked on a scale of 1 to 10, where 1 equals "local responsibility" and 10 equals "federal responsibility," where does primary responsibility for counterterrorism rest — 5 was the most common answer (it was the response given by 35.4% of the forty-eight individuals who answered the question). However, the aggregate data suggests the existence of a slight "federal responsibility" skew in the fusion center perspective — 10.5% of respondents answered in the 1 to 4 (local) range of the scale, while 54.2% answered in the 6 to 10 (federal) range of the scale. Last year an HSPI survey of the counterterrorism intelligence perspectives of law enforcement produced similar, though slightly less skewed, results.[24] (FIGURE 9)

FIGURE 9: Where Does Primary Responsibility for Counterterrorism Rest?



The Intelligence Enterprise & Fusion Centers

As noted earlier in the background section, the ability to gather, receive, analyze, and disseminate information represents the critical operations of the fusion centers (both individually and collectively). HSPI's CTISR survey of those working in the fusion centers provides insight into how — and from the perspective of those working in the centers, how well — these tasks are being carried out.

As one would expect given the history of the fusion centers, those working in the centers view their work as a shared part of a larger enterprise. Just as there is a general perception that counterterrorism is a shared responsibility (FIGURE 9), there exists within the fusion centers a general perception that the collection and analysis of counterterrorism relevant information is also a responsibility that is shared between local and federal authorities.

When asked on a scale of 1 to 10, where 1 equals "local responsibility" and 10 equals "federal responsibility," where primary responsibility for the collection of counterterrorism relevant information rests — 5 was the most common answer (it was the response given by 30.9% of the fifty-five individuals who answered the question).

When asked where primary responsibility for the analysis of counterterrorism relevant information rests — 5 was again the most common answer (it was the response given by 29.1% of those who answered this question). Fifty-five individuals responded to the question using a scale of 1 to 10, where 1 equaled "local responsibility" and 10 equaled "federal responsibility." (FIGURE 10)

"...to assist fusion centers in becoming centers of analytic excellence."
— DHS on "The Path Ahead"

FIGURE 10: Where Does Primary Responsibility for the Collection and Analysis of Counterterrorism Relevant Information Rest?

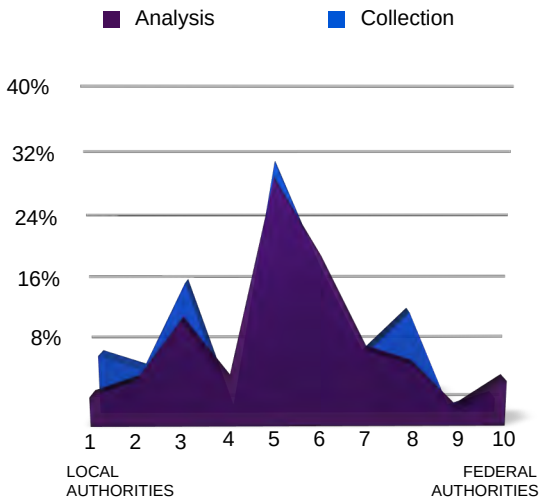
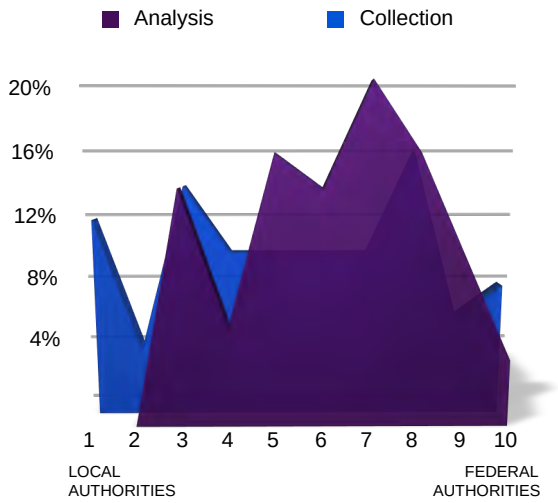


FIGURE 11: Who Has Greater Capability for the Collecting and Analyzing of Counterterrorism Relevant Information?



Beyond actual responsibility, however, those in the fusion center do perceive differences between local and federal capabilities. When asked whether local or federal authorities had greater capability in regard to the collection of information, respondents expressed a wide range of opinion. (FIGURE 11). A fairly wide range of opinion was also expressed when asked whether local or federal authorities had greater capability in regard to the analysis of information — in regard to analysis, the data is skewed in favor of greater federal capability. (FIGURE 11) Fifty people answered each of these questions. For each question they used a scale of 1 to 10, where 1 equaled "local responsibility" and 10 equaled "federal responsibility."

"Most of our intelligence functions still deal with every-day criminal activity."
— Survey Respondent

In regard to their own operations, a majority of respondents indicated that their center has a formal process for developing standing and priority information needs. In regard to standing information needs, 73.5% of respondents reported that their center has a process for developing such. (FIGURE 12) Regarding priority information needs, 67.3% of respondents indicated their center has a process for developing such. (FIGURE 13) This inquiry was asked as two separate questions. Forty-nine individuals answered each question.

" There is no other state level agency which focuses on Counterterrorism or provides a POC for federal agencies responsible for Counterterrorism"
— Survey Respondent

FIGURE 12: Does Your Center Have a Process for Developing Standing Information Needs?

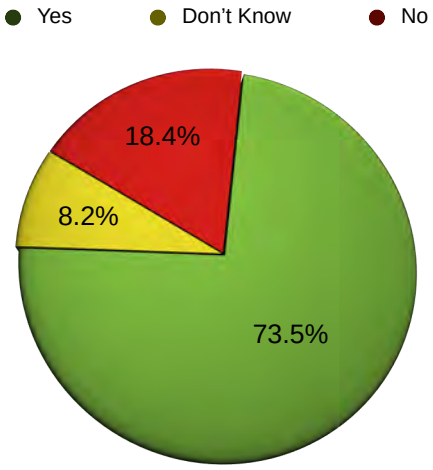
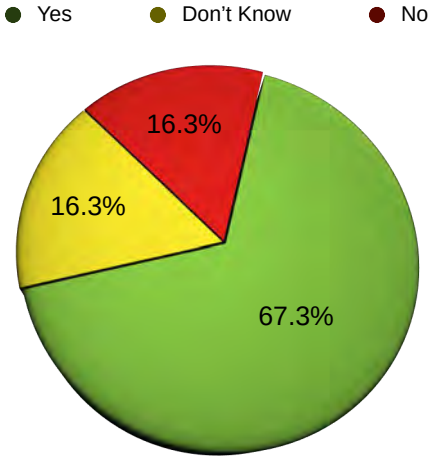
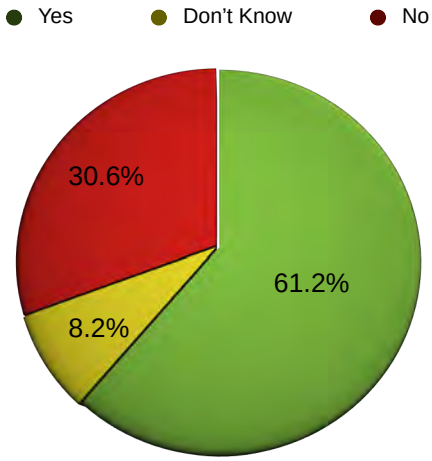


FIGURE 13: Does Your Center Have a Process for Developing Priority Information Needs?



A slightly smaller majority of respondents, some 61.2%, said their fusion center had a written plan for gathering counterterrorism specific information. (FIGURE 14). Forty-nine individuals answered this question.

FIGURE 14: Does Your Center Have a Written Plan for Gathering Counterterrorism Information?

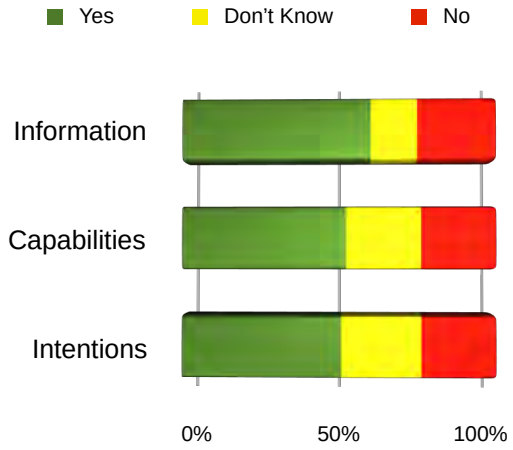


Several additional questions shed light on the fusion centers' current capabilities in regard to the gathering of counterterrorism information.

When asked whether or not their center had an effective strategy for *gathering* information on the group or individuals they identify as posing the greatest terror threat in their jurisdiction, 60.3% of the sixty-eight respondents said their center did, 25% said their center did not, and 14.7% replied that they did not know. When a similar, yet more specific question, was asked about whether or not their center had an effective strategy for *gathering* information about that same group's or individual's *capabilities*, 52.4% of the sixty-three respondents said their center did, 23.8% said their center did not, and 23.8% indicated they were not sure if their fusion center had an effective strategy for such. When asked about the *intentions* of that group or individual, 50.8% of the fifty-nine respondents said their center had an effective strategy for *gathering* information on their *intentions*, 23.7% said their

center did not, 25.4% said they did not know if their center had an effective strategy. (FIGURE 14)

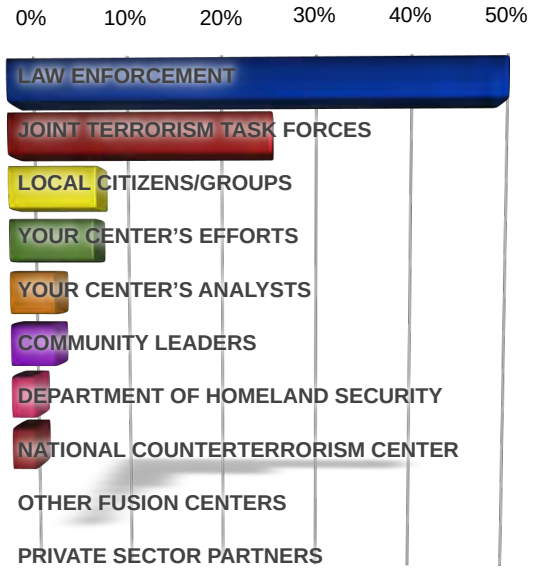
FIGURE 14: Does Your Center Have an Effective Strategy for *Gathering* Information about Those Who Pose the Greatest Terror Threat in Your Jurisdiction?



When asked about who they believe are the most important institutional or organizational sources for counterterrorism information, local law enforcement was the answer most often cited. Of the fifty individuals who answered this question, 48% said information from police officers and detectives was the most important. The FBI's Joint Terrorism Task Forces (JTTFs) were the second most often cited: 26% said the JTTFs were the most important source for counterterrorism information. A rank order of the respondents choices is provided in the next column. (FIGURE 15) HSPI's survey supplied the listed categories.

[We] "do not have the needed access to HSDN sites." **— Survey Respondent**

FIGURE 15: Most Important Sources of Counterterrorism Intelligence



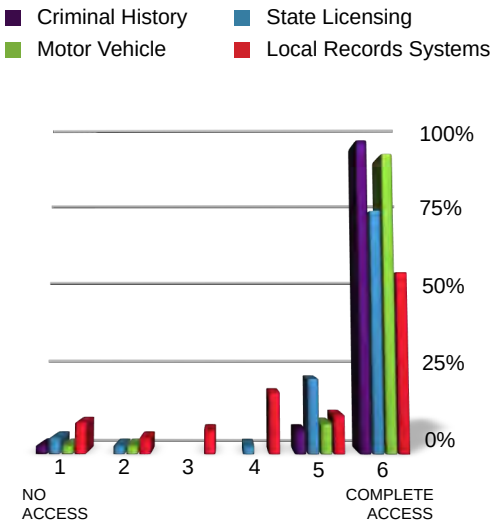
In the question concerning institutional or organizational sources for counterterrorism information, respondents were asked to rank order each of the potential sources from 1 (meaning most important) to 10 (meaning least important). No one identified either "Other Fusion Centers" or "Private Sector Partners" as the most important source of counterterrorism information. The "Other Fusion Centers" category was selected by 6.5% of respondents as the third most important source of counterterrorism information — the category's highest ranking. The most common rankings for "Other Fusion Centers" were 5 and 8: each was cited by 19.6% of respondents. The category representing "Private Sector Partners" was selected by 6.4% of respondents as the second most important source of information. The most common ranking for "Private Sector Partners" was 9 — chosen by 17% or respondents.

These results from the fusion centers mirror the results from an April 2011 HSPI survey of the Major Cities Chiefs Association' Intelligence Unit

Commanders Group. When asked to name the most important sources of counterterrorism intelligence, members of the Intelligence Commanders Group cited information from citizens, law enforcement, and the JTTFs as being the most important.[25]

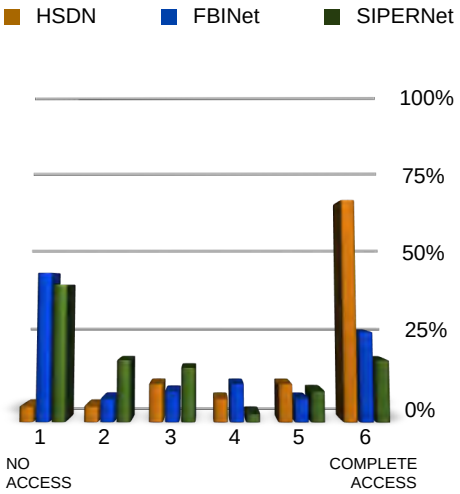
When asked about their level of access to state and local databases from which they might gather information, forty-seven respondents supplied the following information. Large majorities indicated they had complete access to local criminal history databases, state licensing databases, and motor vehicle databases — 91.3%, 70.2%, and 87.2% respectively. A much smaller majority, 52.2%, reported that they had access to local records systems. (FIGURE 16)

FIGURE 16: Levels of State & Local Database Access



When asked about their level of access to national databases, 63.8% stated they had complete access to the Homeland Secure Data Network (HSDN). At the same time, only 25.5% indicated they had complete access to FBINet. Even fewer, 17.4%, reported having complete access to the Secret Internet Protocol Router Network (SIPRNet). (FIGURE 17) Forty-nine individuals answered this question.

FIGURE 17: Levels of National Database Access



In regard to paid database services, including Lexus Nexus and Accurint, 83% of the forty-nine individuals who answered stated that they had complete access.

Relevant counterterrorism information products are not shared proactively. "General products like 'watch out for people stealing propane tanks' are shared, but not 'a group of Somali refugees are attempting to purchase small arms.'" —
Survey Respondent

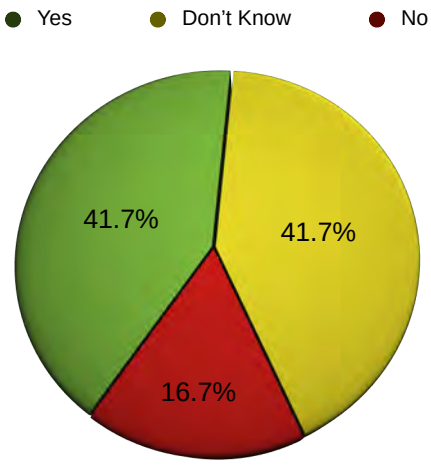
When asked if their center had a formal strategy for gathering information on demographic changes within their jurisdiction, 81.3% said they did not, 14.6% indicated they were not sure, and 4.2% said

they did. Forty-eight individuals answered this question.

Overall, HSPI's survey detected a strong perception among those working in the fusion centers that there are significant gaps in the types of intelligence products to which they have access.

When asked about it directly, equal numbers of the forty-eight respondents stated there either were gaps or that they were unsure as to whether there were gaps in the types of intelligence products to which they had access. (FIGURE 18)

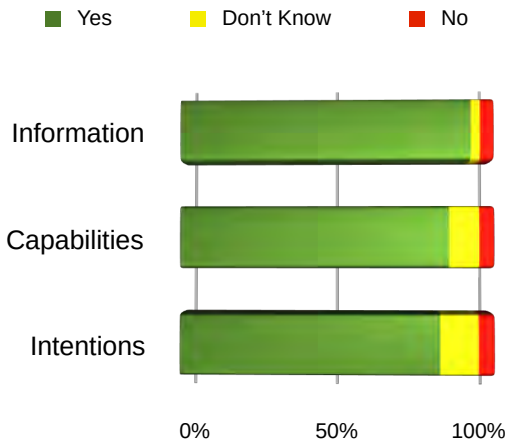
FIGURE 18: Are there Gaps in the Types of Intelligence Products to Which You Have Access



HSPI's CTISR survey asked those working in the fusion centers several questions about their center's ability to send and receive information. Data from their responses produced the following results.

When asked whether or not their center had an effective strategy for *disseminating* information on the group or individuals they identify as posing the greatest terror threat in their jurisdiction, 92.6% of the sixty-eight respondents said their center did, 4.4% said their center did not, and 2.9% replied that they did not know. When a similar, yet more specific question, was asked about whether or not their center had an effective strategy for *disseminating* information about that same group's or individual's *capabilities*, 85.7% of the sixty-three respondents said their center did, 4.8% said their center did not, and 9.5% indicated they were not sure if their fusion center had an effective strategy for such. When asked about the *intentions* of that group or individual, 82.8% of the fifty-eight respondents said their center had an effective strategy for *disseminating* information on their *intentions*, 5.2% said their center did not, 12.1% said they did not know if their center had an effective strategy. (FIGURE 19)

FIGURE 19: Does Your Center Have an Effective Strategy for *Disseminating* Information about Those Who Pose the Greatest Terror Threat in Your Jurisdiction?



A quick comparison of the data illustrated by FIGURE 14 and by FIGURE 19, suggests those working in the fusion centers have a higher level of confidence in their ability to disseminate information than in their ability to gather it.

In the aggregate, the data suggests the fusion centers are acting as information hubs — with the flow of information generally moving from federal partners, through the centers, and then out to law enforcement, state homeland security officials, and public safety and/or emergency response personnel. The private sector was generally absent from this flow of information. (FIGURE 20)

When asked how often they *receive* information from *federal partners*, 63.3% of the forty-nine respondents reported that they receive information every day. Some 20.4% indicated they received information every two or three days, 10.2% stated they did so every week. The remaining 6.1% reported that they received information from federal partners at least once a month.

When asked how often they *disseminate* information to *federal partners*, 41.7% of the forty-eight individuals who answered the question stated that they sent information every day. Another 29.2% reported that they send information every two or three days, while 16.7% indicated they sent information every week. The remaining 12.5% reported sending information to federal partners every two or three weeks to six months.

When asked how often they *receive* information from *major law enforcement entities* in their jurisdiction, 49% of the forty-nine individuals who answered the question stated that they receive information from such every day. Another 30.6% responded that they received information every two or three days, 14.3% that they did so every week, and the remaining 6.1% that they received information every two or three weeks.

When asked how often they *disseminate* information to *major law enforcement entities* in their jurisdiction, 69.4% of the forty-nine individuals who answered the question reported that they sent information every day. An equal number, 14.3%, reported that they send information either every two or three days or every week. The remaining 2% indicated they sent information to law enforcement every two or three weeks.

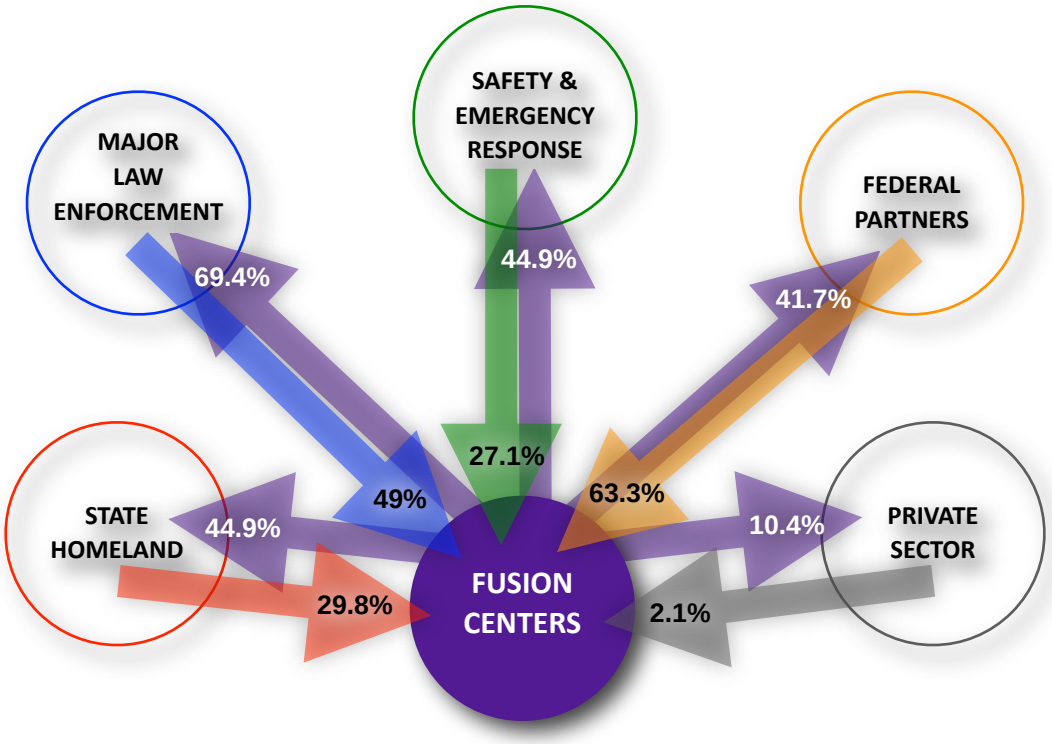
> ***"I am designated as Homeland Security Coordinator for our Fusion Center, but am excluded from briefings given to top level officials including the Governor."*** **— Survey Respondent**

Data regarding the flow of information from and to state homeland security officials suggests there is a greater range in the frequency of information sharing between fusion centers and state homeland security leaders.

When asked how often they *receive* information from *state homeland security officials* in their jurisdiction, respondents reported the following. Of the forty-seven people who answered this question, 29.8% reported that they received information every day, 19.1% that they did so every two or three days, 19.1% that they did every week, and 8.5% that they received information from state homeland security officials every two or three weeks. Some 2.1% of respondents stated that they received information every month, 6.4% that they did so every two or three months, 2.1% that they did so every six months, and 12.8% they they received information from state officials every six months to a year.

When asked how often they *disseminate* information to *state homeland security officials* in their jurisdiction, 44.9% of the forty-nine respondents stated that they sent information to state officials every day. Another 16.3% indicated that they sent information every two or three days, 18.4% that they send information every week, and 8.2% that they did

FIGURE 20: Percentage of Respondents Who Indicated They Receive/Disseminate Information From/To the Following Entities on a Daily Basis



so every two or three weeks. Some 2% stated they send information every month, 6.1% every two or three months, and 4.1% that they send information to state officials every six months to a year.

When asked how often they *receive* information from *public safety or emergency response/ preparedness entities* in their jurisdiction, 25% of the forty-eight individuals who answered the question stated that they did so daily. Another 14.6% reported that they received information every two or three days, 27.1% that they did so every week, and 14.6% that they received information every two or three weeks. Of the respondents, 4.2% indicated that they received information from public safety or emergency response/preparedness entities every month, an equal number, 4.2%, every two or three months. Some 2.1% said they received such information every six months and 8.3% that they received information every six months to a year.

When asked how often they *disseminate* information to *public safety or emergency response/ preparedness entities* in their jurisdiction, the forty-nine respondents reported the following. Some 44.9% of those who answered the question indicated that they did so every day, 18.4% that they send information every two or three days, 20.4% every week, and 2% every two or three weeks. Another 10.2% reported that they send information every month, 2% every six months, and 2% that they send information to safety and emergency response/ preparedness entities every six months to a year.

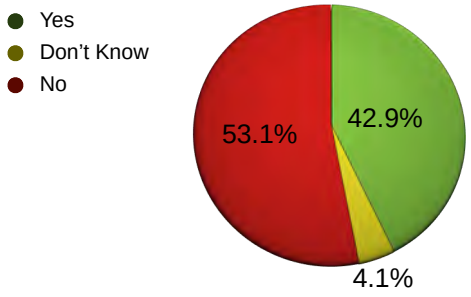
When asked how often they *receive* information from *private sector* entities in their jurisdiction, 2.1% of the forty-eight respondents stated that they did so

every day. Another 12.5% of respondents indicated that they did so every two or three days, 6.3% every week, and 35.4% that they did so every two or three weeks. A smaller number, 12.5% of respondents answered that they received information from the private sector every month, 14.6% that they did so every two or three months, and 8.3% that they did so every six months and the same number, 8.3%, that they did so every six months to a year.

When asked how often they disseminate information to private sector entities in their jurisdiction, 10.4% of the forty-eight respondents answered that they did so every day. Some 18.8% indicated that they did so every two or three days, 25% that they send information every week, and 18.8% that they do so every two or three weeks. Some 8.3% told HSPI that they send information to private sector entities every month, 6.3% that they do so every two or three months, 4.2% that they do every six months, and 8.3% that they do so every six months to a year.

The relative weakness of relationships that exist between fusion centers and private sector entities is illustrated by the data from another survey question. When asked whether or not the owners and operators of critical infrastructure in your jurisdiction are part of your fusion center, a majority of the forty-nine respondents said no. (FIGURE 21)

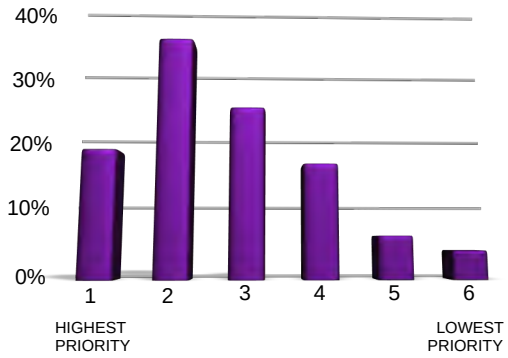
FIGURE 21: Are the Owners and Operators of Critical Infrastructure Part of Your Fusion Center



In regard to the analytical capabilities of the fusion center, HSPI's survey found the following. Those working in the fusion centers view analysis as a critically important function — nearly as important as the receiving and gathering of information. At the same time, however, those working in the fusion centers believe analysis is the area in which the most improvement is needed.

When asked to rate the importance of intelligence analysis as an operational task on a scale of 1 to 6, where 1 equals "highest priority" and 6 equals "lowest priority," the most common rating was a 2. Of the fifty-one individuals who answered this question, 33.3% rated it as such. Another 17.6% rated it as a 1 — highest priority task. The response rates for 3, 4, 5, and 6 were 23.5%, 15.7%, 5.9%, and 3.9% respectively. (FIGURE 22)

FIGURE 22: Rate the Importance of Analysis



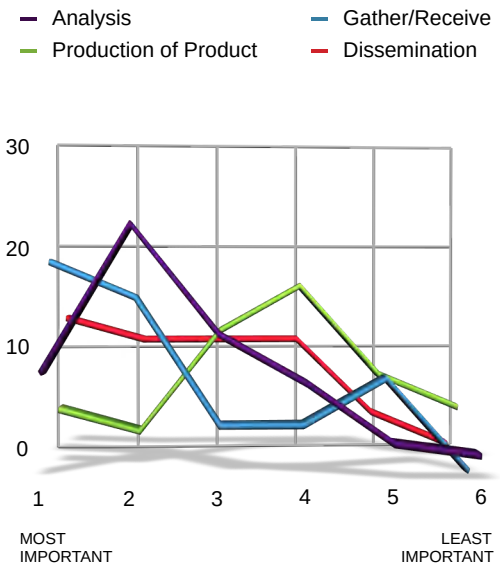
HSPI's survey data suggests that more than half of those asked would select analysis as either the first or second most important of the four Critical Operational Capabilities established by the 2010 New Orleans conference.

Recognizing the importance of a given task in the abstract is much different from its operationalization.

Furthermore, the need to balance its importance against other important tasks (the gathering and reception of information, the production of productions, and the dissemination of information) complicates the endeavor before the fusion centers. Recognizing this, HPSI did the following.

Survey participants were asked to rank order several operational tasks. Their responses provided both independent and relative measures of the importance of these tasks as judged by those working in the fusion centers. FIGURE 23 (below) illustrates the participants' answers. The scale runs from 1 to 6, where 1 equals "most important" and 6 equals "least important." Each point on the scale provides the relative rank ordering of the perceived importance of each task: the gathering or receiving of information, the analysis of information, the production of intelligence products, and the dissemination of information. Between fifty-one and fifty-thee individuals answered these questions.[26]

FIGURE 23: Rate the Importance of Key Tasks



The gathering or receiving of information was most often selected as the most important task: 36.7% of respondents rated it as 1. In the 1 rating, it is followed by dissemination (25.5%) , analysis (17.6%), and the production of products (10.2%). Given the data presented in FIGURE 22, where analysis is identified as the second highest priority by a substantial number of respondents, the data presented here may appear to be counterintuitive.

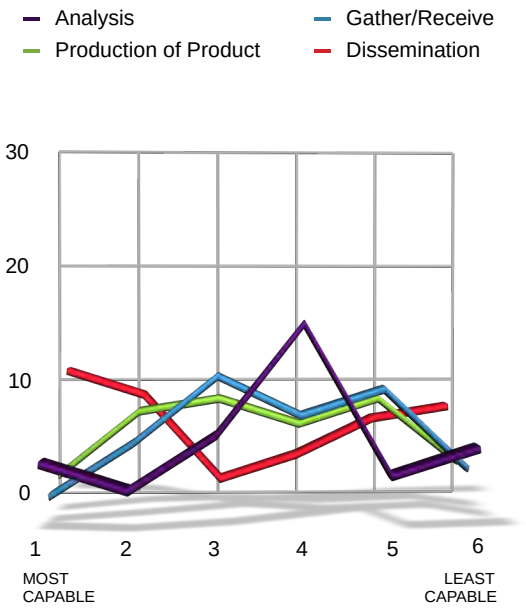
Looking at the relative measure of respondents' ranking of the second most important task, however, supports the results expressed earlier.

Looking at where each task "peaks" suggests that those in the fusion centers rank order the gathering or receiving of information as the most important task, followed by analysis. What comes next appears to be up for debate: both analysis and production of products, barely edge out dissemination. The production of products, however, was commonly chosen as the forth most important task — and edges out the others at the 5th and 6th positions as well. Interestingly, the participant responses indicate that dissemination is never seen as being more important than the other tasks.

Survey participants were also asked about their center's capabilities in regard to the execution of these tasks — using a scale from 1 to 6, where 1 equals "highest capability" and 6 equals "least capability." (FIGURE 24) Like the previous figure, FIGURE 24 provides a relative measure — this time of fusion center capabilities. Each point on the scale provides the relative rank ordering of the perceived capabilities of the respondent's fusion center in regard to each task: the gathering or receiving of information, the analysis of information, the production of intelligence products, and the dissemination of information. Between thirty-seven and fifty-one individuals answered these questions.[27]

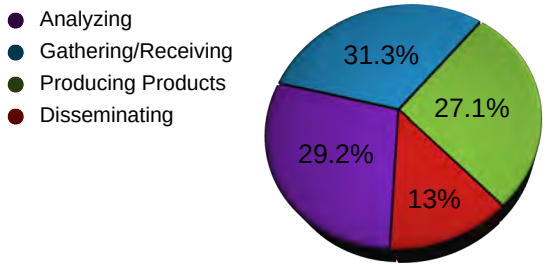
Dissemination was most often selected as the area in which the fusion centers have the most capability: 26.8% of respondents rated it a 1. Dissemination was also the highest rated choice for 2: 22% rated it as such. This is particularly interesting given the results presented above in FIGURE 23. The data suggests that those in the fusion centers perceive that their center's greatest capability lies in carrying out the task they hold to be of the least importance.

FIGURE 24: Rate Your Center's Capabilities Regarding Key Tasks



When asked which task consumes the most amount of their time, the gathering or receiving of information was the answer most commonly given. (FIGURE 25) Of the forty-eight individuals who answered this question, 31.9% cited the gathering or receiving of information.

FIGURE 25: Which Task Consumes the Most Amount of Your Time



When asked to rank order the time they spend on these same four tasks (gathering or receiving information, analyzing information, producing intelligence products, and disseminating information), the forty-six to forty-eight individuals who answered these questions provided the following data using a scale where 1 equals "the most amount of time" and 4 equals "the least amount of time." (FIGURE 26)

FIGURE 26: Rank Order of Time Spent on Each Task

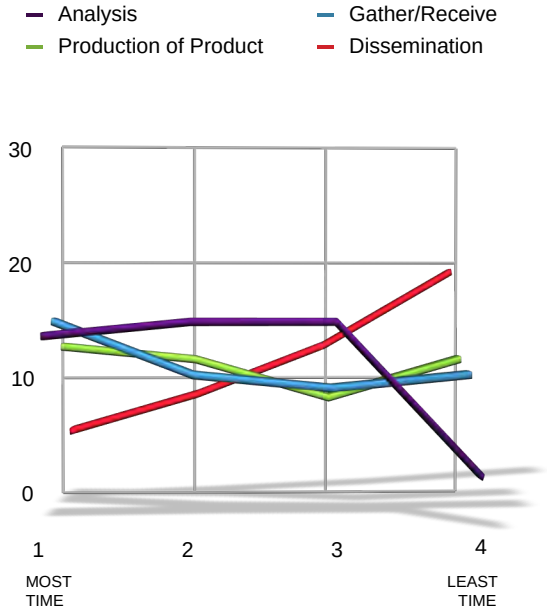


FIGURE 26 again highlights the perceived importance of analysis. When asked about the amount of time spent on each of the four tasks relative to one another, the data for analysis is the most consistent. Some 29.2% rated it as the task they spend the most time on, 31.3% rated it as the task they spend the second greatest amount of their time, another 31.3% rated it as the task upon which they spend the third most time.

It can be assumed that some of the variance on how respondents spent their time can be accounted for by differences in the job function or role they play in their fusion center. Even accounting for that, however, it appears that those working in the fusion centers hold analysis to be important enough that they devote time to it regardless of their specific job function.

The perceived importance of analysis is also revealed by respondents' answers to a survey question about where they would like to see their center improve. When asked to rank order the capability where they would like to see the most improvement in their center, the most common answer was analysis. Of the forty-nine individuals who answered the question, 51.1% responded that improving their center's analytical capabilities was their first priority. The gathering and receiving of information came in second, 19.1% selected it as their first priority. Another 6.5% selected dissemination, while 2.1% chose the production of products. (FIGURE 27)

As with earlier questions regarding the importance of key tasks and their center's capabilities, this question was presented as a series that asked respondents to make a relative rank-ordered judgement. The similar 1 to 6 scale was used, where 1 equaled "highest priority for improvement" and 6 equaled "lowest priority for improvement." Given the results reported above, the data is not surprising. Those working in the fusion centers expressed the opinion that it was more important to increase their analytical capabilities and their ability to gather and receive data than their capability to produce products or disseminate information.[28] (FIGURE 28)

FIGURE 27: Priority Area for Improvement

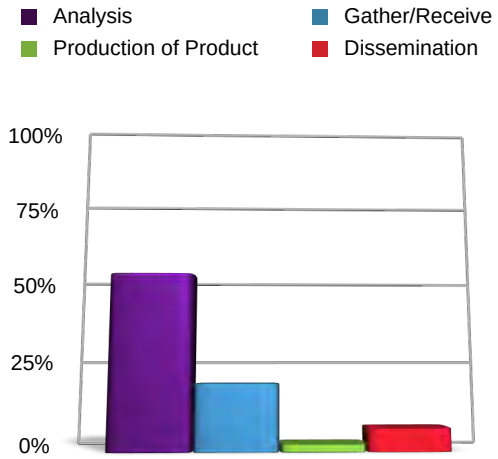
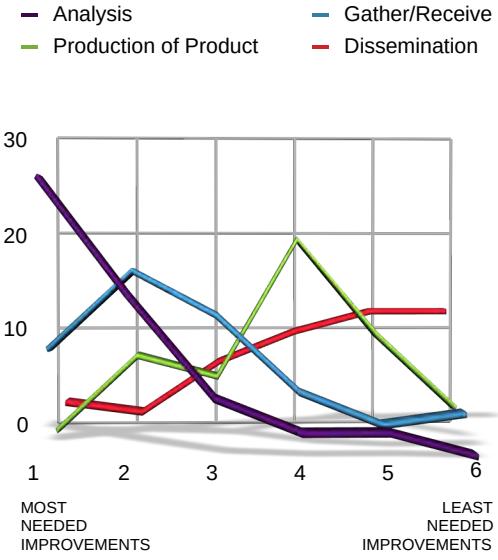
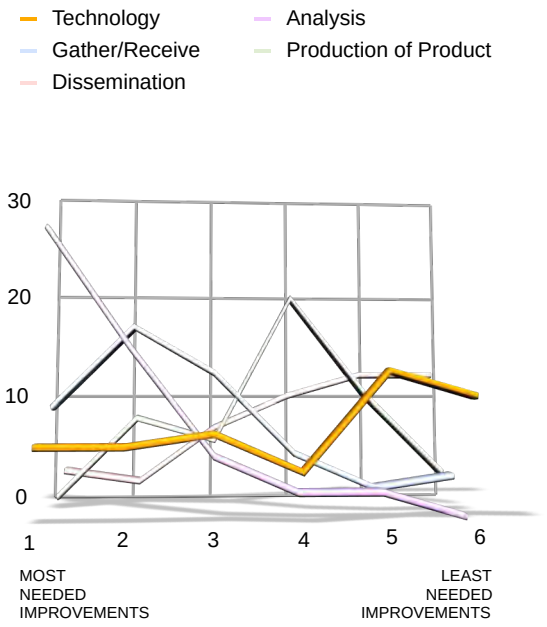


FIGURE 28: Relative Rank-Ordered Areas for Improvement



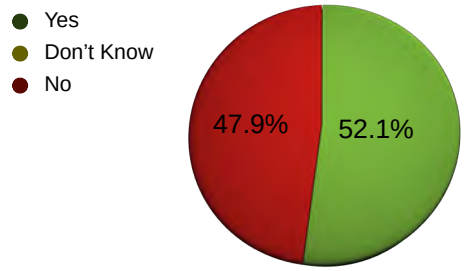
When asked about whether or not they would prioritize improvements in their technological resources, participant responses were mixed. About half of the respondents indicated they would invest in technological resources — though not at the expense of improvements in analytical capabilities or the gathering and reception of information. FIGURE 29 illustrates the rank order for technological improvements as expressed by respondents.

FIGURE 29: Relative Importance of Technological Improvements



The issue of technology presents itself in four other important questions. The first being in regard to their center's information technology (IT) staff. When asked whether or not their center had full-time IT staff, nearly half indicated they did not. (FIGURE 30) Forty-eight individuals answered this question.

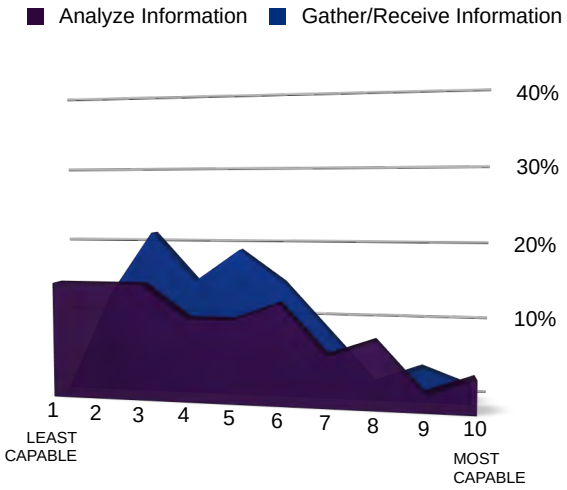
FIGURE 30: Does Your Center Have Full-Time IT Staff?



The real importance of the IT staffing question, however, lies in its relationship to the second and third additional questions regarding technology — both of which address cyber security.

When asked to rank order their center's capability for *gathering or receiving cyber security relevant information*, only a few respondents indicated that their center had high capability in this area. On a scale from 1 to 10, where 1 equaled "no capability" and 10 equaled "high capability" — 34% of the forty-seven individuals who answered the question rated their capability at a 3 or lower. Only 8.5% rated it at 8 or higher. (FIGURE 31)

FIGURE 31: Cyber Security Capabilities

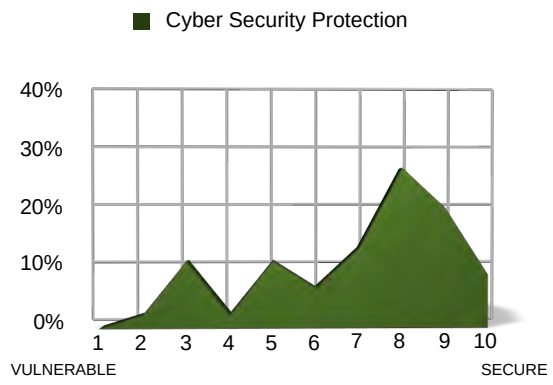


When asked to rank order their center's capability for *analyzing cyber security relevant information*, the data was similar. On a scale from 1 to 10, where 1 equaled "no capability" and 10 equaled "high capability" — 44.1% of the forty-seven individuals who answered the question rated their capability at a 3 or lower. Some 14.9% of respondents rated it at 8 or higher. (FIGURE 31)

The fourth and final technologically driven question also touches on cyber security. When asked to rank order their center's capability for *protecting digital information*, survey respondents expressed a fair amount of confidence. On a scale from 1 to 10, where 1 equaled "no capability" and 10 equaled "high capability" — only 13.1% of the forty-six individuals who answered the question rated their capability at a 3 or lower. Some 54.4% of respondents rated it at 8 or higher.

Nonetheless, the data suggests there is reason for concern. Several respondents indicated that security might be an issue. Furthermore, given the very nature of the fusion center endeavor as an information sharing network, the weakest link determines the strength of the entire chain — both in regard to the intelligence enterprise and in the protection of the privacy rights of those individuals whose information may be exposed. (FIGURE 32)

FIGURE 32: Ability to Protect Digital Information



The final set of data directly tied to the role of the fusion centers in the intelligence enterprise addresses the US' homeland security warning system.

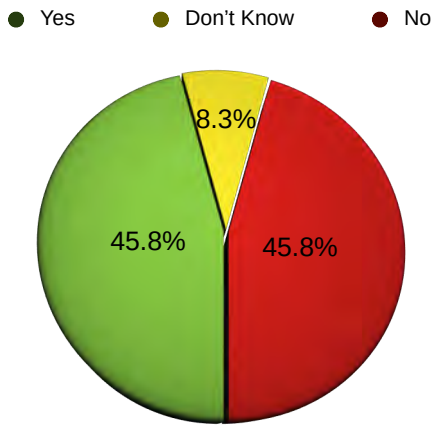
When asked whether or not the United State has an adequate homeland security warning and alert system, respondents were evenly split. Of the forty-eight individuals who answered the question, 45.8% said it did and 45.8% said it did not. (FIGURE 33) When asked to make comments regarding the basis for their assessment of the US' warning system many who answered yes cited their level of access to it, its relative simplicity, and/or the fact that the new National Terrorism Advisory System (NTAS) represents an improvement over the old program. Those who answered no cited a lack of detail or differentiation in the warnings, ill defined protocols, and a lack of testing. Many — including those who answered "yes," "no," and "don't know" to the question regarding the adequacy of the US' warning system — expressed a concern about whether or not there is a firm conceptual understanding of how best to warn Americans so as to elicit the desired response on the part of the public.

"NTAS is an improvement over the old system." — **Survey Respondent**

"NTAS is very flat — preferred old system." — **Survey Respondent**

"NTAS is new and I am not sure of its adequacy." — **Survey Respondent**

FIGURE 33: Is the US' Homeland Security Warning System Adequate?



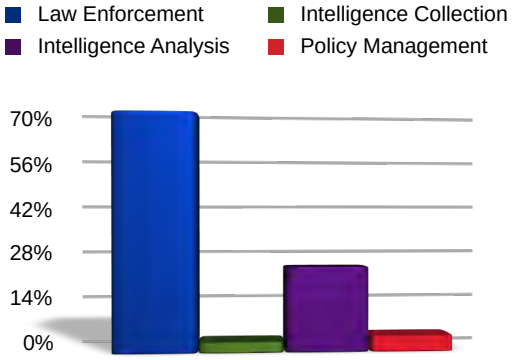
The Fusion Centers — An Operational Profile

As was noted in the background section, the staffing levels of the fusion centers varies — from a minimum of four individuals to a maximum of one hundred.[29] Differences in staff size can be expected to effect the operational capabilities of a given center. Yet, staffing levels are not the only determinant of such.

Fusion centers also vary in regard to the professional backgrounds and skill sets of their staffs. Variance in the presence of local law enforcement, state police agencies, state departments of homeland security, emergency management entities, the National Guard, and various federal bodies (including DHS and the FBI) each effect the professional composition and organizational behavior of each center.[30] In short, fusion centers are affected not just by how many, but who staffs them. For that reason, HSPI asked survey participants a series of questions about the demographic and operational profile of their centers.

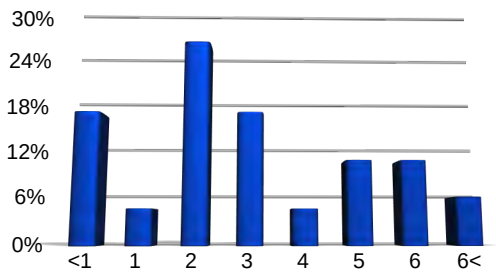
As a set of skills, training, and experiences, law enforcement defines the professional background and ethos of the fusion centers. When asked, which of four categories best described their professional background, 68.6% of the seventy respondents answered law enforcement. Intelligence analysis came in second, 24.3% selected it. (FIGURE 34)

FIGURE 34: Which Category Best Describes Your Professional Background



When asked how long they had served in their current position, the most common answer was two years. Nearly a quarter, some 24.3% of the seventy individuals who answered the question, gave that response. The next two most common answers were three years and less than 1 year — each of which was selected by 15.7% of respondents. (FIGURE 35)

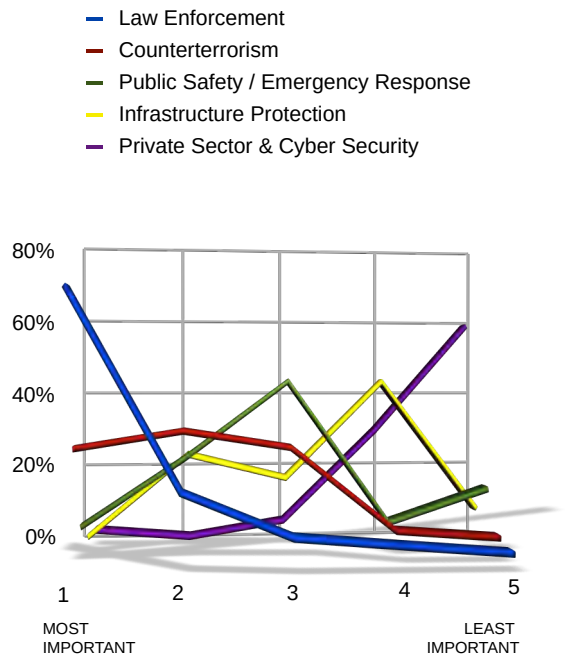
FIGURE 35: How Long Have You Served in Your Current Position



Most respondents indicated they would be considered experienced individuals. Only 4.3% of respondents said they would be considered entry-level personnel. Some 21.4% stated they had mastered the skills and competencies of their current position and were familiar with those of superior positions. Another 21.4% went beyond that and reported that in addition, they also played a training and oversight role. A full 52.9% reported that they provide input and direction in regard to organizational decisions.[31] Seventy people answered this question.

When asked to provide a relative rank ordering of what they considered to be their center's most important activities, the majority cited law enforcement. Fifty-three people answered the question which asked them to rank order various types of activities. (FIGURE 36)

FIGURE 36: Relative Rank-Ordered Most Important Activities



Survey respondents expressed a consistent rank ordering of importance. That order is as follows: Law Enforcement, Counterterrorism, Public Safety/ Emergency Response, Infrastructure Protection, and Private Sector Security (including Cyber Security).

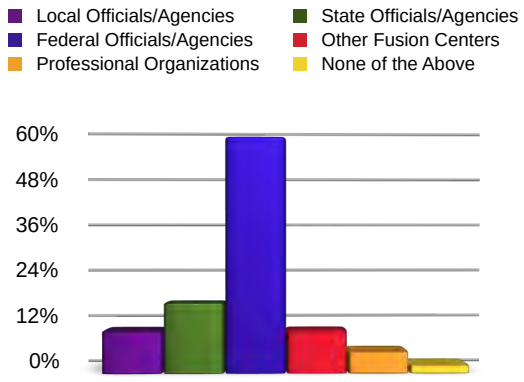
The order holds within the "Most Important" category ranking. Some 63.3% of respondents selected Law Enforcement as the most important. It is followed by counterterrorism, which was selected as the most important fusion center activity by 27.5% of those who answered this question. Public Safety/Emergency Response was chosen as the most important by 8.2%. Infrastructure Protected was ranked most important by 4.1%, followed by Private Sector & Cyber Security which were ranked most important by 4% of respondents. This ranking also holds across the chart, each category peaks at a different point (1, 2, 3, 4, or 5) — but their order stays the same.

When asked a follow-on question about what shapes their rank ordering of their center's most important activities, most stated that such was the product of their center's institutional pedigree (the agencies that created their center), the key relationships and customer base they serve, the decisions of elected officials or senior decision-makers, history or standard operating procedures, or the attacks of September 11, 2001. Of the thirty individuals who answered this question, none of them referenced the current or expected threat domain.

As noted earlier, many in the fusion centers expressed the belief that the taking-in of information (both via gathering and receiving sent information) and its analysis are vitally important. When asked who they look to for guiding sets of principles and assumptions about the intelligence enterprise, 56.7% of the sixty individuals who answered reported that they look to federal officials or agencies. Another 16.7% indicated they look to state officials or

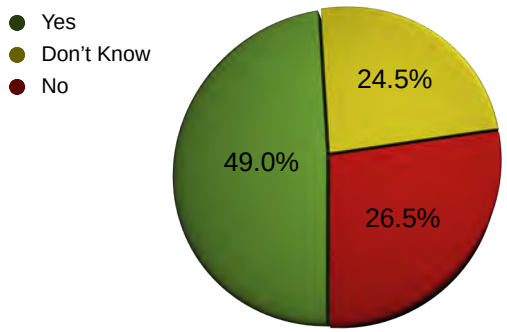
agencies for intelligence guidance, while 10% said they look to local officials or other fusion centers for guidance. (FIGURE 37)

FIGURE 37: Who Do You Look Toward for Guidance in the Intelligence Enterprise



Although intelligence was widely recognized as important, respondents were less confident about its viability as a career. When asked if the intelligence enterprise represented a viable career path within their profession, 51% of the forty-nine individuals who answered said either they did not know, or no. (FIGURE 38)

FIGURE 38: Does intelligence represent a viable career path within your profession?



Many of those working in the fusion centers expressed the belief that their centers have established mechanisms for the informal sharing of information — both within and outside their center. HSPI asked these questions as a means for evaluating the potential of the fusion centers to overcome the stove-piping of information. They also highlight whether or not those in the centers are able to engage in the types of free-flowing/thinking conversations that foster organizational learning.

In regard to both internal and external dialogues, an overwhelming majority reported they felt their center had processes for sharing information that might be interesting or important even if not immediately pertinent. Some 98.2% of the fifty-five individuals who answered the question about the informal sharing of information within the center said they felt such was possible. Of the fifty-four individuals who answered the question about informal sharing with those outside their center, 88.9% said they felt protocols to make such happen were in place.

Finally, when asked whether or not there were tools or procedures in the private sector that could or should be adopted by the fusion centers, many (about one-fifth to one-quarter) said yes. Among those things most cited were social media tools, encryption and decryption tools that could be used throughout the network of fusion centers, common customer feedback tools, as well as mechanisms that collect point of sale and aggregate data concerning purchasing history and patterns.[32]

Conclusion

HSPI's survey of individuals working in the fusion centers provides an important glimpse into a defining feature of the US' modern national intelligence enterprise.

In an absolute sense, the participation of seventy-one individuals represents a small sample size. Yet, it should be noted that the value of any data set, or the judgements drawn from it, are the product of assumptions about the distribution of that data.[33] In short, the question becomes: is it representative of the larger population? We believe it is. Given the homogenous nature of this population (those working in the fusion centers), it is doubtful a larger sample size would have produced radically different data.[34] Thus, it can be assumed that the responses gathered by this survey can be used to draw the following general conclusions.

From the perspective of those in the fusion centers, terrorism represents a persistent threat to the safety and security of the United States. Although the level of risk will vary by location and overtime, in an absolute sense, the threat is here to stay.

Much needs to be done to strengthen the ability of fusion centers to detect and analyze cyber threats. Despite a growing number of warnings about cyber security, too little has been done to enhance the capabilities of the fusion centers in this area.[35] A vital conduit for the exchange of cyber intelligence among public and private partners at the local, state, and federal levels remains underdeveloped. As a result, our level of cyber awareness and our ability to respond to threats are not what they could (or should) be. The US' national network of fusion centers is not being fully leveraged in the struggle to address a growing cyber threat to homeland security.

The national network of state and major urban area fusion centers is supporting greater information sharing. A majority of respondents reported that they send and receive information from local, state, and federal authorities on a regular basis. The fusion centers are acting as hubs for information — but are they acting as hubs for intelligence? At this point, the answer is: not quite, not yet. According to the results of HSPI's survey, the ability and frequency with which fusion centers conduct regional threat assessments is anemic at best, despite the fact that both the *Fusion Center Guidelines* and *Baseline Capabilities Supplement* from DHS and the DoJ stress the importance of such.[36]

Two key factors are preventing the fusion centers from fulfilling their mandate as intelligence resources. One factor is the generally homogenous bureaucratic and professional background of those working in the fusion centers. The second factor is the lack of investment in the analytical skills of those working in the centers. These intertwined conditions work against the ability of the centers to fully translate information into intelligence. They prevent the meaningful fulfillment of what was identified at the 2010 New Orleans conference as a Critical Operational Capability — the analysis and assessment of threat information.[37]

"Law enforcement partners built the fusion center and dominate its executive board. Further, the Statewide Integrated Intelligence Plan focuses on law enforcement activities." — **Survey Respondent**

When asked about their professional background, sixty-eight percent of respondents reported that they came from law enforcement. Clearly there is significant overlap between counterterrorism activities and traditional law enforcement. The skill

sets are largely fungible. Yet, there are key differences.

The presence of a predominant law enforcement background within the fusion centers leads to an emphasis on the immediate or strictly utilitarian value of information. Out of necessity, the law enforcement perspective often dismisses information that lacks specific actionable worth — narrowing the focus to the few key pieces of information that may be used to interrupt an attack and make arrests. Obviously this sifting and narrowing capability is of critical value to the law enforcement profession. To employ an analogy, the law enforcement perspective is that of a chess player. To win, they must focus on the match at hand and the moves of their opponent. The perspective of the intelligence analyst, however, is that of a jigsaw puzzle master. To be successful they must discern clues from the environment and establish the proper relationship between the pieces. To perform well, analysts must move beyond simply linear thinking.[38] The skills of the analyst lead to an emphasis on information that expands their understanding of the scope and context of what they see before them. In counterterrorism, both are vital. In the fusion centers, both are needed — in balance. Case specific tactical expertise, such as that supplied by the FBI's JTTFs, must be balanced with contextual strategic understanding, such as that provided by the NCTC or DHS's Office of Intelligence and Analysis.

At present, the fusion centers have too much of the law enforcement perspective and not enough of the analyst. This affects both the focus and the operation of the fusion centers. It leads background and bureaucracy to trump perception of threat. For example, although respondents indicated that terrorism, particularly homegrown terrorism, posed a direct and persistent threat in their jurisdictions — most indicated that law enforcement was the primary operational focus of their fusion centers. Additionally, the presence of a predominant professional background tends to lead to a bias toward specific sources of information. Note, most respondents rated law enforcement entities and the FBI's JTTFs as more important sources of information than DHS and the NCTC — most likely because information from law enforcement or the JTTFs are believed to have immediate and concrete value. Over time, a habitual reliance on certain sources over others will skew perceptions of threat and organizational relationships. The result could be a stove-piping of information, something the fusion centers were created to overcome.

To their credit, those in the fusion center recognize this imbalance. HSPI's survey indicates that those in the fusion center acknowledge the importance of analytical skills. Most respondents selected analysis as the area they would focus on and prioritize in their center for future improvement and development. This conclusion is supported by anecdotal evidence from conversations between the authors of this report and individuals at the National Fusion Center Association.[39] These discussions uncovered frustration on the part of those in the fusion centers over an inability to routinely secure the skills and critical thinking training necessary to produce mature analysts.

To maximize the potential of the fusion centers and fulfill the mandate under which they were created, greater investment needs to be made in the professional development of those working in them. Put another way, we must invest in people to realize the full potential of this institutional asset.

Two areas, in particular, should be stressed. First, as the above suggests, there ought to be increased investments in the analytical and critical thinking skills of those working in the centers. Such investments must go beyond one-time entry (or even sporadic) training curricula, and include regular

opportunities to develop as intelligence analysts — including opportunities for field experience. Second, investments need to be made in the professional incentive structures of the fusion centers. The current guidelines and evaluations that dominate the fusion process and centers too often focus on process rather than outcome.[40] To reap the benefits of data fusion, what is needed is an incentive system that promotes the development of quality reports, standing relationships, and rigorous analysis over the quantity of information received and disseminated.

In a period of budget austerity, additional investments may appear to be an unaffordable expense. Actually, the opposite is true. Investments in people, especially individuals in the first half of their careers, appreciate over time. Such investments led to the direct benefits of better collection, better analysis, and enhanced response capabilities that improve the entire intelligence enterprise and support more informed risk assessments. From these outcomes, a second (fiscal) benefit yields itself — a richer picture of the threats and context under which spending decisions must be made. Consider the following.

The suspicious activity reporting system (SARS) has proven to be more of a passive collection mechanism based on observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. While this is certainly a good baseline for depicting anomalies, and while institutionalizing this type of reporting within police departments and their respective communities has improved collection, it has flooded fusion centers, law enforcement, and other security entities with white noise.

This white noise complicates the intelligence process and distorts resource allocation and deployment decisions. If fusion centers are going to be true homeland security assets capable of focusing attention on emergent risks, then more focused, threat based collection, analysis, and dissemination must be the goal. In essence, we need to move from "passive collection and dissemination" (SARS) and enhance the data through more active and informed processes — including threat based organizational behaviors. One way of achieving this would be to fully leverage the intelligence enterprise through the inclusion of state and local collection efforts.

Yes, these recommendations require spending money. Yet, we recognize the reality of existing budgetary constraints at all levels of governance. We cannot afford to spend blindly, nor do we need to.

Investments in the capabilities of the fusion centers could (and should) build on existing successful efforts within the intelligence and law enforcement communities. The Interagency Threat Assessment and Coordination Group (ITACG) provides an example for how this may be done. ITACG works to support the development of analysts by connecting them with other analysts in the intelligence community and with their counterparts in law enforcement. It also supplies guidance in the construction of tailored intelligence products and facilitates analyst access to classified information. Furthermore, ITACG acts as a bridge between the perspective of law enforcement professionals and the perspective of the analysts — it helps avoid the stove-piping of perspectives and information by connecting elements within the National Counterterrorism Center, DHS, and FBI to individuals within the fusion centers.

Greater investments in the professional development of individuals, retooled incentive systems, and the greater use of programs like the ITACG will move the fusion centers toward the fulfillment of their full potential and promise. There is a real cost to these investments, but there is also

real value — they would lead to improved homeland security and greater economy of force and resources.

CTISR

The Homeland Security Policy Institute's CTISR program represents the first attempt to systematically and routinely collect data from counterterrorism professionals at all levels of government.

In September 2011, the results of HSPI's first CTISR were released. That survey measured the perspectives of local law enforcement (it can be found on HSPI's website: www.homelandsecurity.gwu.edu). Future surveys will continue to measure how counterterrorism and intelligence practitioners — be they analytical or operational — perceive the terrorism threat domain and their role in the intelligence enterprise undertaken to counter it.

Why is this research important? The short answer is that it affects the national security of the United States by identifying threats, best practices, and opportunities for the improvement of our homeland security capabilities.

The longer answer is that practitioner perceptions affect US national security by providing a bottom-up rich picture of the terror threat faced by the United States. How practitioners conceptualize and perceive the threat is of vital importance. Their perceptions affect which threats are detected and when. Furthermore, their perceptions represent an empirical guide for targeting the tools needed to develop anticipatory intelligence. Whether, and how well this is done, depends on the perceptions of the practitioners themselves — as well as how often and how well those perceptions are being measured and analyzed.

With CTISR, the Homeland Security Policy Institute at The George Washington University is committed to continuing this research and learning all we can from the perceptions of those on the front lines of our homeland security.

_____

ENDNOTES

1 Wilber, Del Quentin. 2002. "Tape shows hijacker's traffic stop." Baltimore, MD; The Baltimore Sun. Accessed online 24 April 2012 at: http://www.baltimoresun.com/bal-md.video09jan09,0,7362620.story. National Commission on Terrorist Attacks upon the United States. 2004. 9/11 Commission Report. New York, NY; W. W. Norton & Company. p.4.

2 Office of the Inspector General. 2011. *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*. Washington, DC; US Department of Homeland Security. p. 49. Cardona, Felisa. 2011. "Lakewood mall-device suspect set off '05 bomb at strip club." Denver, CO; The Denver Post. Accessed online 27 April 2012 at: http://www.denverpost.com/news/ci_18373551. Gathright, Alan. 2011. "Man Held in Colorado Mills Bombing Case. Denver, CO; ABC 7 News. Accessed online 27 April 2012 at: http://www.thedenverchannel.com/news/28385153/detail.html. Larson, Jace and Christina Dickinson. 2011. "Suspect in mall devices set off dry-ice bomb before." Denver, CO; 9 News. Accessed online 27 April 2012 at: http://www.9news.com/news/article/205496/207/Suspect-in-mall-devices-set-off-dry-ice-bomb-before.

3 2011. *Implementing 9/11 Commission Recommendations*. Progress Report. Washington, DC; US Department of Homeland Security. p.12.

4 Global Justice Information Sharing Initiative and Homeland Security Advisory Council. 2006. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC; US Department of Justice and US Department of Homeland Security. p.2

5 The number seventy-seven comes from the DHS webpage denoting "Fusion Center Locations and Contact Information," which was updated on 12 March 2012. Accessed online 12 June 2012 at: http://www.dhs.gov/files/programs/gc_1301685827335.shtm.

6 Office of the Inspector General. 2011. *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*. Washington, DC; US Department of Homeland Security. pp.2-5.

7 National Commission on Terrorist Attacks upon the United States. 2004. 9/11 Commission Report. New York, NY; W. W. Norton & Company. pp.416-419. Rosenbach, Eric and Aki J. Peritz. 2009. *Confrontation or Collaboration? Congress and the Intelligence Community*. Cambridge, MA; John F. Kennedy School of Government, Harvard University. p.96.

8 2010. *National Security Strategy*. Washington, DC; Executive Office of the President. p.20.

9 Critical infrastructure is defined as "assets, systems, and networks, both physical or virtual, which are so vital to the United States that incapacitation or destruction would debilitate security, national economic security, and public health or safety." Office of the Inspector General. 2011. *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*. Washington, DC; US Department of Homeland Security. p.5.

10 Global Justice Information Sharing Initiative and Homeland Security Advisory Council. 2006. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC; US Department of Justice and US Department of Homeland Security. p.10.

11 Global Justice Information Sharing Initiative and Homeland Security Advisory Council. 2006. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC; US Department of Justice and US Department of Homeland Security. pp.11-12. Lambert, David. 2010. "Intelligence-Led Policing in a Fusion Center." FBI Law Enforcement Bulletin. Washington, DC; Federal Bureau of Investigation. Accessed online 22 April 2012 at: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/Dec2010/intelligence_feature.

12 Global Justice Information Sharing Initiative and Homeland Security Advisory Council. 2006. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC; US Department of Justice and US Department of Homeland Security. pp.11-12,D-3,D-4.

13 Office of the Inspector General. 2011. *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*. Washington, DC; US Department of Homeland Security. p.12.

14 Associated Press. "Tensions with Iran raise US safety concerns, but intelligence official says attack unlikely." New York, NY; Fox News. Accessed on 16 May 2012 at: http://www.foxnews.com/politics/2012/02/17/tensions-with-iran-raise-us-concern-possible-terror-attack/.

15 Cilluffo, Frank J., Joseph R. Clark, and Michael P. Downing. 2011. "Counterterrorism Intelligence: Law Enforcement Perspectives" Research Brief Volume 1, Number 1. Washington, DC; Homeland Security Policy Institute. Bjelopera, Jerome P. and Mark A. Randol. 2010. "American Jihadist Terrorism: Combating a Complex Threat." Washington, DC; Congressional Research Service. Raduege, Harry and Paul Nadeau. 2012. "We need lots more cyber patriots." San Antonio, TX; *San Antonio Express*. Accessed online 27 April 2012 at: http://www.mysanantonio.com/opinion/commentary/article/We-need-lots-more-cyber-patriots-3492256.php. Cilluffo, Frank J. 2012. "The Iranian Cyber Threat to the United States." Testimony before the Committee on Homeland Security's Subcommittee on Counterterrorism and Intelligence, and Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies. Washington, DC; US House of Representatives. Accessed on 27 April 2012 at: http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo.pdf. Apuzzo, Matt, Anne Gearan, Adam Goldman, Alicia A. Caldwell, and Randy Herschaft. 2012. "Law enforcement on lookout amid Iran tensions." Springfield, VA; *Army Times*. Accessed on 27 April 2012 at: http://www.armytimes.com/news/2012/02/ap-counterterrorism-officials-lookout-iranian-operatives-021712/.

16 National Fusion Center Association website. Accessed on 30 April 2012 at: http://www.nfcausa.org/.

17 For any of the three measures of central tendency (mean, median, or mode) the average response rate for each question was about the same — 48.77, 49, and 48 respectively.

18 HSPI bears sole responsibility for the survey itself. The questions were written, edited, and ordered by the HSPI. Neither SurveyMonkey nor IBM supplied any support for this survey. The use of their services and/or products should not be construed as an endorsement by HSPI or The George Washington University. For more about either SurveryMonkey or SPSS, see their respective websites http://www.surveymonkey.com/mp/aboutus/ and http://www-01.ibm.com/software/analytics/spss/.

19 United States Government Accountability Office. 2010. Federal Agencies Are Helping Fusion Centers Build Capabilities and Protect Privacy, but Could Better Measure Results. GAO-10-972. Washington, DC; GAO. p.9. Accessed online 30 April 2012 at: http://www.gao.gov/assets/320/310268.pdf.

20 The 2010 statistics suggest that at most 3,708 individuals are working in the fusion centers. This number was arrived at via the following. Assuming one-quarter of the centers have less than ten workers produces a maximum number of 162 (72*.25=18 and 18*9=162). Then assuming half have more than ten but fewer than fifty workers produces a maximum number of 1,764 (72*.50=36 and 36*49=1764). Finally, assuming the final quarter of the centers have more than fifty but fewer than one hundred employees produces a maximum number of 1,782 (72*.25=18 and 18*99=1782).

21 This was asked as an open question — no categories were supplied. Based on the answers provided, responses were categorized as either Domestic/Homegrown Jihadi Terrorists, Domestic/Homegrown Non-Jihadi Terrorists, Foreign Jihadi Terrorists, Drug Trafficking Organizations/Organized Crime, or Multiple/Uncategorized.

22 Because several respondents gave multiple answers, the number of comments exceeds the number of respondents.

23 Again, because several respondents gave multiple answers, the number of comments exceeds the number of respondents.

24 Cilluffo, Frank J, Joseph R. Clark, and Michael P. Downing. 2011. "Counterterrorism Intelligence: Law Enforcement Perspectives." Research Brief. Volume 1, Number 1. Washington, DC; Homeland Security Policy Institute. Available at: http://www.gwumc.edu/hspi/policy/researchbrief901_ctintellocallaw.cfm.

25 Cilluffo, Frank J, Joseph R. Clark, and Michael P. Downing. 2011. "Counterterrorism Intelligence: Law Enforcement Perspectives." Research Brief. Volume 1, Number 1. Washington, DC; Homeland Security Policy Institute. pp.10,12. Available at: http://www.gwumc.edu/hspi/policy/researchbrief901_ctintellocallaw.cfm.

26 An examination of the chart (FIGURE 22) reveals general downward trend for all four of the tasks. The chart gives the false impression that there is less data in the 5 and 6 rankings than the first four. This occurs because the relative importance questions contained two additional tasks — the development and use of intelligence doctrine and the acquisition and use of technological resources. Respondents consistently placed these two at the least important end of the the scale. For example, 22.0% of respondents ranked intelligence doctrine as a 5 and 46% ranked it as a 6. In regard to technological resources, 32% of respondents ranked them as a 5 and 34% as a 6.

27 The survey's questions regarding capabilities included two contained two additional tasks — the use of intelligence doctrine and technological resources. Survey data regarding doctrine suggests a high level of capability — it tied dissemination, then drops and plateaus at 13.5% for ratings 2 and 3, before dropping to 5.4% at rating 4. From there it jumps back to 16.2% for rating 5 and 24.3% for rating 6. These results are indicative of an expressed perception regarding the importance of following established guidelines. Technological resources were rated as follows: 13.3% at 1, 20% at 2, 17.8% at 3, 20% at 4, 13.3% at 5, and 15.6% at 6.

28 The survey's questions regarding areas of improvement included two contained two additional areas — intelligence doctrine and technological resources. In regard to doctrine, survey responses suggest those working in the fusion centers rate it as the area with the least need for improvement. On the 1 to 6 scales, the response rate for each ranking were as follows: 8.5% at 1, 4.3% at 2, 23.4% at 3, 14.9% at 4, 17% at 5, and 31.9% at 6. The results concerning technological resources are reported the text and with FIGURE 26.

29 Office of the Inspector General. 2011. *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*. Washington, DC; US Department of Homeland Security. pp.2-5.

30 United States Government Accountability Office. 2010. Federal Agencies Are Helping Fusion Centers Build Capabilities and Protect Privacy, but Could Better Measure Results. GAO-10-972. Washington, DC; GAO. pp.8-9. Accessed online 30 April 2012 at: http://www.gao.gov/assets/320/310268.pdf.

31 This question was asked with an ordinal set of categories. They were: Entry level — I am trained, but still learning mastering the skills and competencies of my position; Experienced Practitioner — I have mastered the skills and competencies of my position, and am becoming familiar with the skills and competencies of those in superior positions; Seasoned Veteran — Having mastered the skills and competencies of my profession, and with deep knowledge derived from extensive observation or participation, I am now often called upon to provide training guidance or supervision to juniors; Senior Leader — I have mastered the skills and competencies of my profession and now provide input or direction in regard to organizational decisions.

32 This inquiry was asked as a set of three different question, each with a slightly different emphasis. One question focused on private sector tools in general, of the forty-eight people who answered this question, 25% said yes there were tools that should be brought over to the fusion centers. Another question focused on tools for gathering information, forty-seven responded, 19.1% said yes. A third question focus on private tools for disseminating information. Forty-eight individuals answered this question, 21.7% said yes there were.

33 Chava Frankfort-Nachmias and David Nachmias. 2008. Research Methods in the Social Sciences. Seventh Edition. New York, NY; Worth Publishers. pp.177-182. Pindyck, Robert S. and Daniel L. Rubinfeld. 1998. Econometric Models and Economic Forecasts. Boston, MA; Irwin McGraw-Hill. pp.19-56.

34 The caveat being — at this moment in time. As the populations of the fusion centers become more diverse overtime, the validity of this assumption may come into question.

35 Ryan, Jason. 2012. "FBI Director Says Cyberthreats Will Surpass Threat From Terrorists" New York, NY; ABC News. Accessed online 06 June 2012 at: http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/.

36 Global Justice Information Sharing Initiative and Homeland Security Advisory Council. 2006. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC; US Department of Justice and US Department of Homeland Security. Global Justice Information Sharing Initiative. 2008. *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines*. Washington, DC; US Department of Justice and US Department of Homeland Security.

37 Office of the Inspector General. 2011. *DHS' Efforts To Coordinate and Enhance Its Support and Information Sharing With Fusion Centers*. Washington, DC; US Department of Homeland Security. p.12.

38 Lowenthal, Mark M. 2012. *Intelligence: from Secrets to Policy*. Fifth Edition. Washing, DC; CQ Press. pp.119-162.

39 January through February 2012 personal conversations between Joseph Clark and Mike Sena, President of the National Fusion Center Association. On 06 June 2012, Sena testified to this same point before the US House of Representatives' Subcommittee on Emergency Preparedness, Response, and Communications. His testimony may be found here: http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Sena.pdf.

40 2010. *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*. Washing, DC; US Government Accountability Office.

ISBN: 978-0-9839904-4-4

The George Washington University Homeland Security Policy Institute

CTISR

Counterterrorism Intelligence Survey Research

Parati! **Be Ready!**