Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness

Hamilton Bean

INTRODUCTION

Information sharing between federal, state, and local agencies is a key element of the U.S. government's homeland security strategy. For federal officials, the post-9/11 threat environment requires a "trusted partnership" among federal, state, and local agencies to "make information sharing integrated, interconnected, effective and as automatic as possible in order to ensure our national security."[1] To support this vision, the Department of Homeland Security (DHS) and Department of Justice (DOJ) administer more than a dozen homeland security-related information-sharing systems.[2] Additionally, numerous governmental, commercial, and non-governmental organizations provide officials with homeland security alerts, updates, and databases to support preparedness efforts.[3] State-level "fusion centers" also integrate, analyze, and disseminate "all-source" homeland security information.

The 9/11 terrorist attacks focused public attention on the need for better information sharing among intelligence, law enforcement, and emergency management agencies. For example, the report of the Joint Inquiry of the House and Senate Intelligence Committees, which investigated the circumstances surrounding 9/11, noted that "one of the most significant problems examined during the open hearings was the lack of information sharing between agencies."[4] Similarly, the 9/11 Commission's *Final Report* concluded: "The biggest impediment to all-source analysis – to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information."[5] As a result, the 9/11 Commission stated that agencies "should provide incentives for sharing, to restore a better balance between security and shared knowledge."[6] Many of the findings of the Joint Inquiry and the 9/11 Commission were codified into law as part of the Intelligence Reform and Terrorism Prevention Act of 2004. Additionally, former President Bush issued several executive orders requiring federal agencies to develop and implement policies and systems designed to enhance information sharing. These efforts culminated in the 2007 *National Strategy for Information Sharing*.[7]

More than two decades of research has correlated information technology use with organizational effectiveness.[8] As a result, there has been little reason for officials to doubt the premise that improving the country's information-sharing systems will enhance homeland security preparedness.[9] Enormous financial, human, and technological resources have thus been dedicated to information-sharing initiatives across federal, state, and local levels.[10] It is therefore striking that so few empirical studies have sought to confirm the basic premises underlying information-sharing discourse and organizational practice.[11] One reason to reexamine these premises is that results have been marginal or counterintuitive in studies that have attempted to correlate information sharing with decision quality,[12] emergency preparedness,[13] response planning,[14] and law enforcement productivity and effectiveness.[15] These studies generally affirm a 2005 Congressional Research Service (CRS) report which found that "although important, the benefits of sharing information are often difficult to

discern, while the risks and costs of sharing are direct and foreseeable."[16] Additionally, recent reports by both the Inspector General of the Office of the Director of National Intelligence and the Markel Foundation indicated that major challenges in implementing information-sharing initiatives endure.[17]

Admittedly, the government's information-sharing strategy will take many years to implement, and some might argue that evaluating the strategy's efficacy is premature. The goal of this preliminary study is to explore how officials make sense of the connection between homeland security information sharing and preparedness at the local level. In the best case, information sharing evokes images of progress, technological sophistication, security, collaboration, and reform. This study suggests, however, that information sharing also evokes images of turf war, bureaucratic ineptitude, irrelevance, and technological obsolescence. The perspective on information sharing advanced herein is based on the principle that organizational discourse (e.g., the speech and writing of organizational members) and symbolism help to generate understandings of information sharing and preparedness in ways that influence practice.[18] Exploring this discourse and symbolism can, ideally, help stakeholders better design, implement, conduct, and monitor information-sharing efforts that meet preparedness objectives.

This study first reviews recent research concerning information sharing and preparedness to suggest why the assumed definitions of these concepts, and the relationship between them, requires a second look. The initial attempt to provide that second look involved using the government's premises and relevant scholarly literature to generate hypotheses and a survey instrument. The survey results, however, mostly reinforced the ambiguous findings of earlier empirical studies. A communication perspective and respondent interviews attempted to account for this ambiguity. After describing the theoretical perspectives and methodologies used herein, this study provides an analysis of the survey and interview responses. It concludes with a discussion of implications for both research and policy.

THE RELATIONSHIP BETWEEN INFORMATION SHARING AND PREPAREDNESS

William V. Pelfey explained how information sharing ideally leads to improved awareness and preparedness: "If … information sharing [is] effective, threats, risks, and vulnerabilities can be effectively identified, targets can be appropriately hardened, and suspects identified while an event is still in its inchoate stage."[19] Thus, officials who access homeland security information-sharing systems on a routine basis should generally be more aware of potential threats than those who seldom access such systems.[20] Frequency of information system use has also been found to correlate with decision quality.[21] Therefore, based on the posited relationships among frequency of system use, awareness, and decision quality:

> **Hypothesis 1$_A$**: *Frequency of homeland security information-sharing system use will influence awareness of homeland security threats.*

Hypothesis 1B: *Frequency of homeland security information-sharing system use will influence the perceived level of organizational preparedness.*

The ISE [Information Sharing Environment] Implementation Plan notes that information quality issues have hampered information-sharing efforts: "Most critical infrastructure sectors … are still concerned with the limited quantity and quality of information and the need for more specific, timely, and actionable information."[22] In their updated review of the information systems success literature, William H. Delone and Ephram R. McLean found a significant correlation between "information quality" and "individual impacts."[23] Accuracy, timeliness, completeness, relevance, and consistency defined information quality while decision-making performance, job effectiveness, and quality of work defined individual impacts. It is thus reasonable to assume that stakeholders who find the information available via information-sharing systems of high quality will tend to use those systems more frequently and report higher levels of job effectiveness than those who perceive the information quality to be low. Therefore:

Hypothesis 2A: *Level of perceived homeland security information quality will influence frequency of information-sharing system use.*

Hypothesis 2B: *Level of perceived homeland security information quality will influence perceived level of job effectiveness.*

The concept of preparedness eludes agreed upon definitions and measures. Ronald D. Fricker, Jerry O. Jacobson, and Lois M. Davis state:

> Because of the lack of authoritative threat and outcome assessments, preparedness or lack thereof in any particular jurisdiction is largely a matter of subjective opinion. Without comprehensive threat assessments, it is exceptionally difficult to define how much preparation is enough and hence specify what 'appropriate' preparedness is for any jurisdiction.[24]

Pelfrey attempted to establish a more concrete definition of preparedness by explaining that preparedness can be seen as both a "cycle" and an "end-state." As a cycle, the four phases of preparedness are prevention, awareness, response, and recovery – success in all four areas is required for preparedness efforts to be effective, according to Pelfrey. Although emergency management officials may engage in various prevention activities – protection, preemption, deterrence, and mitigation – these activities are more often the responsibility of law enforcement. Awareness, response, and recovery, however, concern emergency managers. For example, emergency managers are responsible for being *aware* of the early signs of a chemical or biological attack, *responding* to an emergency scene (i.e., containment, control, management of the incident, mitigation, and treatment), and *recovery* (i.e., rehabilitation, restoration, and repair).[25]

Preparedness is also defined – and more commonly understood by the public – as an end-state. The assertion that "our organization is prepared for homeland security emergencies" connotes the end-state of meaning of preparedness. Pelfrey argues that the cycle framework is more appropriate for homeland security practitioners than the end-state framework because preparedness depends on "enactment" within an ever-shifting social context. This study explores the government's premise that homeland

security information sharing supports preparedness using both the end-state meaning of preparedness (tested in Hypothesis 1_B above), as well as the four-part cycle of preparedness described by Pelfrey. The second phase of the preparedness cycle, "awareness," is accounted for in Hypothesis 1_A above. For reasons discussed below, information sharing is viewed here as contributing mainly to the first two phases of the preparedness cycle (prevention and awareness), with response and recovery capabilities being largely unrelated to the frequency of information-sharing system use. Therefore:

> **Hypothesis 3_A**: *Frequency of homeland security information-sharing system use will influence perceived ability to "prevent" homeland security emergencies.*
>
> **Hypothesis 3_B**: *Frequency of homeland security information-sharing system use will have no significant influence on perceived ability to "respond" to homeland security emergencies.*
>
> **Hypothesis 3_C**: *Frequency of homeland security information- sharing system use will have no significant influence on perceived ability to "recover" from homeland security emergencies.*

Studies by Brian J. Gerber et al. and Martin J. Zaworski underscored the ambiguous relationship between information sharing and preparedness.[26] Gerber et al. tested the hypothesis that state-level government communication of threat information to municipal government agencies aids in preparedness action. This hypothesis was only partially supported. In one model, increasing state government communication of threat and other related information to municipal government actually *decreased* preparedness action. To account for this unexpected finding, the authors stated: "These … results can be viewed as coherent if one accepts this premise: Information sharing from state to municipal officials should matter on an issue of coordination [i.e., adopting new mutual aid agreements] but should matter less on whether a city is able to actually perform a [homeland security] plan test."[27] From this perspective, information sharing contributes to awareness and prevention, but it may not necessarily help in response and recovery efforts (Hypotheses 3_B and 3_C).

Finally, in a study of whether automated information sharing helped law enforcement officers work better, Zaworksi found no significant difference in perceived effectiveness or performance between the group of officers that used automated information-sharing technology and the one that did not.[28] Additionally, "There was no difference between [the group that used automated information sharing technology and the one that did not] in how they think [the technology] affects their productivity [and] essentially no difference between the two groups in how they saw the role of information sharing in making arrests."[29] Zaworksi stated: "Because [test group] officers have access to regional information and thus would seem to be better equipped to make arrests, this result was unexpected."[30] Zaworksi speculated that differing management climates within the control and test groups explained this result; but when combined with the findings from the studies mentioned above, taking another look at how homeland security information sharing relates to preparedness is warranted.

METHODS

This study involved two phases. In the first phase, a survey was administered to information-sharing system users to test hypothesized relationships between information sharing and preparedness. Support for the hypothesized relationships was generally weak; therefore, in the second phase of the study, interviews were conducted with homeland security, law enforcement, and emergency management officials to better understand how these officials made sense of the meanings of and interconnections between information sharing and preparedness.

In Phase 1, an online survey was administered to LLIS.gov (Lessons Learned Information Sharing) members to understand their perceptions and practices concerning information sharing and preparedness. LLIS.gov is a national network linking emergency response providers and homeland security officials. LLIS.gov "seeks to improve preparedness nationwide by allowing local, state, and federal homeland security and response professionals to tap into a wealth of front-line expertise on the most effective planning, training, equipping, and operational practices for preventing, preparing for, responding to, and recovering from acts of terrorism."[31] To access LLIS.gov, one must generally be an emergency response provider, law enforcement official, or a homeland security official at the local, state, or federal level.

LLIS.gov administrators permitted the posting of a twenty-seven-item survey on the homepage of the website, which was available to registered users from May 1, 2007 to May 15, 2007; 101 responses, eighty-three of which were mostly complete, were received. All responses were anonymous. The terms and conditions governing the use of LLIS.gov precluded random or stratified sampling techniques. In this study, the correlation coefficient and probability values for linear models containing two variables are reported. Results from this sample are likely not representative of the LLIS.gov user population. The sample may under-represent users who engage in information-sharing and preparedness activities yet are too busy to participate in an online survey. Certainly, such users might have answered survey questions differently than did the sample. As a result, findings from this study are not generalizable to the LLIS.gov population. Nevertheless, convenience sampling is often used in exploratory research, and the results can still provide important insights.[32]

Because of the limitations of the survey, and the ambiguity surrounding conceptions of information sharing and preparedness, a second research phase was necessary. Phase 2 involved interviews with information-sharing systems users from May 15 to August 3, 2007. Interviews were semi-structured, and each lasted an average of forty minutes. Interview questions are provided in Appendix A. In general, interview themes were related to respondents' attitudes, perceptions, and practices concerning information sharing and preparedness. A semi-structured approach permitted more detailed questions based on the interviewees' responses. In other words, respondent interview techniques were used to: (1) elicit respondents' understandings of "information sharing," "preparedness," and associated concepts; (2) identify the decisive elements of an expressed opinion concerning the relationship between these concepts; and (3) to determine what influenced this opinion.[33] One administrator for a federal-level information-sharing system and nine LLIS.gov users scattered across the country were

interviewed, for a total of ten interviews. The nominal titles of the interview participants are listed in Appendix A.

FINDINGS

PHASE 1: SURVEY

Appendix A lists several tables which provide descriptive information about the survey respondents. Respondents' use of and perceptions about homeland security information sharing and associated systems, as well as an overview of the hypotheses and survey results are provided in Table 1.

Table 1: Information Sharing and Preparedness Hypotheses and Results

Hypothesis	Results
Hypothesis 1_A. Frequency of homeland security information-sharing system use will influence "awareness" of homeland security threats.	Respondents who use homeland security information-sharing system more frequently are significantly more likely to report being aware of homeland security threats. (r = .25, p = .022)
Hypothesis 1_B. Frequency of homeland security information-sharing system use will influence the perceived level of organizational preparedness ("end-state").	No significant association was found between participants' frequency of information-sharing system use and perceived level of organizational preparedness ("end-state").
Hypothesis 2_A. Level of perceived homeland security information quality will influence frequency of information-sharing system use.	No significant association was found between perceived information quality and frequency of information-sharing system use.
Hypothesis 2_B. Level of perceived homeland security information quality will influence perceived level of job effectiveness.	There is a significant positive relationship between homeland security information quality and perceived level of job effectiveness. (r = .23, p = .046)
Hypothesis 3_A. Frequency of homeland security information-sharing system use will influence perceived ability to "prevent" homeland security emergencies.	No significant association was found between participants' frequency of information-sharing system use and perceived ability to prevent homeland security emergencies.*
Hypothesis 3_B. Frequency of homeland security information-sharing system use will have no significant influence on perceived ability to "respond" to homeland security emergencies.	No significant association was found between participants' frequency of information-sharing system use and perceived ability to respond homeland security emergencies.
Hypothesis 3_C. Frequency of homeland security information-sharing system use will have no significant influence on perceived ability to "recover" from homeland security emergencies.	No significant association was found between participants' frequency of information-sharing system use and perceived ability to recover from homeland security emergencies.

* Result requires explanation provided below.

As predicted, respondents who more frequently used homeland security information-sharing systems were significantly more likely to report being aware of homeland security threats (r = .25, p = .022). However, frequency of use generally did not significantly correlate with the remaining three phases of the preparedness cycle described by Pelfrey (prevention, response, and recovery), nor did frequency of use significantly correlate with preparedness as an end-state. Respondents saw the use of LLIS.gov as overwhelmingly unhelpful in preventing homeland security emergencies (this finding is unsurprising when considering that LLIS.gov does not claim to provide "actionable" information); therefore, the use of LLIS.gov was disaggregated from "other information sharing systems" in order to determine whether those other systems (e.g., COPLINK, LEO, RISS) were perceived as being more helpful. When this disaggregation was performed, there was, in fact, a significant association between participants' frequency of system use and perceived ability to prevent homeland security emergencies (r = .25, p = .026). Thus, all measures of preparedness with both the combined and disaggregated system-use variables were tested; prevention was the only measure where the results changed significantly.[34]

Supporting studies within the information-systems success literature, there was a significant positive relationship between homeland security information quality and perceived level of job effectiveness (r = .23, p = .046). However, perceived information quality was not significantly correlated with information-sharing-system frequency of use. Frequency of use is a widely employed – but increasingly contested – variable in information systems research;[35] therefore, the survey results were also analyzed using respondents' overall opinion about the usefulness of information-sharing systems. There was no change in the results when opinion was substituted for frequency of use as an independent variable. In other words, those who held a more favorable opinion of information-sharing systems did not perceive themselves or their organizations to be significantly more (or less) prepared for homeland security emergencies than those who held a less favorable opinion. However, emergency managers (M = 4.71, SD = 1.15) were more likely than the other occupational subgroups (M = 3.98, SD = 1.46), such as law enforcement or public health personnel, to believe themselves to be prepared for homeland security threats when preparedness was defined as an end-state ($t(81)$ = 2.08, p = .041).

Overall, however, there is little evidence that increased information-sharing system use significantly increases perceived level of preparedness when preparedness is defined as an end-state. Nevertheless, there is some support for the premise that with more frequent use of information-sharing systems, users will tend to perceive themselves to be more aware of potential homeland security threats and perceive their organizations to be more capable of preventing homeland security emergencies. This finding reinforces Gerber et al.'s claim that information sharing contributes mainly to the first two phases of the preparedness cycle (prevention and awareness), while perceived improvements to response and recovery remain largely independent of information-sharing efforts.[36] Discussion with survey respondents would be needed, however, to adequately explain the dynamics of this situation.

These results also suggest that one's perceived level of job effectiveness tends to rise as the perceived quality of homeland security information increases. This finding

reinforces and extends Zaworski's conclusion that information "comprehensiveness" assists law enforcement officers in doing their jobs.[37] This study suggests that other components of information quality (accuracy, timeliness, relevance, and consistency) are important for increasing perceived job effectiveness in a homeland security context. These results, however, say little about the meanings stakeholders give to the terms information sharing and preparedness.

PHASE 2: INTERVIEWS

The section above outlined the theoretical case for predicting a significant, causal relationship between information sharing and preparedness. While there were important limitations to the survey, as well as some indications of support for a handful of hypotheses, findings also affirmed the ambiguous and unexpected results of earlier empirical studies. What then accounts for the ambiguous relationship between information sharing and preparedness? A communication perspective helps to explain this ambiguity. Specifically, a communication perspective emphasizes the active role that audiences play in categorizing messages via pre-existing historical, cultural, and political frameworks, and evaluating those messages in terms of source credibility, intention, and trustworthiness.[38] This perspective maintains that information sharing and preparedness are not objective phenomena with concrete properties and causal, law-like effects; rather they "are labels for the organized, institutional claim-making process which constitutes these phenomena."[39] In other words, information sharing and preparedness are the result of social processes through which groups assert and negotiate which objects, concepts, and practices represent those activities.[40] A communication perspective makes sense for this study because it is important to understand how stakeholders construct the meanings of homeland security information sharing and preparedness and how they act in accordance with those meanings.

Interview responses from ten homeland security, law enforcement, and emergency management officials suggest the following explanations: (1) definitions of information sharing and preparedness are contextually based, multiple, and at times conflicting, making the impact of information sharing difficult to ascertain;(2) information received via these systems is usually vague, which constrains preparedness action; (3) information glut and associated responses dampen the influence of information sharing on preparedness; and (4) both information sharing and preparedness occur in the context of institutional norms that shape interpretations of message credibility, intention, and trustworthiness.

The Problem of Definition

No consensus definition of information sharing arose from the interview respondents. Instead, respondents offered an array of definitions for information sharing, many of which expressed dissatisfaction with current processes:

Information sharing means a centralized area where you can grab stuff.

> [Information sharing means] *every little bit of information about everything that has to do with day-to-day crises to doom-and-gloom…all day, everyday, without filter.*
>
> *There's a very fine line between information and shit, and I think what we see a lot of times is that everybody's swapping shit.*
>
> *I don't know, and that's one of the problems I think we have right now.*

Several respondents also defined information sharing as a task that local officials are expected to do without much reciprocity from the federal level.

> *Information sharing means a two-way street, but more often it's a one-way street.*
>
> *[Information sharing] means information going to the JTTF* [Joint Terrorism Task Force] *and very little coming back.*

One law enforcement official explained the roots of his frustration with the "one-way street." He stated that "the FBI has been horrible to work with. They've been a huge stumbling block." This official explained that his city's police department had discovered the name of a resident on a terrorist watch list. When he queried the FBI as to why this might be the case, the response he received was, "I can't tell you." The response was all the more frustrating because the FBI had earlier sponsored this official's security clearance in order to facilitate information sharing. This official stated: "They [the FBI] have an elitist attitude. Of course, they'll tell you differently. They come here and say 'we're here to help' and 'we'll share our information,' but it's all just smoke and mirrors. They want *you* to give *them* information so they can put it in a file somewhere."

Vague Information

For the majority of respondents, vague information created significant obstacles to improving preparedness. Respondents commented on the quality of the homeland security information they received from federal-level systems.

> *It's all after-the-fact. There's little value added.*
>
> *When it first came out, I was pretty active on LLIS, but then I thought: 'Why am I doing this?'*
>
> *It's mostly useless.*

One respondent elaborated on how vague information constrains preparedness action:

> *We'll get a vague warning about threats to water treatment facilities, and there are several water treatment facilities in this area. The warning will be based on 'unconfirmed information.' So I'm left wondering whether I should I go speak with the water treatment operators. I'll call the FBI to get more information and they'll say, 'we don't have any more information.' I can't get any specifics. There is just not enough detail for me to go to the city and request the money to harden those facilities. If I go to my chief with that information, he's going to laugh at me.*

Respondents explained that the types of information that would be useful for them in doing their jobs would include:

> *Geographically-specific information and intelligence would be helpful instead of broad, general statements about threats.*
>
> *Specific information about suspects and bad guys.*
>
> *Actionable intelligence. This is something I need to know because it's something I could or should react to.*[41]

Respondents universally valued interpersonal communication with their colleagues, finding it the most useful source of relevant information. One respondent explained: "The best source for information I get is from my contemporaries in other jurisdictions close by that I work with on a regular basis. We meet frequently and email frequently, [my colleagues provide] information that has been vetted and is of value." The value officials placed on interpersonal communication likely stems from the opportunity it provides for officials to demonstrate their expertise, value, and influence, and to "bespeak their past and future competence."[42] Nevertheless, the government's information-sharing strategy continues to emphasize impersonal electronic systems, databases, and alerts.

Information Glut

Information glut is a perennial problem in intelligence and national security-related organizations.[43] The volume of information respondents typically receive has led some to simply delete or ignore much of it.

> *If I didn't have department to run it would be kind of fun to just sit at home and look at all this stuff.*
>
> *I can't tell you how many passwords I have. They say, 'Here's the next thing. It's a special thing for senior government officials, just log on.' I don't even do it anymore … I'll look at them and there's never been anything on there that's of any value…. To be honest, I do this, and my guess is other people do it as well in my position, is that an awful lot of stuff gets deleted without ever being read…. If everything's a priority, nothing's a priority.*

Respondents emphasized the need for some sort of information "filter." Whether state-level fusion centers – the emerging linchpin in the government's information-sharing strategy – can successfully fulfill that role is an open question. Some respondents recognized the value of the fusions centers, while others have not yet perceived any benefit.

> *[Fusion centers] need to be staffed by more than just law enforcement … the all hazards approach has not been embraced by a lot of areas.*
>
> *We need people in leadership positions deciding what's important.*

What I'd prefer is a system where we recognize the sender as someone who has credibility and the information is not just something somebody's sending to kind of cover their ass.

We're looking at getting a watch officer to distill this information down into a daily brief to help reduce some of the time spent reading stuff.

Institutional Norms

Institutional identities play a significant role in how information sharing is interpreted. Several local officials indicated that longstanding distrust of the federal bureaucracy has not waned in recent years.

You've got all these hyper [federal-level] people bouncing around on their cell phones and Blackberries not paying attention to what's going on because they're all trying to share some shit so that they're not the one blamed for not passing something on.

There are a lot of people in Washington with word processors and a great imagination typing up more and more stuff that none of us have time to do anyway.

Other officials, however, indicated a more positive relationship. "We've always had excellent working relationships with [federal officials]," stated one official. Several respondents also acknowledged that federal information sharing was hindered by antiquated classification rules and procedures the government is currently trying to address. As one official explained:

Our law enforcement officials learned about a chlorine truck that needed to be tracked. Classification issues prevented the information from being shared with the fire department and emergency management organizations – but those are the agencies that have done the training and can best respond, so they need to know. By federal rules, they can't share the information about the truck beyond law enforcement. It's [still] an issue at this point.

These examples suggest that the meaning of information sharing is constructed in reference to institutional identities and local organizational contexts. While many respondents acknowledged that *in principle* information sharing is vital to preparedness, several officials perceived current information-sharing initiatives as a way for federal officials to bridge the government's post-9/11 (and Katrina) credibility gap with the public. The mocking tone of some of the responses highlighted above might, ideally, spur stakeholders to more critically examine current policies and practices. The issues identified by the respondents are certainly well known to many government officials. The government has responded to these challenges, in part, by seeking to foster "a culture of information sharing" within and among federal, state, and local agencies. The comments presented above indicate enduring friction points as the government attempts to change perceptions, align institutional subcultures, and alter information-sharing practices.

CONCLUSION

An assumption circulating within information sharing discourse is that the effectiveness of information sharing can be measured in terms of information flow, distribution, timeliness, coordination, and related system performance measures.[44] The Information Sharing Environment's [ISE] stated mission is to ensure the *ability* of agencies to share information – but just who is responsible for ensuring that such abilities to share information *tangibly* improve preparedness remains unclear. This study indicates that using system performance measures and capabilities to assess the effectiveness of information sharing is inadequate and potentially wasteful and misleading. As one local official in this study explained, "We're in uncharted territory, with a lack of legal assistance, and a lack of leadership in some cases. [Information sharing is done] by a bunch of local people who all of a sudden have got millions of dollars pouring at them, and they're trying to make the best use of it with limited guidelines. It's been very challenging." In developing metrics to assess the benefits of information sharing, officials must engage in the difficult task of relating system use to tangible improvements in preparedness.

Information-sharing initiatives also unfold within varying budgetary constraints and divergent funding priorities. As a result, future research needs to address how financial and structural conditions influence information-sharing processes and practices. This study also suggests the need for comparative and longitudinal research of information sharing. However, future studies that attempt to construct concrete variables for hypothesis testing may similarly confront the contingency of the meanings of information sharing and preparedness. Although information sharing and preparedness are socially-defined concepts, their meanings can be mapped within different organizational contexts and across time using both qualitative and quantitative methods. Doing so can potentially assist policy makers and practitioners assess the utility of information-sharing strategies and the impact of associated organizational change efforts. Assessing whether the users of a given information-sharing system find the system valuable to preparedness efforts, as well as systematically explicating the features of highly useful systems, can aid in the their development. Additionally, a longitudinal approach would help assess how definitions of information sharing and preparedness, their associated practices, and stakeholder perceptions are changing over time.

Finally, attempting to create a "trusted partnership" and a "culture of information sharing" in absence of clear, abundant evidence regarding how information sharing tangibly improves preparedness may ultimately undermine the government's information-sharing strategy. This study highlighted local-level officials' uncertainty regarding the effectiveness of current information-sharing processes. As one respondent concluded: "I hope somebody someplace has more information that they're utilizing to protect the country because I'm not seeing a lot of stuff that's of great value." Given similar findings in recent reports, and the resources being dedicated to information sharing at all levels of government, further scrutiny of how information sharing relates to preparedness is warranted. This preliminary study has provided a modest step in that direction.

APPENDIX A – SELECTED SURVEY DATA

Respondent Demographics (N=83)*

Age		**Gender**		**Education**	
21-29 years	5%	Male	71%	Some college	11%
30-39 years	16%	Female	23%	2 year degree	6%
40-49 years	30%	N/A	6%	4 year degree	17%
50+ years	45%			Some graduate credits	19%
N/A	5%			Master degree or higher	42%
				N/A	5%
Occupation		**Role**		**FEMA Region**	
Emergency Mgmt.	25%	Management	48%	I	5%
Law Enforcement	18%	Operations	18%	II	8%
Fire	5%	Support	8%	III	21%
Public Health	12%	Other	19%	IV	11%
Other	31%			V	11%
N/A	8%			VI	12%
				VII	6%
				VIII	4%
				IX	12%
				X	4%

* Some categories do not total 100% due to some respondents not providing an answer.

Source from Which Most Often Receive Homeland Security Information (N=83)

Homeland security email / bulletins / alerts	34
Face-to-face meetings with colleagues	5
Email or telephone calls with colleagues	17
Newspapers / magazines	5
Radio	1
Television	2
Websites / Databases	18
Other	1

Most Frequently Used Homeland Security Information Sharing Systems

COPLINK, HSIN (Homeland Security Information Network), InfraGard, Intelink, LEO (Law Enforcement Online), LLIS (Lessons Learned Information Sharing), RISS (Regional Information Sharing Systems)

Frequency of Homeland Security Information Sharing Systems Use **(N=83)**

	LLIS	**Other Systems**
Less than once per month	16%	35%
Monthly	48%	22%
Weekly	34%	31%
Daily	2%	12%

Survey Questions Related to Preparedness

In your opinion, how prepared is your organization for homeland security threats in your region? (preparedness as an "end-state")
In your opinion, how *aware* are you personally of homeland security threats facing your region?
In your opinion, how *aware* is your organization of homeland security threats facing your region?
In your opinion, how prepared is your organization to *prevent* a homeland security emergency in your region?
In your opinion, how prepared is your organization to *respond* to a homeland security emergency in your region?
In your opinion, how prepared is your organization to *recover* from a homeland security emergency in your region?

Interview Participants (Nominal Titles)

Administrator, Federal-level Information Sharing System
Assistant Coordinator, County Office of Emergency Management
Assistant General Manager, City Emergency Preparedness Department
Coordinator, Regional Homeland Security
Detective
Director of Municipal Information Sharing System
Director of Public Safety, County-level
Director, City Office of Emergency Management
Director, County Department of Emergency Services
Intelligence Detective

Interview Questions

1. What does "homeland security information" mean to you?
2. How would you characterize the quality of the homeland security information you receive?
3. What kind of information is most helpful to you in terms of doing your job?
4. What does "information sharing" mean to you?
5. What does "preparedness" mean to you?
6. What are the information-sharing activities you engage in? How often? Why (forced/voluntary)? How have these changed over time?
7. In your opinion, how does information sharing relate to preparedness?
8. Please point to any examples of how information sharing has influenced your work.
9. Describe your interactions with federal/state level agencies. Have information-sharing initiatives changed your interactions with them? If so, how?

Hamilton Bean is a Ph.D. candidate in the Department of Communication at the University of Colorado at Boulder. His research investigates the intersection of organizational communication and public policy. His work appears in journals in the fields of intelligence, national security, and homeland security. Since 2005, he has been affiliated with the National Consortium for the Study of Terrorism and Responses to Terrorism (START) – a DHS-funded Center of Excellence based at the University of Maryland. Mr. Bean can be contacted at hamilton.bean@colorado.edu.

This research was supported by the United States Department of Homeland Security through the National Consortium for the Study of Terrorism and Responses to Terrorism (START), grant number N00140510629. However, any opinions, findings, and conclusions or recommendations in this document are those of the author and do not necessarily reflect views of the U.S. Department of Homeland Security. The author thanks Michaela Huber and Lisa Keränen for their assistance in the development of this study.

---

[1] Program Manager, "Information Sharing Environment," speech given before the DNI's Information Sharing Conference & Technology Exposition: "Intelink and Beyond: Dare to Share," Denver, CO (August 26, 2006), 8, http://www.ise.gov/docs/20060822_speech.pdf.

[2] United States Government Accountability Office (GAO), "Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives" GAO-07-455 (Washington, DC: GAO, April 2007), http://www.gao.gov/products/GAO-07-455.

[3] Hamilton Bean and Lisa Keränen, "The Role of Homeland Security Information Bulletins within Emergency Management Organizations: A Case Study of Enactment," *Journal of Homeland Security and Emergency Management* 4, no. 2 (2007), http://www.bepress.com/jhsem/vol4/iss2/6/.

[4] Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, "Report of the Joint Inquiry into the Terrorist Attacks of September 11, 2001" (2003), 637, http://www.gpoaccess.gov/serialset/creports/911.html.

[5] 9/11 Commission, "Final Report of the National Commission on Terrorist Attacks upon the United States" (2004), 416, http://www.9/11commission.gov/.

[6] Ibid., 416.

[7] *National Strategy for Information Sharing*, (2007), http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html.

[8] William H. DeLone and Ephram R. McLean, "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," *Journal of Management Information Systems* 19, no. 4 (2003): 9-30.

[9] For a valuable assessment and critique of this issue, see Calvert Jones, "Intelligence Reform: The Logic of Information Sharing," *Intelligence & National Security* 22, no. 3 (2007): 384-401.

[10] The program manager for the Information Sharing Environment, Ambassador Thomas E. McNamara, commented to *Washington Technology* staff writer, Alice Lipowicz that federal-level investment in information sharing will total hundreds of millions of dollars with additional hundreds of millions of dollars invested at the state and local level. Alice Lipowicz, "Info-sharing is Work In Progress: Negroponte's Plan to Link Federal Agencies Could Run into Millions," *Washington Technology*, December 18, 2006, http://washingtontechnology.com/Articles/2006/12/18/Infosharing-is-work-in-progress.aspx.

[11] Martin J. Zaworski states, "Unfortunately, empirical data establishing a link between information sharing and performance in the law enforcement environment is either extremely difficult to find or non-existent." See Martin J. Zaworski, "Assessing an Automated, Information Sharing Technology in the Post '9-11' Era: Do Local Law Enforcement Officers Think It Meets Their Needs?" doctoral dissertation, Florida International University, Miami, 2004, 186. Excerpted in "Automated Information Sharing: Does It Help Law Enforcement Officers Work Better? *National Institute of Justice Journal*, no. 253 (2006).

[12] Shaila M. Miranda and Carol S. Saunders, "The Social Construction of Meaning: An Alternative Perspective on Information Sharing," *Information Systems Research* 14, no. 1 (2003): 87-106.

[13] Brian J. Gerber and others, "On the Front Line: American Cities and the Challenge of Homeland Security Preparedness," *Urban Affairs Review* 41, no. 2 (2005): 182-210.

[14] Steven R. Haynes and others, "Leveraging and Limiting Practical Drift in Emergency Response Planning," 40th Annual Hawaii International Conference on System Sciences, Waikoloa, HI, 2007, *HICSS 2007*, 200-208.

[15] Zaworski, "Assessing an Automated, Information Sharing Technology in the Post '9-11' Era."

[16] Harold C. Relyea and Jeffrey W. Seifert, "Information Sharing for Homeland Security: A Brief Overview," RL32597 (Washington, DC: Congressional Research Service, January 10, 2005), 33.

[17] Office of the Director of National Intelligence, Office of the Inspector General, "Critical Intelligence Community Management Challenges" (November 12, 2008), http://www.fas.org/irp/news/2009/04/odni-ig-1108.pdf; Markle Foundation Task Force, "Nation At Risk: Policy Makers Need Better Information to Protect the Country" (March 10, 2009), http://www.markletaskforce.org/.

[18] David Grant and others, *The Sage Handbook of Organizational Discourse* (London: Sage, 2004).

[19] William V. Pelfrey, "The Cycle of Preparedness: Establishing a Framework to Prepare for Terrorist Threats," *Journal of Homeland Security and Emergency Management* 2, no. 1 (2005): 9, http://www.bepress.com/jhsem/vol2/iss1/5.

[20] James N. Danziger and Kenneth L. Kraemer, "Computerized Data-Based Systems and Productivity among Professional Workers: The Case of Detectives," *Public Administration Review* 45, no. 1 (1985): 196-209.

[21] DeLone and McLean, "The DeLone and McLean Model of Information Systems Success."

[22] *ISE Implementation Plan* (2006), 6, www.ise.gov.

[23] DeLone and McLean, "The DeLone and McLean Model of Information Systems Success."

[24] Ronald D. Fricker, Jerry O. Jacobson, and Lois M. Davis, "Measuring and Evaluating Local Preparedness for a Chemical or Biological Terrorist Attack," IP-217-OSD (Santa Monica, CA: RAND, 2002), 6.

[25] Pelfrey, "The Cycle of Preparedness."

[26] Brian J. Gerber and others, "On the Front Line;" Zaworski, "Assessing an Automated, Information Sharing Technology in the Post '9-11' Era"

[27] Brian J. Gerber and others, "On the Front Line," 202.

[28] Zaworski, "Assessing an Automated, Information Sharing Technology in the Post '9-11' Era"

[29] Zaworski, "Automated Information Sharing: Does It Help Law Enforcement Officers Work Better?" 25.

[30] Ibid.

[31] Lessons Learned Information Sharing, "Frequently Asked Questions," https://www.llis.dhs.gov/faq.cfm.

[32] Earl Babbie, *The Practice of Social Research*, 6th ed. (Belmont, CA: Wadsworth, 1992).

[33] Thomas Lindlof and Bryan C. Taylor, *Qualitative Research Methods*, 2nd ed. (Thousand Oaks, CA: Sage, 2002), 178.

[34] In this study, participants' frequency of use of LLIS.gov (the survey site) and other information sharing systems besides LLIS.gov were positively correlated ($r = .28$, $p = .010$); therefore, these two frequency variables were averaged.

[35] Michael J. Cuellar and others, "Forty Four Years of Computer Personnel Research: Achievements, Challenges, & the Future," *Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research* (2006), 164-168, http://portal.acm.org/citation.cfm?id=1125214.

[36] Brian J. Gerber and others, "On the Front Line."

[37] Zaworski, "Assessing an Automated, Information Sharing Technology in the Post '9-11' Era."

[38] H. L. Goodall and others, "Strategic Ambiguity, Communication, and Public Diplomacy in an Uncertain World: Principles and Practices," Report # 0604 (Tempe, AZ: Consortium for Strategic Communication, Arizona State University, 2006), 5, http://comops.org/article/116.pdf.

[39] Kathleen J. Tierney and others, *Facing the Unexpected: Disaster Preparedness and Response in the United States* (Washington, DC: Joseph Henry Press, 2001), 17.

[40] Ibid.

[41] These responses underscore that stakeholders face a dilemma in determining an "appropriate" level of equivocality in preparedness messages. Sellnow et al. argue that "unequivocal statements during a crisis might be less valuable than probabilistic statements, reflecting more realistically the lack of precise predictability in many crisis situations and allowing stakeholders to make their own qualitative assessments." This study suggests, however, that an overabundance of equivocal information in pre-event contexts can lead information sharing systems users to devalue those systems. This finding affirms Sellnow et al.'s claim that "the question of appropriate levels of equivocality in crisis messages remains

largely unanswered." Timothy L. Sellnow and others, "Chaos Theory, Informational Needs, and Natural Disasters," *Journal of Applied Communication Research* 30, no. 4 (2002): 269-292, quotes on 288-290.

[42] David Constant and others, "What's Mine Is Ours, Or Is It? A Study of Attitudes About Information Sharing," *Information Systems Research* 5, no. 4 (1994): 400-421, 414.

[43] Rob Johnston, "Analytical Culture in the U.S. Intelligence Community: An Ethnographic Study" (Washington, DC: Center for the Study of Intelligence, 2005), https://www.cia.gov/library.

[44] See Wayne Parent, "Statement of Wayne Parent, Deputy Director of the Office of Operations Coordination, U.S. Department of Homeland Security, before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Committee on Homeland Security, United States House of Representatives," May 10, 2007, http://homeland.house.gov/SiteDocuments/20070510132347-84079.pdf.