NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PREVENTING TERRORISM USING INFORMATION SHARING NETWORKS

by

Paul France

September 2006

Thesis Advisor:	Nadav Morag
Second Reader:	Robert Simeral

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Preventing Terrorism Using Information Sharing Networks		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Paul France			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Many states currently do not have an intelligence fusion center, and therefore, their ability to prevent and deter a terrorist attack is limited by the lack of information sharing. Wisconsin in addition to many states lacks a central hub for information exchange and currently has no system in place that allows the variety of technologies to gain access to a common database to gather and/or exchange information. The vast majority of public safety agencies currently operate their own systems that are incapable of exchanging information. The inability to exchange and/or access information in user-friendly format has inhibited many state and local efforts to keep its citizens safe from the possibility of a terrorist attack.

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. Terrorism Early Warning Systems (TEW's) embody the core of collaboration and are an effective tool to maximize available resources and build trusted relationships. The fusion process should be organized and coordinated on a statewide level between the major Urban Area Security Initiative (UASI) areas and the statewide fusion center concept.

14. SUBJECT TERMS Information Sharing, Network, Intelligence Fusion Center, Terrorism Early Warning System, Wisconsin, Milwaukee			**15. NUMBER OF PAGES** 99
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PREVENTING TERRORISM USING INFORMATION SHARING NETWORKS

Paul C. France
Wisconsin Homeland Security
B.A., University of Wisconsin, 1990
M.S., Hartford University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Paul C. France

Approved by: Nadav Morag, Ph.D.
Thesis Advisor

Captain Robert Simeral, USN (Ret.)
Co-Advisor

Douglas Porch, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Many states currently do not have an intelligence fusion center, and therefore, their ability to prevent and deter a terrorist attack is limited by the lack of information sharing. Wisconsin in addition to many states lacks a central hub for information exchange and currently has no system in place that allows the variety of technologies to gain access to a common database to gather and/or exchange information. The vast majority of public safety agencies currently operate their own systems that are incapable of exchanging information. The inability to exchange and/or access information in user-friendly format has inhibited many state and local efforts to keep its citizens safe from the possibility of a terrorist attack.

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. Terrorism Early Warning Systems (TEW's) embody the core of collaboration and are an effective tool to maximize available resources and build trusted relationships. The fusion process should be organized and coordinated on a statewide level between the major Urban Area Security Initiative (UASI) areas and the statewide fusion center concept.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to dedicate this thesis to my mother, who unexpectedly passed away during my course of study at NPS. Thank you mom for giving me the drive and will to succeed. I know you would have been proud. I miss you. I would like to thank the State of Wisconsin and The Office of Justice Assistance for my sponsorship, and David Steingraber and Michael Kunesh for their support and encouragement in pursuing my degree. Mike, you are more than the Homeland Security Director and my boss, you are a great mentor and I thoroughly enjoy working with you. I sincerely thank both Nadav Morag and Bob Simeral for your excellent insight, knowledge and support helping me complete this thesis. You both are two of the best and most knowledgeable instructors and homeland security professionals; I have ever had the privilege of learning from. It was a pleasure working with the two of you. Finally, I would like to wholeheartedly, thank my family for all of their support. To my beautiful and wonderful wife, Jennifer, thank you for all of your support and encouragement as I worked my way through the homeland security program. I promise to continue to support you in the same way while you are pursuing your academic goals. I am so appreciative of all you do and proud to be your husband. To my precious daughters, Miranda and Samantha, thank you for your understanding while daddy was away at school, always on the computer doing schoolwork, and for being such "little ladies." I am so proud of both of you I promise to make up for lost time and missed events.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Many states currently do not have an intelligence fusion center, and as a consequence, their ability to prevent and deter a terrorist attack is limited by the lack of information sharing. Wisconsin not unlike many states, lacks a central hub for information exchange and currently has no system in place that allows the variety of technologies to gain access to a common database to gather and/or exchange information. The vast majority of public safety agencies currently operate their own systems that are incapable of exchanging information. The inability to exchange and/or access information in user friendly format has inhibited many state and local efforts to keep its citizens safe from the possibility of a terrorist attack. How can information sharing be improved?

Intelligence fusion centers and terrorism early warning systems provide an opportunity for states and locals to break down the informational silos created by historical legal and bureaucratic impediments to information sharing. The intelligence reform efforts continuously underway at the federal level are contributing to an atmosphere that encourages information sharing. However, states must also be key leaders in this area. State and local leaders are positioned to mobilize state homeland security resources and design truly integrated information sharing networks.

States planning to implement a statewide fusion center should learn from those states that have already set up and are operating intelligence fusion centers. A fusion center is a physical location where officials receive, process, and analyze all-source information and synthesize their analyses into intelligence products for dissemination to relevant agencies and officials. Fusion centers can also serve as primary mechanisms for information sharing at the state and local levels. Fusion center analysts process and analyze information from state and local public safety agencies. The center shares it with relevant federal, state, or local agencies. Fusion centers also process information from federal sources, determines its relevance within the state or local jurisdiction, and disseminates it as necessary.

The failure to communicate and share vital information can also hinder investigations. More than one agency investigating a similar case and not sharing information will also lead to the failure of apprehending criminal behavior prior to an incident. In addition, many criminal investigations can have a terrorism nexus. For example, crimes such as dealing in counterfeit currency, credit card fraud, smuggling, and money laundering or trafficking in stolen or forged documents, narcotics trafficking and trafficking in stolen goods are undertaken by various terrorist groups in order to generate funding. This makes it important to communicate in both directions across the organizational divisions between homeland security investigations and traditional criminal investigations.

The failure to exchange information and to connect the dots helped produce the tragic events of 9/11. The culture of information-sharing must be changed from "need to know" to "need to share." The government has a vast amount of information and without a system in place for people to access data there can only be an extremely limited amount of information exchange.

Fusion centers provide a clear link between local and federal public safety agencies. This enables fusion centers to coordinate interagency information sharing more effectively than could be done with the traditional approach. Fusion centers also take an all-source, multidisciplinary approach that facilitates the collection of information from a wide range of sources and perspectives. Fusion centers and terrorism early warning centers can be structured differently and have different missions and some similar obstacles may have to be overcome through different methods. Terrorism early warning centers need to be integrated with state intelligence fusion centers. This creates an information sharing enterprise where information can flow from the local level up through the state to the federal government and flow from the federal level back down to the local level. Information needs to be shared in order to effectively prevent terrorist attacks.

The policy recommendation is to create an information sharing network. This network will consist of a TEW in the city of Milwaukee linked to a statewide fusion center in Madison, Wisconsin. The state fusion center should have direct access to the

National Counter Terrorism Center (NCTC) and Homeland Security Operations Center (HSOC). The information sharing network will be tapped into the national intelligence community so that the state can leverage national intelligence. Personnel and analysts assigned to the Wisconsin Statewide Intelligence Center should have access to the many different databases that store a variety of information. This data could be obtained through a secure porthole allowing the user to log onto one secure porthole and access information from many databases.

An optimum local information sharing network in Wisconsin would have personnel from the following agencies assigned to the statewide fusion center, this list would include:

- Wisconsin State Patrol
- Milwaukee Police Department
- Madison Police Department
- Dane County Sheriff's Office
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Milwaukee Fire Department
- Madison Fire Department
- USDHS Border Patrol
- USDHS Immigration & Customs Enforcement
- Federal Bureau of Investigation
- U.S. Secret Service
- U.S. Postal inspection Service
- Wisconsin Department of Corrections
- Wisconsin Department of Public Health (DHFS)
- Wisconsin Department of Agriculture
- Wisconsin Department of Natural Resources
- Wisconsin Attorney General Office
- Wisconsin Department of Military Affairs
- USDHS Intelligence & Analysis

Wisconsin and additional states that have fusion centers or those that are in the conceptual stage for a statewide intelligence center and/or a local TEW should reach out to the High Intensity Drug Trafficking Areas (HIDTA) and become partners in information sharing. Milwaukee, Wisconsin has a HIDTA office and they should be integrated into the information sharing network. The HIDTA program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. Law enforcement organizations within HIDTA's assess drug trafficking problems and design specific initiatives to reduce or eliminate the production, manufacture, transportation, distribution and chronic use of illegal drugs and money laundering. One of the key priorities of the Program is to assess regional drug threats and facilitate coordination between federal, state and local efforts; to improve the effectiveness and efficiency of drug control efforts to reduce or eliminate the harmful impact of drug trafficking.

The development and exchange of intelligence is not easy. Information sharing not only requires strong leadership; it also requires the commitment, dedication and trust of a diverse group of men and women that agree in the power of collaboration. 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, state and prevent criminal activity. TEWs embody the core of collaboration and as resources decrease, TEWs will become even more of an effective tool to maximize available resources and build trusted relationships. The fusion process should be organized and coordinated on a statewide level between the major urban (UASI) areas and the statewide fusion center concept and integrate information sharing across public safety disciplines and jurisdictions.

I. INTRODUCTION

A. PROBLEM STATEMENT

Many states currently do not have an intelligence fusion center, and as a consequence, their ability to prevent and deter a terrorist attack is limited by the lack of information sharing. Many states lack a central hub for information exchange and currently have no system in place that allows the variety of technologies to gain access to a common database to gather and/or exchange information. In Wisconsin not unlike most states, the vast majority of public safety agencies currently operate their own systems that are incapable of exchanging information. The inability to exchange and/or access information in user friendly format has inhibited Wisconsin's efforts to keep its citizens safe from the possibility of a terrorist attack. For example, currently a traffic patrol officer in Wisconsin cannot gain access to the Department of Corrections database to search for pertinent information that may be relevant to an investigation. In addition, local authorities do not have access to Interpol in order to check on the status of an immigrant.

The inability to exchange information in real time makes it less likely that suspects operating in a terrorist capacity will be apprehended. A variety of law enforcement agencies conduct investigations on a regular basis. The vast majority of them do not know, nor have the ability to identify what the other is doing. The current patrol officer is unable to access information in case management databases because their operating systems are mutually exclusive and incompatible with one another. There is no secure gateway that allows local first responders and law enforcement to access local records management systems. Vital information stored within such records management systems is vital to conducting an investigation. In addition, the lack of ability to access such information allows for the failure to connect the dots. Currently there is no legal issue with sharing such information. The problem lies with the failure to have an information sharing network in place that allows for law enforcement to access the information.

Mohamed Atta was stopped for speeding and issued a warning when there was a warrant for his arrest. Failure to have access to this information prevented police from detaining him.[1] The failure to communicate and share vital information can also hinder investigations. More than one agency investigating a similar case and not sharing information will also lead to the failure of apprehending criminal behavior prior to an incident. In addition, many criminal investigations can have a terrorism nexus. For example, crimes such as dealing in counterfeit currency, credit card fraud, smuggling, and money laundering or trafficking in stolen or forged documents, narcotics trafficking and trafficking in stolen goods are undertaken by various terrorist groups in order to generate funding. This makes it important to communicate in both directions across the organizational divisions between homeland security investigations and traditional criminal investigations.

The failure to exchange information and to connect the dots helped produce the tragic events of 9/11. The culture of information-sharing must be changed from "need to know" to "need to share." The government has a vast amount of information and without a system in place for people to access data there can only be an extremely limited amount of information exchange.[2]

The criminal justice system in Wisconsin is a loosely connected community of independent agencies. There are over 600 independent law enforcement agencies within the state. Most of the state's law enforcement agencies are small and do not have staff dedicated to intelligence functions. Officers in these smaller, local agencies interact with the community daily, but presently lack the tools and resources necessary for developing, gathering, accessing, receiving, and sharing intelligence information.

To successfully deploy a statewide information sharing solution, members of this diverse community must be actively involved in articulation of a collective vision. Representation of all parties must be involved in defining the scope and objectives of the solution. Key concerns involve establishing an effective organizational structure,

[1] Susan Candiotti, "Another Hijacker was stopped for a Traffic Violation," *CNN.com*, January 9, 2002, http://edition.cnn.com/2002/US/01/09/inv.hijacker.traffic.stops (accessed October 12, 2005).

[2] Thomas H. Kean and Lee H. Hamilton, *The 911 Commission Report* (Washington, D.C.: National Commission on Terrorist Attacks upon The United States, 2004), 417.

securing funds, developing comprehensive and detailed strategic and tactical plans while addressing a host of technical and policy issues. To successfully integrate all stakeholders, Wisconsin must accommodate the disparate information systems already in place and strategies must accommodate a wide-range of information privacy and system security considerations. Compliance with federal requirements concerning intelligence data bases and privacy laws will be a key concern for information sharing.

A program and capability review conducted, evaluated Wisconsin's information sharing capability and found that the state is currently served by four major systems in various stages of development: the Health Alert Network (HAN), the State Emergency Management GIS System, the Justice Gateway, and the Wisconsin Statewide Intelligence Center (WSIC). Each of these systems has been designed to fulfill a specialized role and serve a different group of stakeholders. Nevertheless, the state recognizes the danger of having information silos that are unable to communicate. It is therefore vital to develop a state intelligence and information sharing structure and plan to ensure that as these systems continue to grow, they grow in a way that allows them to share necessary information. An information sharing network will connect to other response disciplines through the Wisconsin Justice Gateway, the Health Alert Network (HAN), the state Emergency Operations Center (EOC), fusion center, Milwaukee urban area early warning system and existing state systems. An intelligence fusion center will also provide non-law enforcement intelligence bulletins to the public safety community across the state.

A recent incident will highlight the potential of the need for information sharing to decrease, mitigate and respond to risks:

On November 22, 2005 an explosive device was discovered in a downtown Madison parking ramp, heavily used by city, county and state employees. The Improvised explosive Device (IED) was fortunately rendered safe by the Dane County Bomb Squad. The process was repeated the very next day and the devices were described by law enforcement as "unstable and extremely deadly." Multiple agencies at the federal, state and local levels were involved in the investigation of these related incidents. Madison Police Department had a description of a late model dark Honda with a partial license plate number suspected of being involved. Requesting assistance from the

Division of Motor Vehicles, investigators received it in the way of four large envelopes containing thousands of pages with over 60,000 possibilities. This required weeks and hundreds of hours of staff time to sort through and follow up on the leads. In the midst of the investigation, on Christmas Eve, another explosive device in the same parking structure was detonated, injuring one person and destroying a car. Fortunately, again, the injuries were minor. As late as January 12, 2006, Madison was again plagued by threats of suspicious objects being placed around downtown, effectively shutting down much of the area.

Decreased, mitigated risk is directly associated with the availability of public safety officials to make better informed decisions. These decisions are based on accurate, timely and actionable information. Had the investigators been able to quickly analyze and sort through the information, it is entirely plausible to extrapolate an outcome that would not have included any further incidents. The bottom line is the potential to disrupt, deter, or mitigate an act of terrorism or a simple criminal action through the sharing of information is the most basic action government can take to protect its citizens. The amount of information currently shared electronically is staggeringly low; here is an opportunity to help remedy the situation. We must endeavor to provide law enforcement officers with more complete information about potential suspects. Providing statewide access to the hundreds of thousands of defendants , aliases, and case information the state's many criminal justice databases is a necessary step in protecting the public from potential terrorist threats. Without this access, law enforcement could miss another opportunity to stop a terrorist before the attack is carried out. Chapter III provides additional examples including 2 case studies that support the need for Wisconsin to create an information sharing network.

The fusion center will be the state's primary and central distribution center for information and intelligence sharing functions amongst emergency services. When completed, the fusion center will be a hub for all major information systems and link them across disciplines to assure seamless flows of information. The statewide fusion center will also be inter-linked with a Terrorism Early Warning Center (TEW) in the most populated area in the state, Milwaukee.

While an information sharing plan is being developed, Wisconsin should continue to support the development of these systems as they increase functionality and serve ever larger numbers of responders. This policy recommendation will expand the information sharing network to fulfill the needs and demands of emergency service partners and private sector stakeholders. The network's mission will be to develop strong links across multi-agency and multi-disciplined programs. While the statewide fusion center will operate with a primary focus on homeland defense issues, it will work in the background to support all intelligence and information sharing in the state. Information will flow vertically and horizontally into the center from federal sources as well as from state, local, tribal and private sector sources. Intelligence will be shared across multi-disciplines through systems such as the Wisconsin Justice Gateway, the Health Alert Network and the Emergency Operation Center (EOC) when required.

B. SPECIFIC RESEARCH OBJECTIVE

The objective of this thesis is to identify steps that collectively will comprise a model that can be used as a template for statewide information sharing. The expectation is that through information sharing, public safety agencies can better protect the safety of citizens and ultimately assist in the terrorism prevention efforts.

This thesis will study a variety of alternatives to help Wisconsin and other states in preventing potential terrorist attacks through building an information sharing enterprise. It also will identify an effective method that can be used to design a statewide strategy for information sharing and put forth specific steps required in order to establish an intelligence fusion center and information-sharing network. Specific solutions will be identified based on research, case studies, and best practices from around the country that will put Wisconsin in the forefront of terrorism prevention through information sharing.

This thesis will address two policy options: creating a Terrorism Early Warning Center (TEW) based on the Los Angeles TEW or the creation of a statewide intelligence fusion center coupled with an information sharing enterprise that interlinks the City of Milwaukee TEW system to the fusion center. The latter option would provide for a statewide information sharing capacity. Building this capability would enable Wisconsin

to work proactively and uniformly in the prevention and deterrence of terrorism. An urban area TEW will not fully enhance statewide capability in information sharing. Only a statewide central hub would be able to disseminate information throughout the state.

Wisconsin law enforcement officials and homeland security authorities have determined that information-sharing needs to be improved in order to better protect and serve the public. The intelligence community must enhance its capacity to obtain intelligence relevant to protecting the homeland. The U.S. Department of Homeland Security advises this must include local, state as well as federal agencies working together to provide real time actionable information.[3] Lack of a means to properly collect, analyze and disseminate information and the difficulty in current operating systems to access data bases is as a weakness in the prevention of terrorism.

Information sharing using current technology through the use of a statewide intelligence fusion center could substantially reduce the potential of a terrorist attack. Implementation of an information sharing enterprise could potentially allow law enforcement authorities to prevent a terrorist attack by putting together pieces of information from multiple sources and disseminating that intelligence to the proper public safety officials. The recommendation or model could be used as a template nationwide, expanding existing policy and strategy options for information sharing by other jurisdictions.

C. LITERATURE REVIEW

Based on preliminary research, it appears that the concept of intelligence fusion has begun to emerge as the fundamental process to facilitate the sharing of homeland security information and intelligence at the national level. That being said, it is then imperative that this must become the guiding principle in an individual state initiative to prevent terrorism. The objective of the research is to link information in a manner that will facilitate an operational design of a system to allow for information sharing throughout the public safety community. According to the Heritage Foundation, state and local representation in the Intelligence Community would greatly facilitate this

[3] U.S. Department of Homeland Security, *The National Strategy for Homeland Security*, 2002, http://whitehouse.gov/homeland/book/index/html/ (accessed September 4, 2005).

mission by bringing unique perspectives and needs to the process of creating a usable, integrated intelligence picture.[4] Fusion centers, which are collaborative efforts to combine and analyze anti-terrorism information from multiple sources, have become increasingly popular as part of homeland security and overall strategies in the prevention of terrorism. A number of states, including Arizona, Colorado, Illinois, Kansas, Maryland, Massachusetts and New York, currently operate so-called fusion centers, and many more states, such as Missouri, are considering doing so. The problem with so many states approaching this task from different perspectives is that there is currently a lack of protocols regarding connectivity between centers and different levels of government.[5] Therefore, minimum guidelines need to be recognized for establishing and operating intelligence fusion centers.

The components of this proposed information sharing network include 1) the practical need for the system, 2) which specific type of system would be optimal, 3) which data bases will be queried & compatible, 4) the method of transmission, 5) the dissemination of intelligence and 6) the uses of such a system in preventing a terrorist attack.

Lt John Sullivan, of the Los Angeles County Sheriff's Department, is considered to be one of the nation's leading experts in information-sharing through the use of terrorism early warning centers. According to Sullivan effective and rapid dissemination of indications and warnings to local emergency response agencies is an essential yet problematic element of terrorism management efforts in the United States. A TEW should consist of a multilateral, multidisciplinary effort to monitor open source data to identify trends and potential threats, monitor specific threat information during periods of heightened concern, assess potential targets, and perform net assessments to guide decision-making during actual events.[6] The TEW embraces a networked approach and there is no single entity in charge. Public safety entities collaboratively work together as a network. A particular agency may take the lead and coordinate the process to make sure

[4] James J. Carafano, "Terrorist Intelligence Centers Need Reform Now," *The Heritage Foundation,* 2004, http://www.heritage.org/Research/HomelandDefense/em930.cfm/ (accessed November 15, 2005).

[5] Alice Lipowicz, "Justice Issues Fusion Center Guidelines," 2005, *Washington Technology,* http://www.washingtontechnology.com/news/1_1_/daily_news/26893-1.html. (accessed October 26, 2005).

[6] John Sullivan, e-mail message to Author, November 19, 2005.

notifications are made, and the right people are linked together. The TEW brings together law enforcement, fire, health, and emergency management, because those are the operators that are going to manage these responses in the field. The underlying principles to close the information gap, with the fire service, emergency management discipline and the health community. While these disciplines do not need to know criminal information, the TEW can get the information they need to them with a real emphasis on force protection and protecting the responders so that an event can be mitigated.

The TEW in Los Angeles monitors trends and assesses threats that could result in terrorist attacks in Los Angeles County. Currently, members of the TEW evaluate media accounts, information from other Federal, State, and local agencies, and other open-source data to determine the information's credibility. As part of its assessment, the TEW identifies terrorism precursor events so that prevention and mitigation efforts can be undertaken. The role of the TEW in a crisis is to provide intelligence and support to incident commanders and give recommendations that assist in the decision making process.[7] The Los Angeles model also incorporates a Terrorism Liaison Officer (TLO) to assist in the sharing of information. This network of Terrorism Liaison Officers gives the TEW the ability to communicate effectively and efficiently. In addition, TLOs have the ability to provide local information from their agencies to the TEW.[8]

The TEW model also incorporates the Red Team concept. Those assigned to the TEW form a small active risk assessment group that regularly conducts vulnerability risk assessments to critical infrastructure within their jurisdiction. The assessments are used by the team to create "playbooks" that are designed to assist first responders in a response to a terrorist attack.[9] The L.A. TEW has amassed a huge library of resources that will assist them in a coordinated response to a terrorist attack.

---

[7] Office of State and Local Coordination and Preparedness, "Terrorism Early Warning Group," 2005, http://www.ojp.usdoj.gov/odp/docs/TEWBrochure.pdf. (accessed November 17, 2005).

[8] Ibid.

[9] Greg Krikorian, "Terrorism Early Warning Group Works to Keep L.A.'s Guard Up," *Los Angeles Times*, 2004, http://www.policeone.com/policeone/frontend/parser.cfm?object=News&tmpl=&operation=full_news&id=93416/ (accessed November 10, 2005).

The fusion center concept is to serve as conduit between the federal and local government. The ability to receive information through a single source from the federal government has been a long time complaint of local government. William Welsh writes that local government officials are overwhelmed with terrorist alert information and intelligence. The locals need to continue to design systems that allow for a single primary conduit to gather and disseminate information.[10] State fusion centers will allow the locals the flexibility to have specific intelligence requirements and receive information from a single source and point of contact.

The Office of Domestic Preparedness has made strengthening information sharing and collaboration capabilities a national priority. Incorporated into the new priority capabilities is both information sharing and dissemination, and law enforcement investigation and operations. One of the federal goals of this national priority is to strengthen information sharing from the federal level to the state and local level through the homeland security information network.[11] Information sharing is categorized under prevention, one of the four critical mission areas that the Office of Domestic Preparedness has identified.

Mark Lowenthal writes that intelligence exists solely to support policymakers and that policymakers have a constant need for tailored, timely intelligence that will provide background, context, information, warning and assessment of risks, benefits and likely outcomes.[12] Information is constantly being collected and shared on a daily basis from numerous public safety entities around the country on a local level. Decisions are being made expeditiously by trained individuals assigned to work in fusion centers and TEWs.

In order to effectively share information there has to be a process put into place. There needs to be a central storage house of locally gathered threat and other terrorism related information that is gathered. There also must be a clear process for analyzing and dissemination of relevant information. The integration of justice systems and information

---

[10] William Walsh, Fusion Forward, 2005, http://www.washingtontechnology.com/news/20_4/statelocal/25616-1.html. (accessed November 30, 2005).

11 Office of Domestic Preparedness, 2006 Homeland Security Grant Program, http://ojp.usdoj.gov/odp/docs.fy2006hsgp.pdf. (accessed December 29, 2005).

[12] Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington DC: CQ Press, 2003), 3.

sharing is not a new idea. Agencies throughout the nation have long recognized the importance of integrating information systems to share critical data prior to key decisions having been made. Nearly every state in the nation is actively planning or implementing integrated justice information systems.[13] The U.S. Department of Homeland Security and the U.S. Department of Justice has recognized the importance of integrated systems strategic planning and coordination and is allowing federal funding to support such initiatives. New initiatives bring forth new issues and information sharing through integration of data bases raised important legal, constitutional and policy issues that must be addressed. Integration and sharing of information between law enforcement agencies with other governmental agencies, and with the general public raises new and important privacy and confidential issues that also must be addressed.[14]

According to the Office of Justice Programs (OJP), the OJP information sharing advisory committee to the Assistant Attorney General was created to facilitate and support the exchange of justice information. The advisory committee recommends that any approach to information sharing must take into account the safety of the general public and current justice processes including the sensitivity to balance complex issues such as; the balance between the need to share information to keep the public safe and the need to secure and control access to information.[15] States have the responsibility to build a statewide information repository that supports the operational intelligence needs of state and local public safety agencies. States playing a lead role will need to develop standards consistent with national standards to enable the sharing of information between local jurisdictions, to state systems and other states, as well as with national systems.

---

[13] National Association of State and Chief Informational Officers, "Justice Information," 2005, http://www.search.org/programs/info/jiem.asp/ (accessed November 12, 2005).

[14] Office of Justice Programs, "Global Justice Information Sharing Initiative," September, 2004, http://www.it.ojp.gov/topic.jsp?topic_id=8/ (accessed November 6, 2005).

[15] Office of Justice Programs, "Guiding Principles and Strategic Vision of the Global Justice Sharing Initiative," September 14, 2004, http://www.it.ojp.gov/documents/200409_GAC_Strategic_Plan.pdf. (accessed November 16, 2005).

D. TENTATIVE SOLUTIONS

This thesis will study alternatives to help Wisconsin in preventing a possible terrorist attack through building an information sharing enterprise as well as protocols for inter-state communication between fusion centers. One solution would be to support a Terrorism Early Warning Center (TEW) in Milwaukee. Milwaukee is the most highly populated urban area in Wisconsin and generates the greatest amount of intelligence.

A second option is to create a statewide information sharing enterprise supported by an intelligence fusion center. The statewide fusion center will serve as a central hub for information gathering, fusion and dissemination. The President's Executive Order dated August 27, 2004 requires the strengthening of the intelligence community. There is a need for the establishment of interface standards for an interoperable information sharing enterprise that facilitates the automated sharing of intelligence information among agencies within the Intelligence Community.[16] A TEW needs to interface with a fusion center on the state level in order to facilitate such an endeavor.

Fusion centers embody the concept of collaboration. Collaboration allows agencies to maximize available resources and work jointly toward a common goal. Centers should plan for future connectivity using current technology and adhere to certain standards.[17] Basic standards such as the use of extensive markup language (XML) would allow networks to communicate with one another.

A fusion center with statewide capabilities, interconnected with a TEW located in Milwaukee will provide for redundancy and backup capabilities if something should happen to either site. A state fusion center allows for interconnectivity to the state emergency operations center and the Department of Military Affairs Joint operations Center. A state fusion center also shows leadership on behalf of the state to the locals and will provide a conduit to the National Intelligence Counterterrorism Center (NCTC). A local TEW in the city of Milwaukee will allow for greater resources to be used in the

[16] President George W. Bush, "Executive Order: Strengthened Management of the Intelligence Community," August 27, 2004, http://www.whitehouse.gov/news/releases/2004/08/20040827-6.html. (accessed September 15, 2005).

[17] Peter A. Modaferri, "Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards," *Police Chief* 72, no. 2 (February 2005): 25.

most urban and vulnerable city in the state of Wisconsin. Working in a collaborative effort, the TEW and state fusion center will cover the needs of the state, both urban and rural.

E. RESEARCH METHODOLGY

Information sharing has already been shown to be a productive method of solving and preventing complex problems and crimes. If current technology can accommodate an information sharing enterprise that will allow the public safety community to communicate, share information in real time and allow access to data, then society as a whole should be safer from a potential terrorist attack.

This research will consist of a literature review of current information regarding the most accurate information sharing methods and mechanisms to achieve information-sharing capabilities. The review will include a brief history of intelligence, the intelligence cycle, the dissemination of information, and the culture of "need to know" and how that impacts this project. In addition, the technology necessary and business requirements needed to be successful in creating an information sharing network will be addressed.

Interviews with intelligence experts, who have implemented information sharing capabilities through the use of fusion centers and terrorism early warning centers, as well as interviews and personal experiences regarding failures in exchanging information in real time will provide direct insight how this directly affects the safety of the community.

Unfortunately at this point in the development of our homeland security efforts, definitive standards have yet to be established for intelligence fusion centers. Specific case studies of the LA Terrorism Early Warning System and the Illinois Fusion Center will effectively allow for measurement of the success of fusion centers because it can be shown that the fusion process and capabilities of information sharing has proven to be successful.

While it is difficult to measure prevention, the tangible evaluation of outcomes and impact of a program, case studies can yield strong indications of success. In

addition, the 9/11 report offers substantial analysis into the failures of the intelligence community and the inability to connect the dots because of a lack of policy in place to permit agencies to do so.

F. THE NEED FOR INFORMATION SHARING

Since September 11, 2001, federal, state, and city governments have established initiatives to improve the sharing of information to prevent terrorism. Many of these initiatives were implemented by states and cities and not necessarily coordinated with other sharing initiatives, including those by federal agencies. At the same time, the Department of Homeland Security (DHS) has initiatives under way to enhance information sharing. Overall, there should be enterprise architecture, to integrate sharing between federal, state, and city authorities.

Terrorism poses an imminent and grave threat to our nation. Hostile groups are continuing to plan attacks in this country and abroad. To prevent terrorism to the greatest extent possible and to swiftly punish it when it occurs, the government must have adequate legal authorities and must develop a strong organizational structure. Improved intelligence collection and better sharing of information are central to success. Information sharing will be effective only if it is managed well, with some entity having clear responsibility for setting standards and ensuring implementation and it takes full advantage of available technology, which can be leveraged both to facilitate appropriate information sharing and to protect privacy.

The only way to prevent terrorist attacks is to gather intelligence. It is to collect the information that reveals who the terrorists are, who is backing them with money and resources, and where they are likely to strike. Policymakers must go further to build a new intelligence system to support transformed national security needs. Threats involving unknown perpetrators, methods, and targets cannot be countered with strategies designed for use by federal officials to combat more predictable adversaries. Today, state and local law enforcement, public health, and emergency response personnel are on the front lines of detecting and responding to terrorist threats; corporate managers are responsible for

securing key infrastructure such as energy supplies, chemical plants, and telecommunications; and workers and neighborhood residents may hold information that can help prevent attacks.

Cold war intelligence policies were aimed to protect sources and methods and keep adversaries from gaining access to military secrets. To achieve these goals, defense and intelligence agencies compartmentalized acquisition, analysis, and dissemination of information, an approach that worked reasonably well as long as policymakers knew who the enemy was, what information to look for, where to look for it, and who needed to have it. Analysts became specialists and information was shared among carefully defined groups of federal officials and contractors who were specified in advance and who held appropriate security clearances based on lengthy, costly background investigations.

These policies are ill-suited to the challenge of counterterrorism. Their dual requirements of appropriate security clearance and "need to know" designation inhibit the free flow of information to and from today's diverse community of relevant federal, state, local, and private sector actors.

It is impossible to anticipate "need to know" in a world where enemies are little understood, means of attack are unpredictable, and potential targets are many, diverse, and changing. The need for intelligence, to gather information about threats and vulnerabilities from state and local governments and the private sector and return needed information to them, creates a heightened government responsibility to protect core values of openness and privacy. Policymakers must build a new intelligence system to fight terrorism. The formal, hierarchical, and compartmentalized information strategies of the past need to be replaced with a new architecture featuring flexible, decentralized networks of public and private information providers, analysts, and users. Policymakers should establish procedures to assure access to critical information needed to address national security priorities while taking into account openness and privacy concerns.

II. INTELLIGENCE

Espionage, counterintelligence, and covert action have been important tools of U.S. political leaders since the founding of our nation. During the Revolutionary War, General George Washington directed a broad range of clandestine operations that helped the colonies win independence. Washington ran networks of agents and double agents, employed deceptions against the British army, launched sabotage operations and paramilitary raids, used codes and ciphers, and disseminated propaganda and disinformation to influence foreign governments. America's founders all agreed with General Washington that there was a necessity of procuring good intelligence. In a letter written to one of his officers in 1777, Washington wrote:

> The necessity of procuring good intelligence is apparent and need not be Further urged-All that remains for me to add is, that you keep the whole matter as secret as possible. For upon secrecy, success depends in most enterprises of the kind & for want of it, they are generally defeated, however well planned.... [letter to Colonel Elias Dayton, 26 July 1777][18]

A. HISTORY OF INTELLIGENCE SHARING

Presidents in the early Republic were actively involved in intelligence activities especially covert actions. In his first State of the Union message, Washington requested that Congress establish a secret service fund for clandestine activities. Within two years the fund represented over ten percent of the federal budget. Thomas Jefferson drew on it to finance the United State's first covert attempt to topple a foreign government, one of the Barbary Pirate States, in 1804-05. It failed. James Madison employed agents of influence and clandestine paramilitary forces in trying to acquire territory in the Florida region from Spain during 1810-12. Several presidents dispatched undercover agents on espionage missions overseas. One spy, disguised as a Turk, obtained a copy of a treaty between the Ottoman Empire and France. Also during this period, Congress first tried to exercise oversight of the secret fund, but President James K. Polk rebuffed the lawmakers and thought that the experience of every nation on earth has demonstrated that

[18] Provost Phyllis McNeil, *The Evolution of the U.S. Intelligence Community*, ed. Loch K. Johnson and James J Wirtz (Los Angeles: Roxbury Publishing Company, 2004), 5.

emergencies may arise in which it becomes absolutely necessary to make expenditures, the very object of which would be defeated by publicity.[19]

The first organized intelligence capabilities were implemented by the military. The U.S. Navy established the Office of Naval Intelligence (ONI) in 1882. The Army soon followed and created the Division of Military Information (DMI) in 1885. By 1939 there were several more governmental agencies that had intelligence units such as the Agriculture, Commerce and Interior Departments.[20] Each intelligence unit had its own operations, methods, ambitions and secrets and operated in a world of its own.

Due to a lack of collaboration between intelligence units from various governmental agencies a central information clearing house was needed. President Truman recognized the need for a centralized intelligence system. Taking into account the views of the military services, the State Department, and the Federal Bureau of Investigation (FBI), he established the Central Intelligence Group (CIG) in January 1946. The CIG had two missions: providing strategic warning and conducting clandestine activities. The CIG functioned under the direction of a National Intelligence Authority composed of a Presidential representative and the Secretaries of State, War and Navy. Rear Admiral Sidney W. Souers, USNR, who was the Deputy Chief of Naval Intelligence, was appointed the first Director of Central Intelligence (DCI).[21]

Under the provisions of the National Security Act of 1947, which became effective on 18 December 1947 the National Security Council (NSC) and the Central Intelligence Agency (CIA) were created. The 1947 Act charged the CIA with coordinating the nation's intelligence activities and correlating, evaluating, and disseminating intelligence which affects national security. In addition, the Agency was to perform other duties and functions related to intelligence as the NSC might direct. The Act defined the DCI's authority as head of the Intelligence Community, head of the CIA, and principal intelligence adviser to the President, and made him responsible for protecting intelligence sources and methods. The act also prohibited the CIA from

---

[19] McNeil, *Evolution of U.S. Intelligence Community,* 5-6.

[20] Thomas F. Troy, *The Quaintness of the U.S. Intelligence Community*, ed. Loch K. Johnson and James J Wirtz (Los Angeles: Roxbury Publishing Company, 2004), 21-22.

[21] Ibid., 24.

engaging in law enforcement activity and restricted its internal security functions. The CIA carries out its responsibilities subject to various directives and controls by the President and the NSC.[22] It is clear that the inability of the CIA to effectively collaborate and share information with the FBI and other federal entities, created an intelligence stove pipe.

Throughout history our nation has utilized intelligence gathering and covert operations in an effort to keep the homeland safe and to be effective during wartime. During that time there were several occasions when intelligence collection and the process of fusing information came into question. During the Vietnam War concerns grew that policymakers were pressuring the intelligence community to provide information that would be supportive of policy. Policymakers and the intelligence community were never at more odds than during the order of the battle debate, which focused on the number of enemy units that were in the field.[23] The opposing views on what constituted enemy units lead to a breakdown in intelligence communications.

There have been complete failures in the history of the intelligence community. All the capabilities and intelligence collection capacity available at that time did not prevent the Emperor of Japan form successfully attacking Pearl Harbor. The ultimate failure in intelligence came on September 11, 2001. The 9/11 attack on the Trade Towers has often been compared to that of the Japanese against Pearl Harbor as another infamous case of intelligence failure. On both occasions, there was ample evidence that the enemy might be pushed to undertake a desperate act. But the signs leading up to 9/11 were ignored for at least three of the same reasons that the Japanese were able to catch the U.S. Pacific fleet at anchor on the morning of 7 December, 1941. Good intelligence indicators lost in the noise of disinformation; a belief that the enemy lacked the technical capacity to undertake the action; finally, mirror imaging, the assumption on the part of the intelligence consumer that the action undertaken was unlikely because it was illogical.

While in retrospect the footprint of a surprise attack becomes easy to trace, before the event it usually requires a great effort of foresight and intuition to cull out good

[22] Lowenthal, *Intelligence*, 18-19.

[23] Ibid., 21-22.

information from a plethora of data. Relevant information may be filtered out as it is sent up the bureaucratic chain because it seems unimportant, trivial or irrelevant to more important concerns, such as local FBI agents reporting that Arab students in flight schools only wished to learn how to take off, not to land. Noise becomes a problem especially when intelligence services have overlapping mandates, are competitive and therefore fail to cooperate to share and analyze information, or believe that the other service has a special responsibility for the collection of a particular type of intelligence. It is now obvious that the inability of the CIA and the FBI to communicate at least contributed to the failure to detect the 9/11 attacks, as the failure of army and naval intelligence to cooperate aided the Pearl Harbor debacle. Also, as noted above with respect to the Japanese attack, the fact that intelligence analysts could not conceive of the possibility of this type of threat because it didn't make any sense to them. If one can understand the mindset of a Jihadist, flying planes into buildings is a perfectly logical and desirable method to accomplish your goals, even though the rest of us just shake our heads in disbelief and cannot imagine what that could prove or how it could actually advance anyone's political agenda. Therefore, while stovepipping is unquestionably a major factor, understanding the mindset of the enemy has to be included as well. Most intelligence and/or policy planning agencies have their "Red Team" people who dream up all sorts of exotic ways and means to carry out attacks. Most of the time, people don't take these scenarios seriously because they seem too much like fantasy or science fiction. Perhaps that approach has to be rethought. Even so, that does not mean that every idea dreamed up by the Red Team has to be accepted. It is their job to be creative. Terrorists more often then not stick to their traditional methods of explosives and firearms and it would be a mistake to view terrorism solely through the lens of 9/11.

A second factor in intelligence surprise occurs when the technological capabilities of the enemy are underestimated. The United States discounted the ability of the Japanese Navy to project a fleet across the Pacific to launch an air attack with aerial torpedoes against U.S. ships. Despite this successful precedent, the United States Navy persisted in its belief that the Japanese Navy was incapable of orchestrating such an operationally and technologically sophisticated maneuver. Ironically, although the 9/11 conspirators demonstrated an organizational capacity to coordinate the simultaneously hijacking of

four airliners, no one suspected that the hijackers' weapon of choice would be the box-cutter. In addition, as opposed to the Pearl Harbor example, the enemy not only used a combination of primitive, almost iron-age technology (what is in fact a knife), along with highly advanced technology (passenger aircraft) but perhaps more importantly, that the enemy used our technology against us – something that the Japanese did not have the desire or opportunity to do. This, of course, has to do with the nature of terrorism as opposed to conventional war since terrorism springs up from within, as terrorists are too weak to field an army and navy against us. Moreover, today's society is more technology-intensive than was US society in the 1940s and this too is a factor that should be considered.

The final cause of intelligence surprise is mirror-imaging, the belief that the perpetrators will not carry out a particular act because the defender, in their place, would not do it. It seemed inconceivable to the U.S. planners in 1941 that the Japanese would be so foolish to attack a power whose resources so exceeded those of Japan, thus virtually guaranteeing defeat.[24] Likewise, the notion of suicide bombing is so alien to the American and Western outlook, that we find it difficult to fathom the mindset of enemies prepared to conceive of an operation of such horrific proportions, one in which they are prepared to immolate themselves in acts of fiery desperation. In fact, one interpretation of the events of 9/11 is that many of the hijackers did not realize that, by signing on to Osama bin Laden's desperate mission, they would be committing suicide. The fact that bin Laden and his henchmen were willing to use their own people in this way, if in fact some of the hijackers were unaware of the actual goals of the mission, gives us insights into their minds and what life would be like in bin Laden's world. Their own people went to their deaths willingly; at the very least we can be sure that the terrorist pilots did so. It is not just Bin Laden pulling the strings, it's not a question of absolute blind loyalty to a leader; it is a question of fanatical religious belief.

The attack on Pearl Harbor and the 9/11 terrorist attack on the World Trade Center are similar in the fact that there were major intelligence failures that may have prevented the event from happening. An intelligence failure is any misunderstanding of a

[24] Frederic L. Borch, "Comparing Pearl Harbor to 9/11," *Journal of Military History*, July 2003.

situation that leads a government or its military forces to take actions that are inappropriate and counterproductive to its own interests**.** It is a mistake to think that any human endeavor, including intelligence, will be error-free. Enemies may be underestimated or overestimated, and events that should be predictable go unforeseen. Because intelligence work is the product of a team effort, there are certain peculiarities common to the bureaucratic environment that helps explain failure. Arguably, the worst kind of intelligence failure is surprise attack.

The case of Pearl Harbor is regarded as the worst case of intelligence failure in history. No intelligence agency had prepared a report for the possibility of an attack there, although everyone talked about it. Naval intelligence (ONI) did not even have a minimal amount of strategic or tactical intelligence. They thought Japan would attack Thailand about that time of year. The problem was that America lacked Human Intelligence (HUMINT) on Japan. The U.S. had a few geisha girls on the payroll, but no agents in the Japanese elite. The U.S. had broken the Japanese code, but what they were intercepting was just diplomatic and espionage information (movement of spies), nothing of the nature of military plans, and they changed their codes a day before the attack. Japanese radio transmissions deceived the Americans into thinking the task force was assembling for training maneuvers.

Not sharing information and the failure to connect fragmented pieces of information into actionable intelligence are the primary factors in the failure to prevent 9/11. The 2004 Executive Summary of the 9-11 Commission Final Report stated that all the following were specific intelligence failures, which occurred:

- Not watch listing future hijackers Hazmi and Mihdhar and not trailing them after they traveled to Bangkok
- Not sharing information linking individuals in the *Cole* attack to Mihdhar
- Not taking adequate steps in time to find Mihdhar or Hazmi in the United States
- Not linking the arrest of Zacarias Moussaoui, described as interested in flight training for the purpose of using an airplane in a terrorist act, to the heightened indications of attack
- Not discovering false statements on visa applications by the Hamburg cell

- Not recognizing passports manipulated in a fraudulent manner by the Hamburg cell
- Not expanding no-fly lists to include names from terrorist watch lists
- Not searching airline passengers identified by the computer-based CAPPS screening system
- Not hardening aircraft cockpit doors or taking other measures to prepare for the possibility of suicide hijackings

Unfortunately over time a wall had been built to separate criminal and intelligence investigations. These separations lead to a lack of coordination in the intelligence community. Most notably, there was a lack of sharing information between the FBI and the CIA. The requirement to have some separation between criminal and intelligence investigations grew out of a 1980 case, United States v. Truong Dinh.[25] One can point to the Reagan or Bush I administrations for when the *Truong* requirement took hold in the Department of Justice. Some time in the 1980s, the exact moment is hidden in historical documentation; the Department applied the *Truong* analysis to an interpretation of the FISA (Foreign Intelligence Surveillance Act) statute. This caused the failure to share information to strengthen between the FBI and CIA. The *Truong* requirement for some separation between criminal and intelligence investigations does not mean complete isolation and the FBI through internal policy caused a failure in sharing information.

B. THE INTELLIGENCE PROCESS

The intelligence cycle in the civilian arena, is the process of developing raw information into finished intelligence for consumers, including policymakers, law enforcement executives, investigators, and patrol officers. These consumers then use this finished intelligence for decision making and action. Intelligence may be used, for example, to further an ongoing investigation, or to plan the allocation of resources. The process is a five step process that includes decision making and feedback as part of the last step. It is a continuous ongoing circular of activity as outline in the diagram below.[26]

[25] *United States v. Truong Dinh Hung*, 629 F.2d 908, 913-14 (4th Cir. 1980).

[26] Loch K. Johnson and James J. Wirtz, *Intelligence Collection* (Los Angeles: Roxbury Publishing, 2004), 41-42.

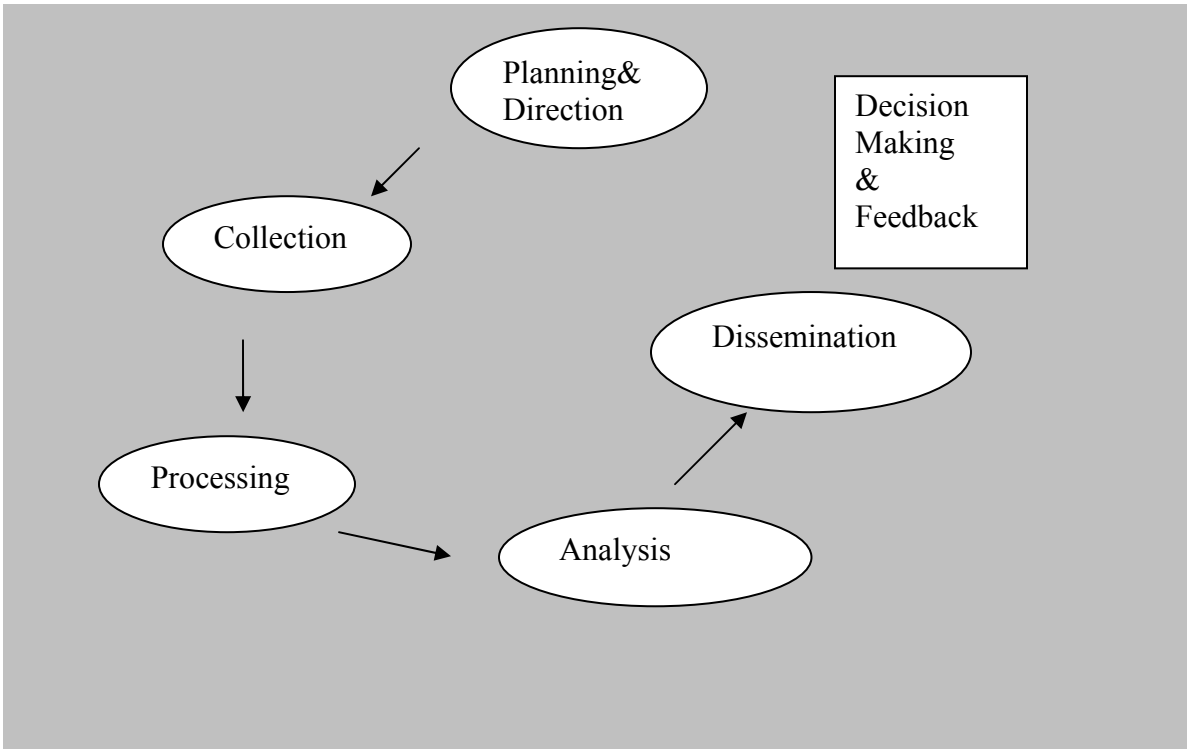


Figure 1. The Intelligence Cycle

Planning and direction involves management of the entire intelligence effort, from identifying the need for data to delivering an intelligence product to a consumer. It is both the beginning and the end of the cycle. It is the beginning because it involves formulating specific collection, processing, analysis, and dissemination requirements. It is the end because finished intelligence, which must support decision-making and action, frequently generates new information requirements.

The intelligence process is primarily consumer driven. That is, nearly the entire process depends on guidance from the consumer, the end user of the intelligence. Consumers from all levels of government, federal, state, and local may initiate requests for intelligence. In addition, policymakers, executives, investigators, and patrol officers usually have different information needs. Thus, the effective planning and direction of the intelligence effort requires an understanding of the needs of a variety of consumers. However, if the consumers do not know what to ask for because they don't know what kinds of information might be obtained by the intelligence community then there will be

a disconnect. If the process is exclusively consumer driven, this is a problem. The best model would involve both inputs and requirements from consumers as well as having the intelligence community through out bits of information that it thinks might be of interest to various consumers and telling them, "if you're interested, there's more where that came from." That way, different types of information might be made available to consumers who were unaware of them earlier and may then expand the scope of the types of information that consumers might need.

Collection is the gathering and reporting of the raw information that is needed to produce finished intelligence. To be effective, collection should be planned, focused, and directed. There are many sources of raw information, including open sources such as governmental public records, media reports, the Internet, periodicals, and books. Although often underestimated, open source collection is important to an intelligence unit's analytical capabilities. There are also confidential sources of information. Law enforcement officers collect such information from various sources, including citizens who report crime, investigations that are conducted, and speaking with persons who participate in criminal activity. To gather this information, law enforcement officers use a variety of collection methods such as interviews, undercover work, and physical or electronic surveillance.

Processing involves conversion of raw information into a form usable by analysts. This is accomplished through information management. Information management is the indexing, sorting, and organizing of raw data into files so that the information can be rapidly retrieved. The processing step includes entry of data into a computer, reduction of data, collation of paper files, and other forms of information management. Effective processing requires an understanding of the consumers' needs, the types of information that are being processed, the collection plan, and the analytic strategy.

Analysis and production is the conversion of basic information from all sources into finished intelligence. It includes integrating, evaluating, and analyzing all available data, which is often fragmentary and even contradictory and preparing intelligence products. Analysis gives additional meaning to the raw information. Analysts, who are subject-matter specialists, consider the information's reliability, validity, timeliness, and

relevance. They integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications of the information for consumers.

Intelligence and analysis units may devote their resources to producing strategic intelligence for policymakers and executives, providing operational intelligence to continuing investigations, or making available tactical intelligence for an immediate law enforcement need. These important functions are performed by monitoring current crime and non-crime events, warning decision makers about actual and potential threats to public safety and order, and forecasting developments in the area of criminal activity. Intelligence and analysis units may produce numerous written reports, which may be brief, one page or less or lengthy studies. They may involve current intelligence, which is of immediate importance, or long-range assessments. The Agency presents some finished intelligence in oral briefings.

The last step, which logically feeds into the first, is the distribution of the finished intelligence to the consumers, the same consumers whose needs initiated the intelligence requirements. These recipients of finished intelligence then make decisions or take action based on the intelligence that has been provided. This step should also include an opportunity for feedback, to assess the value of the intelligence that has been provided.[27] The decisions, actions, and feedback may lead to the levying of more information requirements, thus triggering the intelligence cycle once again.

C. NEED TO KNOW VS. NEED TO SHARE

One of the most important needed changes for the intelligence community is cultural. The U.S. intelligence community remains handicapped by internal barriers and walls meant to protect intelligence sources and methods. While the need-to-know principle cannot be completely discarded, the intelligence paradigm must shift from a need-to-know to a need-to-share because no single intelligence analyst or agency has a monopoly on knowing everything or being right all the time about the various terrorist

[27] Johnson and Wirtz, *Intelligence Collection*, 41-42.

threats. This means better communication and information-sharing, which requires an integrated information sharing network.

Intelligence agencies typically compartmentalize their information, for the most part to protect it. The federal intelligence agencies, spread through six Cabinet departments, must learn to share information on terrorism rather than stovepipping it. Had the CIA alerted the FBI sooner that key plotters of al Qaeda were in the U.S., or had the FBI shared its concerns about Middle Easterners taking flying lessons, the September 11 attacks might have been foiled. Establishing an intelligence sharing process that allows the locals and the federal government to exchange information is vital to preventing another attack to the homeland.

The National Counter Terrorism Center (NCTC) is designed to be a central location where all terrorist-related intelligence, both foreign and domestic, is gathered, coordinated, and assessed. It is composed of elements of the FBI, CIA, Department of Defense, Department of Homeland Security, Department of State, and other intelligence agencies. According to the Administration, the NCTC will:

- Optimize the use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies;
- Create a structure that ensures information sharing across agency lines;
- Integrate terrorist-related information collected domestically and abroad in order to form the most comprehensive threat picture possible; and
- Provide terrorist threat assessments for the national leadership.[28]

The original Terrorism Threat Integration Center (TTIC) prior to NCTC had developed a secure Web site to provide access to top-secret information to government officials from all agencies involved in the war against terrorism. It will soon have a Web site with secret and law enforcement sensitive information that will give access to a much broader community of analysts. Eventually, online capabilities will have sensitive but unclassified information that will allow more information sharing with state and local officials and the private sector.[29] Currently, the Director of the NCTC reports directly to

[28] U.S. Department of State, "Fact Sheet: Bush to Create Terrorist Threat Integration Center," January 28, 2003, usinfo.state.gov/topical/pol/terror/03012806.htm. (accessed February 15, 2006).

[29] John Brennan, Terrorist Threat Integration Center, "Our First Line of Defense for Homeland Security," in Testimony before the Committee on the Judiciary, U.S. Senate held in Washington, DC, September 23, 2003.

the Director of National Intelligence. This is part of the new beginning in changing the old adage need to know vs. need to share information. State intelligence fusion centers and Terrorism Early Warning Systems play an imperative role in the exchanging of information.

D. COLLABORATION AND COORDINATION

> Intelligence and information sharing for the purpose of preventing, preparing for, and responding to potential terrorist attacks on the United States; the responsibility of the Department of Homeland Security for comprehensive, nationwide, terrorism-related threat, vulnerability, and risk analyses; the integration, analysis, and dissemination of homeland security information, communications of terrorism-related information by the federal government to State, local, and private sector entities; liaison of the Department of Homeland Security with U.S. intelligence and law enforcement agencies; information gathering, analysis, and sharing by Department of Homeland Security entities; the role of intelligence in threat prioritization; are vital in our Nation's efforts against terrorism.
>
> ***Source: Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment***

The policy of the intelligence community should be that intelligence is produced in a way that balances the need for maximum utility of the information to the intended recipient with protection of intelligence sources and methods. The controls and procedures established by this directive should be applied uniformly in the dissemination and use of intelligence originated by all Intelligence Community components. Originators of classified intelligence information should write for the consumer. This is intended to provide for the optimum dissemination of timely, tailored intelligence to consumers in a form that allows use of the information to support all need to know customers. The originator of intelligence is responsible for determining the appropriate level of protection prescribed by classification and dissemination policy. Originators shall take a risk management approach when preparing information for dissemination. In the interest of the widest possible dissemination of information to consumers who need to know, classifiers should carefully consider the needs of all appropriate intelligence

consumers regarding sources and methods information or sensitive analytic comments and use tearlines and other formats to meet consumer needs for intelligence.

Not everyone necessarily needs to have open access to intelligence information. Those that do need to go through the background investigation phase of the FBI in order to have clearance. Part of the problem is that it currently takes to long to process the backgrounds and grant clearances. There is no way around this requirement. The backgrounds are designed to allow the government to assess whether a candidate is sufficiently trustworthy to be granted access to classified information. Applicants must meet certain criteria, relating to their honesty, character, integrity, reliability, judgment, mental health, and association with undesirable persons or foreign nationals. The FBI is currently in charge of conducting backgrounds and attempt to complete them in 45-60 days. This may not always be the case and therein lays the problem. The FBI must make the commitment to allocate enough resources to effectively complete security clearances with the set forth timeframe. Our nation can ill afford to get bogged down in a process that prevents clearances from taking place.

Chapter III looks at two separate information-sharing capabilities where coordination and collaboration is a key to success in preventing terrorist activity. The intelligence fusion center concept is an entity that is involved with hard analytical fusion of information that produces intelligence that is pushed up to the federal level and pushed downward to local law enforcement and public safety agencies. The terrorism early warning system is an information sharing entity that is utilized at the local level that brings together several individuals using a multidiscipline approach to sharing information. The concept utilizes red teaming, conducts regular vulnerability assessments and plays a supportive role in a crisis. The key is to interlink the two concepts and create an enterprise between the local and state levels.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES

There is a problem with information sharing and the ability to obtain and disseminate that information. Creating an enterprise can help alleviate this problem. An information sharing enterprise is a structure for directly linking together public safety agencies and entities to facilitate the flow of information and foster cooperation among them. In an information sharing enterprise, public safety agencies directly share terrorism-related information with each other. Officials from these agencies act as nodes within the enterprise, transmitting terrorism-related information from their own agency to local police and to other agencies for which this information would be relevant. There is a clearly established product line to cover the dissemination of information within the intelligence community.[30] In an information sharing enterprise, law enforcement agencies and fusion centers do not serve as the single, centralized hubs for information management. However, they still play a vital role as nodes that are capable of producing and disseminating analyzed intelligence throughout the network.

An information sharing enterprise requires more resources and manpower than other information sharing mechanisms. Public safety agencies must be willing to dedicate staff, either on a full- or part-time basis, to gather and disseminate information. Participating agencies must also be able to identify information that is relevant and be willing to share that information with appropriate local entities. Several jurisdictions have established information sharing networks by adopting the Terrorism Early Warning Group (TEW) model such as Los Angeles County. TEWs are multidisciplinary networks that facilitate or perform all of the principal information and intelligence sharing functions at the local level.[31] Currently Wisconsin does not have the capability, or the capacity to analyze information, fuse it into a workable product and share it effectively through proper dissemination. The city of Milwaukee is the largest, most populated and vulnerable urban area in the state of Wisconsin. Milwaukee needs to build its capabilities in order to effectively prevent terrorism through information sharing. There is no central

[30] Lowenthal, *Intelligence*, 48.

[31] John P. Sullivan, *Building a TEW Network*, 2005, unpublished PowerPoint slides.

clearinghouse for tips, investigative information and/or general open source information that enhances collaboration and the sharing of intelligence.

In October 2004, the City of Oak Creek, a suburb of Milwaukee was subject to an intentional act of sabotage which resulted in the collapse of two separate power transmission towers. The preliminary investigation revealed that an unknown suspect or suspects intentionally loosened and removed several bolts from the base of two power transmission towers. The result was a disruption to train service and air service at Mitchell International Airport located in Milwaukee. The FBI was immediately called in to assist in the investigation and terrorism has never been ruled out.[32] Throughout the investigation more and more evidence had come forth that could have been provided prior to the incident and pieced together, had a TEW been in place. Witnesses had observed a suspicious van in the area of the transmission towers and one had failed to report that activity and a second witness had reported it to local police who checked the area, but never followed up on the tip.[33] A TEW would have enabled local patrol officers to forward suspicious information through the Terrorism Liaison Officer (TLO) program. A tipster line into the TEW would provide an opportunity for local citizens to report suspicious activity. Different pieces of information and/or clues can be submitted to the TEW for analysis. Information fused can provide intelligence to support investigations. The TEW interconnected to the statewide intelligence center would allow for the two entities to leverage resources and search multiple databases and effectively piece information together. Currently there is no one single source or warehouse of information in the most vulnerable urban area in Wisconsin. A TEW would be the single point of contact for all information to come into and disseminate from. The TLO program would train representatives from various public safety agencies and the private sector on what to look for regarding suspicious activity and what should be reported. Currently in the Milwaukee area every agency is operating on their own individual server utilizing different software programs that are not compatible with one another and will not allow the exchange of data and/or information in real time.

---

[32] Derrick Nunnally and Linda Spice, "Evidence Found in Towers' Collapse," *JS Online,* October 11, 2004, http://www2.jsonline.com/news/metro/oct04/265866.asp/ (accessed March 18, 2006).

[33] Sgt. Mike Meyer, interview by Author, March 21, 2006.

Terrorism exercises conducted have repeatedly singled out the need for improvement in information sharing. An exercise conducted on March 2, 2006 involved suspicious individuals as role players being stopped and questioned regarding their possible involvement in leaving a suspicious package outside of City Hall. A routine records check indicated that they were who they said they were. However, the local dispatch center not having access to additional data bases were unable to gather information from surrounding jurisdictions that the suspects had been questioned regarding the purchase of explosive chemicals commonly used in IEDs. A TEW would have been able to pull the information together from searching multiple data bases. A quick check with the statewide intelligence center would have lead to more information on the suspects. The overarching concept is to pull information together from multiple sources to create intelligence that can be shared.

A. LOS ANGELES TERRORISM EARLY WARNING SYSTEM

The LA TEW integrates criminal and operation intelligence to support strategic and tactical users. As a part of this process the TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team. Within a single TEW, this process is known as all source/all phase fusion, where intelligence is derived from all potential sources to include; classified, sensitive but unclassified and open sources or OSINT to provide information and decision support at all phases of a threat response.[34] Information needed to understand an event is available from local through global sources.

Identifying global distributed threats and achieving an understanding of their impact requires more than simple information sharing. It demands collaborative information fusion and the production of intelligence among cooperative agencies that are distributed among locations where terrorist operate, plan, or seek to attack. Developing the intelligence needed to anticipate, prevent, disrupt, or mitigate the effects of an attack requires the production of intelligence in a collaborative and integrated endeavor by a number of agencies across this dispersed area. This is known as co-production of intelligence. In essence the TEW is designed as a node in a counter-

[34] John Sullivan, interview by Author, February 21, 2006.

terrorist intelligence network. To achieve this local through global fusion, or co-production, the TEW has developed an organizational structure and processes, including Intelligence Preparation for Operations (IPO) and the Transaction Analysis Cycle; it conducts exercises, and is forming a networked framework for node-to-node collaboration.[35] Organizationally, the TEW is organized into six cells: the Officer-in-Charge or OIC - Command, Analysis/Synthesis, Consequence Management, Investigative Liaison, Epidemiological Intelligence (Epi-Intel) and Forensic Intelligence Support cells. The Forensic Intelligence Support cell, which includes technical means and such external resources as virtual reach back, supports the others. These are supported by a network of Terrorism Liaison Officers (TLOs) coordinated by the TEW. The foundational TEW organization can be described as:

- The **OIC (Command) cell** provides direction, sets intelligence requirements, and is responsible for interacting with the incident command entities.
- The **Analysis/Synthesis cell** coordinates net assessment activities and develops an iterative collection plan (including tasking requests for information to the various net assessment elements). The Analysis/Synthesis cell is also responsible for developing the results of all the cells' analysis into actionable intelligence products.
- The **Consequence Management cell** assesses the law, fire and health (EMS-Hospital-operational medical) consequences of the event.
- The **Investigative Liaison cell** coordinates with criminal investigative entities and the traditional intelligence community.
- The **Epidemiological Intelligence (Epi-Intel) cell** is responsible for real-time disease surveillance and coordination with the disease investigation.
- The **Forensic Intelligence Support cell** exploits a range of technical means of support the TEW fusion process. These include CBRNE reconnaissance, the use of sensors and detectors, geospatial tools (including mapping, imagery and GIS products), and cyber means.[36]

The TEW has developed a local network of Terrorism Liaison Officers (TLOs) at each law enforcement, fire service, and health agency in its area of operations. In addition, private sector counterparts, known as infrastructure Liaison Officers (ILOs) are

[35] John Sullivan, interview by Author, February 21, 2006.

[36] U.S. Department of Homeland Security, Terrorism Early Warning Group, 2005.

also being established to ensure the flow of information between the TEW and key critical infrastructure and cultural entities. TLOs and ILOs provide the outer sensing capacity for the TEW and are users of TEW products.[37] The LA TEW model has a proven record of being successful in the prevention of terrorism in both real life threats and through terrorism prevention exercises. The Terrorism Early Warning Group (TEWG) Functional Exercise, conducted on Tuesday, August 30, 2005 in Los Angeles, California, was the thirteenth in a series of 39 exercises to be conducted as part of Operation Chimera – 2005 Los Angeles County Operational Area (OA) Exercise Program. The exercise proved to be very successful, bringing together highly skilled representatives from the TEW cadre, the Los Angeles County Department of Health Services Acute Communicable Disease Control (ACDC) program, the DHS Technical Advisory Group (TAG) and the TEW Terrorism Liaison Officer (TLO) program to test the challenges presented by an aerosolized anthrax release.[38]

Throughout the exercise, it was recognized that the TEW was able to identify, validate and appropriately disseminate the various pieces of intelligence generated during the course of the exercise. During the course of the exercise, members of the Analysis/Synthesis Cell effectively vetted leads and showed restraint on releasing information that could not be confirmed.[39] Cells within the TEW provided support to one another by exchanging information throughout the exercise and the Epidemiological Intelligence (Epi-Intel) Cell became fully integrated with the Analysis/Synthesis Cell following the presumptive identification of Bacillus anthracis (anthrax).

Financing terrorism has evolved over time and the terrorist will help support their network and activities by any criminal means. In 2002 U.S. Immigration and Customs Enforcement (ICE) seized a container filled with counterfeit shampoos, creams, colognes and perfumes along with eight tons of fake Vaseline jelly, sent by a member of Al Qaeda. The LA TEW played a significant role in piecing together information and providing intelligence to policy makers. There have been several instances where the TEW has

[37] John Sullivan, interview by Author, February 21, 2006.

[38] John Sullivan, "FYI TEW," e-mail message to Author, March 20, 2006.

[39] Ibid.

played a supportive role in counterfeiting investigations in California where arrest have been made and suspects have had ties to Hezbollah.[40]

The LA TEW played a significant role in fusing information and providing valuable intelligence that thwarted a terrorist attack at Disneyland. A videotape was received that contained a creditable threat of a Sarin gas attack at Disneyland. The LA TEW conducted the initial analysis of the tape and the initial investigation that lead to preventing the attack from taking place.[41] (Further information detailing the success of this event is classified).

The TEW model is scalable and adaptable. Co-production of intelligence to counter the evolving terrorist threat requires the development of multilateral structures. Much of the information necessary to understand the dynamics of a threat, or even to recognize that a threat even exist is developed from the bottom up as well as through horizontal structures as opposed to top down structures. Multilateral exchanges of information including indicators of potential attacks and alliances among networked criminal actors are needed to counter networked adversaries. This requires the development of new analytical processes and policy. The TEW model and the processes evolving within the TEW network are the first step in the pursuit of preventing another attack on our nation's homeland.

B. ILLINOIS STATEWIDE INTELLIGENCE FUSION CENTER

Intelligence analysis and production is the merging of data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with an emphasis on the larger public safety and homeland security threat picture. Intelligence information sharing and dissemination capabilities are necessary tools to enable efficient prevention, protection, response and recovery activities. Simply put the goal of a fusion center is to get the right information, to the right people, at the right time.

The Illinois Statewide Terrorism Intelligence Center (STIC) is a joint initiative between the Illinois State Police and the Illinois Association of Chiefs of Police, in

[40] Sullivan, "FYI TEW."

[41] Ed Reed, interview by Author, March 20, 2006.

concert with their partners in the criminal justice community. The original proposal was developed in response to a commonly-voiced complaint by law enforcement agencies regarding the absence of a centralized intelligence-sharing mechanism for terrorism-related information in Illinois. The STIC was designed to serve as a one-stop resource for Illinois' criminal justice agencies for both domestic and international terrorism-related information. The STIC coordinates the exchange of information between local police officers and agents assigned to the FBI's Joint Terrorism Task Force to ensure the appropriate persons are linked, eliminating the bureaucratic frustration of being transferred from one person or agency until the proper assistance is located. The overarching concept is deceivingly simple: hire, train, and staff a pool of analysts to provide a broad spectrum of terrorism-oriented intelligence and analytical resources to law enforcement officers in Illinois. Specific goals for STIC are:

- To supply 24-hour, seven-day-a-week access for terrorism-oriented intelligence queries for all law enforcement agencies throughout the state, providing a focal point for both state and federal database inquiries.
- Maintain a centralized repository to capture incoming query data which will be analyzed and assessed; these assessments are provided to law enforcement agencies throughout Illinois as well as to the Illinois Emergency Management Agency.
- To facilitate a strong working relationship between local police officers and the FBI's Joint Terrorism Task Forces.
- To act as police liaison with the Illinois Emergency Management Agency for predictive consequence management resource allocation.
- To serve as a national model for multi-agency, anti-terrorism intelligence initiatives.
- Included in the initiative is the use of an extranet server which will enable secure, password-protected access by any law enforcement officer or criminal justice agency to terrorism intelligence documents and STIC reports via a web-based format.
- In addition to a repository for query data, the STIC database will be used as a pointer system for terrorist-based investigative referrals between agencies to promote direct interagency intelligence-sharing opportunities.[42]

[42] State of Illinois, Statewide Intelligence Fusion Center, http://www.illinoishomelandsecurity.org/ittf/terrorismreport19.htm. (accessed February 20, 2006).

The STIC is located in Springfield, Illinois in the newly opened State Emergency Operations Center, a state-of-the art facility that will help the state better protect Illinois residents by bringing key terrorism prevention and emergency response assets together in one location. The center will enable decision makers from several state agencies to receive timely, disaster related information that will help them make better decisions to respond to emergencies and to help protect the public in the event of an act of terrorism or a natural disaster. The STIC opened in 2003 with a primary focus on analyzing terrorism related intelligence. Since then it has incorporated units specializing in other categories of criminal activity, including narcotics, violent crimes, sex offenses and motor vehicle theft. STIC analysts specialize in certain areas of critical infrastructure: water, electricity, telecommunications, etc.., and some have skills in foreign languages including Arabic and Urdu. Coordinators from each unit and representatives from the command staff make up a Threat Integration Group (TIG) that meets daily to review and analyze the activity reported during the previous 24 hours. The TIG provides feedback to the field officers and other state level decision makers. The center is linked to the Illinois State Police Office of Counter Terrorism, which has 14 representatives on two FBI Joint Terrorism Task Forces (JTTF). That link ensures that leads identified at the STIC are followed up by JTTF and that the STIC is aware of the task forces' investigations. In addition, the STIC includes an infrastructure security awareness program that links analysts with the security chiefs of major corporations in the state, offering an effective information sharing pathway among state and federal officials and the private sector.

The STIC operates three shifts 24/7 and allow for one half hour overlap on each shift for shift change briefing. Each analyst known as Terrorism Research Specialist receives a minimum of 150 hours of training. This instruction consist of 61 hours of database training, 69 hours of classroom and practical training and 20 hours of in-service which consist of specialized topics. The STIC utilizes several state agency databases for gathering information in addition to private such as Lexis-Nexis. They have access to LEO; Law Enforcement Online, which is maintained by the FBI and access to Interpol. The scope of the STIC intelligence operations is tactical intelligence support. Law enforcement agencies can request information directly from the field. For request from the field with an ongoing law enforcement activity, the STIC attempts to within a 15

minute timeframe, check their principle intelligence database and the Chicago law enforcement automated directives and their online reports database as well as place phone calls to the El Paso Intelligence Center (EPIC) where several federal databases are checked for information regarding a specific individual. Additional queries are made through the FBI Chicago and/or Springfield office.

The information is captured on an incoming data collection form that later serves as the principle reporting format for dissemination to the requester, and becomes the foundation for the in-house intelligence file. Field request take top priority over additional STIC intelligence activities and the goal is to provide the requestor with initial information to either confirm or deny a known terrorism nexus. Upon completion of the 15-minute run-up period, routine intelligence follow-up and additional research occurs and ultimately leads to an entry into the STIC's main database.

The STIC also receives non-urgent requests from various law enforcement and homeland security entities. This includes simple requests for information (RFIs) through the JRIES system, a nationwide internet message system managed by the Department of Defense and Department of Homeland Security that is being implemented in all 50 states. These calls are process similarly, but do not demand the quick turn around as a field request.

The STIC also provides strategic intelligence support. The support functions are divided into three primary functions: (1) Groups/Methods/Targets; each analyst is assigned a certain number of domestic/international terrorist groups; (2) terrorism methodologies and (3) infrastructure targets to continually monitor, collect intelligence on and assess. This effort leads to formal threat and vulnerability assessments; Special Projects and Data Fusion. The fusion process is based on a 24 hour period. Currently the STIC captures, analyzes, documents and stores data from a variety of sources to include: incoming intelligence postings from other agencies(between 30 and 40 each day), media news reports, official bulletins/alerts/ be on the lookout (BOLOS) (i.e., FBI weekly bulletin), requests and/or incident reports forwarded directly to STIC, JRIES postings, and other known threat activity. This information is then noted directly on the three shift reports done throughout the 24 hour cycle. Based on the type/relevance of the incoming

information, further intelligence analysis may occur. Notable information is then presented and disseminated on both the daily intelligence notes and the internal daily command briefing. Other periodic incident analysis and/or reporting occur as required.

The other side of information management is information sharing. One of the principle missions of STIC is to serve as an information clearinghouse or central repository for all terrorism-related information that comes through the center. The STIC accomplishes this by utilizing a series of internal computer-networked files categorized as administrative, groups (domestic and international), methods, targets (infrastructure), threats (both suspicious incidents with a possible terrorism nexus, and threats to public officials for the Executive Protection Unit), requests, research, STIC intelligence products (reports, alerts, summaries, BOLO's, etc.), and mapping. All intelligence work done by the STIC is maintained in one of these electronic files, and all qualified intelligence is entered into the STIC database.

In addition, the STIC uses two secure Web pages within the Illinois Technology Office (ITO) website at www.ito.state.il.us. Law enforcement officials are granted access to the STIC site, which is a repository of law enforcement sensitive information. Civilian corporate security and consequence management entities are granted access to the shared zone site. The STIC also publishes via email distribution a daily intelligence notes for law enforcement and homeland security organizations. For internal command recipients, the STIC compiles a daily command briefing which features data fusion over a 24 hour period. The STIC also shares all request information with either the FBI Chicago or Springfield JTTF, depending on jurisdiction boundaries. Information is also sent through the Illinois Wireless Information Network (IWIN) to officers in the field.

Information collection is governed by 28 CFR Part 23 and more or less underlies all activities of the fusion center. Information that is terrorism related is maintained by the center. If a review of information determines that additional investigation is warranted, officials will begin documenting the use of that information, as required by regulation. The files are purged every 24 months, although information relating to ongoing investigations is retained.

C. INTEGRATING STRATEGIES

Administration and congressional efforts to reorganize national security intelligence have focused mainly on reducing barriers to sharing information among federal agencies, improving federal information technology capabilities, coordinating analysis of federal and local law enforcement and intelligence data, and supporting state and local emergency communication. Around the country, newly expanded joint terrorism task forces bring together federal and local law enforcement officials. Terrorism investigators more easily combine law enforcement and intelligence data as permitted by the USA PATRIOT Act, which Congress passed soon after the terrorist attacks. Federal airport security officers conduct more rigorous screening of passengers under the terms of the Aviation and Transportation Security Act, enacted two months after the attacks. The Department of Homeland Security, charged with coordinating domestic intelligence gathering and information sharing, has begun collecting data about vulnerabilities in the nation's critical infrastructure. A new National Counter Terrorism Center, under the supervision of the director of central intelligence, is in charge of synthesizing counterterrorism intelligence from all sources.

Concerns have arisen about conflicts with government openness, especially when secrecy has been expanded without public debate. Many of these actions could be considered as emergency measures, extraordinary steps to counter extraordinary threats. They represent important building blocks for a new generation of intelligence policy. More security issues that affect openness and privacy will be decided in the future. The administration will determine if additional rules are needed to shield sensitive but unclassified information from public view, which might include scientific research, law enforcement records, or infrastructure vulnerability reports. Policymakers have to define policies and procedures for information sharing.

Defending against terrorism threats will require policymakers to replace the formal, hierarchical intelligence structure with a horizontal, cooperative, and fluid architecture that gets information from those who have it to those who need it through the development of virtual communities of information sources, analysts, and users. Hard-wiring intelligence relationships when actors, methods, and targets are uncertain impair our ability to adapt to changing threats and vulnerabilities.

Advances in information technology can facilitate this transformation. Internet and teleconferencing technologies allow virtual communities to gather and share information in real time. Government officials should spend more time setting priorities, coordinating communication, supplying technical assistance, and assuring data quality. Collecting more information from more sources will require more analytical capability to prevent information overload. The first step in designing an intelligence system to fight terrorism while protecting openness and privacy is to understand what information is needed to support each homeland security challenge. For example, to protect America's borders, we need more complete information about people and goods entering the country. To detect potential terrorist threats within the United States, we need to enhance traditional investigative techniques by cross-referencing databases such as airline reservation records, phone logs, and credit histories with government law enforcement, immigration, and intelligence information. To protect critical infrastructure in areas such as agriculture, food, water, public health, emergency services, telecommunications, energy, transportation, banking, and finance, we need to map vulnerabilities against capabilities of potential terrorists, people who have access to those infrastructures, and the means available to carry out effective attacks. To respond to emergencies, we need two-way communication in real time between first responders and other officials about the extent and nature of the attack, the resources available to respond, and the risk of further terrorist action.

To effectively perform the necessary functions to be successful in completing the previously described tasks, capabilities need to be integrated. Analysts must be able to access many different data bases in order to gather information necessary to connect the dots. There are currently thousands of public safety agencies that operate with their own records management systems (RMSs) and do not have the ability to access another agency's data base. Data needs to not only be accessible, but also must be readable. How can different systems make sense out of the data? There must be a common language so that data can be interpreted. Chapter IV will look at the business requirements necessary in order to put such an integrated system together. The basic fundamentals of developing an information sharing network will be addressed and how a

statewide fusion center can become integrated with a major urban area terrorism early warning system. Without the proper technological and business requirements in place an integrated network is not possible.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INFORMATION SHARING ENTERPRISE

Preventing a terrorist attack requires that Federal, State, local and private sector entities have an effective information sharing and collaboration capability to ensure that they can seamlessly collect, process, analyze and disseminate information regarding threats, vulnerabilities and consequences in support of prevention, response and consequence management efforts.[43] Currently in Wisconsin, there are many public safety agencies operating on different systems. The difference in data structures and the lack of interoperability makes it nearly impossible to effectively share information. A major concern lies within licensing agreements that use off the shelf software products that simply are incompatible with one another. This causes a significant hindrance to information sharing.[44] The terrorist attack of 9/11 has clearly spelled out the need for all public safety agencies to correct the inadequacies and barriers that impede information sharing, so that future tragedies could be prevented. States need to put a system in place using available technology that will allow different agencies to access and disseminate information.

During a February 2003 speech, President Bush exemplified the importance of information sharing so that those working on the front line can prevent terrorism.[45] Information sharing is the process by which raw data are collected and disseminated among relevant agencies or individuals. Information sharing helps inform public safety officials of the terrorist threats they face so that they can take the appropriate measures to address those threats. Jurisdictions can employ local law enforcement agencies, fusion centers, or information sharing networks as mechanisms or organizational structures to share terrorism-related information.

---

[43] Wirtz and Johnson, *Strategic Intelligence*, 2.

[44] Mickey McCarter, "Info-sharing Evangelists," *HS Today*, September 2005, 12.

[45] Criminal Intelligence Coordinating Council, "National Criminal Intelligence Sharing Plan," Bureau of Justice Assistance, June 2005, http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf. (accessed September 26, 2005).

A. GATEWAY

An information sharing network is a structure for directly linking together public safety agencies and entities to facilitate the flow of information and foster cooperation among them. In an information sharing network, public safety agencies directly share terrorism-related information with each other. Officials from these agencies act as nodes within the network, transmitting terrorism-related information from their own agency to local police and to other agencies for which this information would be relevant. In an information sharing network, law enforcement agencies and fusion centers do not serve as the single, centralized hubs for information management. However, they still play a vital role as nodes that are capable of producing and disseminating analyzed intelligence throughout the network.

Justice systems are best integrated when users access the data where they reside, in a decentralized framework with a common architecture that connects legacy systems, to speed deployment and reduce associated time and costs. In an integrated system, authorized users can manipulate data and create a meaningful profile of an individual or situation based on information from law enforcement agencies, the courts, prisons, drivers' licenses, parole officers, prosecutors, public defenders and so forth. Criminal incidents, sentencing orders and citations can be filed, read and accessed by relevant parties within one architecture. Mobile access to databases can provide relatively accurate assessments of crime and criminal locations; quick access to prior criminal records in neighboring counties, cities or states; and essentially the ability to create a holistic picture of a criminal or event within minutes.

The challenge for Wisconsin is to integrate the major information providers (State Agencies, Federal Agencies and Local Records Management Systems or RMSs) in a way that does not require Gateway users to repeatedly search or query each source looking for information. The concept of creating a justice information sharing system is essential in solving the problem. In the State of Wisconsin, the major criminal justice information providers are:

- The Department of Transportation (DOT) provides information on vehicles and citations.
- The Health Alert Network(HAN) is a gateway to public health information

- The Consolidated Court Automation Program (CCAP) provides information from the courts
- Time provides Wisconsin criminal histories and links to Federal Agencies
- Protect provides information from the District Attorneys
- Corrections are in the process of acquiring an RMS system.
- Local RMSs provide information about Law Enforcement activity at the local level.
- The Department of justice hot files and criminal history repository.

Integration of these data sources relying only on a query/response approach is difficult or impossible, because data sources are poorly organized offering hundreds or thousands of data fields of potential interest and sequential querying of each data provider is time consuming and feasible only in high profile cases.

Using the Global Justice eXtensible Markup Language Data Model, (GJXML) various agencies would be able to obtain valuable information. This technology would clearly improve access to justice information across boundaries. Wisconsin information sharing would incorporate a statewide implementation of GJXDM.

The GJXDM provides multiple ways to describe relationships between objects, such as a person who owns a vehicle, a person who has a residence, a person or organization has contact information, etc. It is designed to be used as a model for the exchange of information. GJXML allows disparate organizations to talk seamlessly without having to understand each others internal systems. This technology describes how data for a certain type of exchange is formatted using schemas; xml files detailing the types of data that can be used and how it must be structured.[46] Figure II shows the traditional point to point model where several different systems are mapping repeatedly in order to obtain data. The canonical standard approach shows a central hub that multiple users can access to obtain information and data.

[46] Office of Justice Programs, "Implementing Xml for Maximum Interoperability," *U.S. Department of Homeland Security*, 2005, www.ojp.gov/ (accessed September 6, 2005).

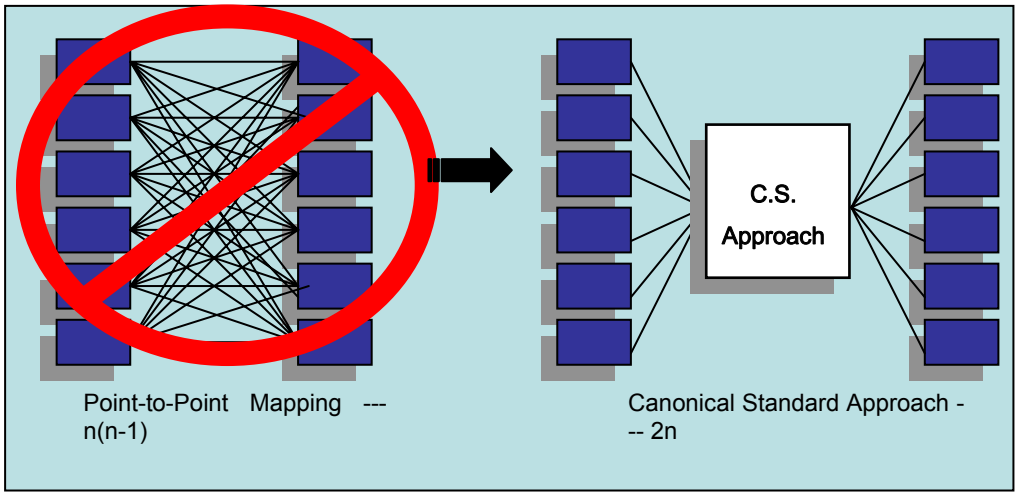


Figure 2. Communication Exchange Model

The GJXML model is based on a common language that acts as a catalyst in defining common terms between disparate systems. The data dictionary is the data model's underpinning structure. It is, in effect, a spreadsheet containing identification of data elements, and the meanings or definitions of those data elements, all of which are unique. The data model builds relationships between the data elements, and the result, in simple terms, is that disparate systems connect via the unique identifiers.[47] Much of the data shared between justice and public safety agencies, or even justice and transportation agencies, is similar, so each organization needs to define and represent those elements in the same manner for interoperability to take place, otherwise fragmentation can occur. In addition, the federal government has initiated a national data dictionary and national reference model in the form of an XML schema that can be integrated with state and local systems too.[48]

Information sharing would be designed to connect information seekers in the criminal justice system with the major information provides (Law Enforcement, District Attorneys, The Courts and Corrections) using Web Services(WS) and WS – Security running over the State of Wisconsin Enterprise Security Systems (ESS), Enterprise Services Bus (ESB) and the Enterprise Directory (EDIR).

[47] Jim McKay, "XMLout of the Shadows," *Government Technology* (June 2005): 18.

[48] Paul Embley, "Information Technology Standards," *Police Chief* (June 2004): 37.

B. FUNDAMENTALS USED IN DEVELOPMENT

The Wisconsin version of the Justice XML Reference Model would use three broad functional categories: (1) Federated Directories; There are currently multiple directories throughout law enforcement in the State of Wisconsin. A federated directory structure allows these multiple directories to be viewed as if they were one directory. In a Web services environment, federated directories can be implemented as a Web service where each organization provides a Web service that identifies and authenticates its users. The service would also identify the user's role within the organization; (2) integration servers, to integrate the local RMS systems; there is a need for software that enables one application to communicate with another on an ongoing basis. The foundation of an integration server is a message transport system; (3) Web Portal; The Web portal is a site that provides a variety of services include searching, news, directories, email, discussion groups, document repositories, data repositories, link repositories and publish/subscribe services.

The World Wide Web is more and more used for application to application communication. The programmatic interfaces made available are referred to as Web services. Web services provide a standard means of interoperating between different software applications, running on a variety of platforms and/or frameworks. Web services are characterized by their great interoperability and extensibility thanks to the use of XML, and they can then be combined in a loosely coupled way in order to achieve complex operations. Programs providing simple services can interact with each other in order to deliver sophisticated added-value services.

The Enterprise Services Bus (ESB) will also play a primary role in information sharing and interoperability. ESB is open-standards-based messaging middleware that provides secure interoperability among enterprise applications via extensible markup language (XML), Web-services interfaces and standardized rules-based routing of documents. Because sharing data through ESB doesn't depend on the data format, application and data integration is much easier to achieve. The intention is that the ESB would support a secure gateway through which hundreds of state and local law enforcement officials could log on to the system and thus be able to share vital information with one another. The key advantages of an ESB are; they are a faster and

cheaper accommodation of existing systems, they have increased flexibility and are easier to change as technology changes, they are standards based and they have scales from point solutions to enterprise wide deployment.[49]

It is clear that there will be a high level of dependency on the information systems built to support the activities of information sharing. Compromise of these systems either in terms of loss or inaccuracy of information or unauthorized individuals gaining access to it can be extremely costly to the enterprise. Security breaches can occur; therefore the system must be protected.

Security of the enterprise protects it from unauthorized attempts to access information or interfere with its operation. It is concerned with: (1) confidentiality; that information is disclosed only to users authorized to use it; (2) integrity; that information is modified only by users who have the right to do so and only in authorized ways. Information should only be transferred between intended users an in intended ways; (3) accountability, users should be accountable for their security relevant actions. A particular case of this is non-repudiation, where responsibility for an action cannot be denied; (4) Availability; use of the system cannot be maliciously denied to authorized users.[50]

Privacy is also a part of the integrity and security of an information sharing enterprise. Therefore, it is imperative that any information sharing enterprise incorporate a "privacy Policy". With all this new technology come concerns by the public over the use, or potential misuse of personal information contained within these systems. As agencies begin to take advantage of information sharing and the technology that allows them to do so, their responsibility for assuring proper use and dissemination of this information is paramount.[51] The administrators of such a system must have a process in place the captures the essence of privacy. Upon adopting a statement of purpose the policy should consider at a minimum the following;

---

[49] William Welsh, "Wisconsin Rides Enterprise Bus to Savings," *Washington Technology*, July 5, 2004, http://www.washingtontechnology.com// (accessed September 2, 2005).

[50] Lee Rech, "Patch Management," *IT Security Magazine* (March 2005): 7.

[51] Paul F. Kendall, *Justice Information Privacy Guideline* (Washington D.C.: National Criminal Justice Association, September 2002), 13-14, NCJA.

- What is the purpose of the information sharing system?
- Do information collection practices mirror the system's purpose?
- What are the goals trying to achieve through interagency information sharing?
- Are there limits to interagency sharing or access provided by jurisdictional laws or guidelines?
- What is the standard for determining accuracy of data and modification?
- In an integrated system, who is ultimately responsible for data quality?

These are just some of the questions that should be answered to ensure the security and integrity of information sharing enterprise systems.[52]

There are several fundamental principles that guide the development and implementation of an information sharing enterprise. Technical solutions must be driven by business requirements. Information must be captured at the originating point rather than reconstructed later. In addition, information is only captured once and should be reused, rather than recaptured when needed again. Justice organizations within the enterprise should have the right to design, operate and maintain systems to meet their own operational requirements. As with any other network participants must meet agreed upon data, communication, security requirements and standards in order to participate.

Security and privacy must be priorities in the development of integrated justice capabilities and in the determination of standards. As indicated earlier, there must be a privacy policy adopted.[53] Due to the singular consequences of decision making throughout the justice enterprise, establishing and confirming the positive identity of the record subject is crucial.

[52] Kendall, *Justice Information Privacy Guideline*, 13-14.

[53] National Association of State Chief Informational Officers, "Concept for Operations for Integrated Justice Information Sharing," http://axle.doit.wisc.edu/~gwp/WIJIS/ConOps2003.pdf. (accessed September 25, 2005).

C. SYSTEM TECHNOLOGY

There are several operating requirements for integrated justice information sharing that have significant implications for infrastructure development and statewide IT architecture.

Operational requirements

- Ability to query and retrieve information from relevant information systems throughout the justice system, and other relevant governmental agencies, without prior specific knowledge of the detailed structure of these systems.
- Ability to electronically send/transmit information from operational information systems in one agency/jurisdiction for inclusion in another (recipient) information system.
- Ability to request information from one system and incorporate it into another system without human intervention.
- Ability to be notified of critical events, actions and transactions on a case, person or event.
- Ability to trigger events and other actions in other systems based on actions taken in operational justice information systems.
- Ability to transmit electronic documents between organizations, including tagged data elements.
- Ability to ascertain or confirm the identity of an individual and link identity to documents, decisions and other official actions.
- Ability to determine the current legal status of an individual.
- Ability to manage and process the collection and distribution of fines, fees, costs, restitution, assessments, and other types of monetary accounts across organizational boundaries.
- Ability to discover agencies which have information concerning a specified individual (raises questions concerning need for centralized indices or search engines operating against "exposed" portions of criminal justice databases)
- Ability to discover the information needed to address a message to the criminal justice agency having jurisdiction in a specific geographic locale.[54]

These universal operating requirements for integrated justice information sharing are broadly applicable and representative of integrated justice initiatives nationally. The

[54] National Association of State Chief Informational Officers, Concept for Operations."

list should not be viewed as all inclusive, but should be a thorough representation of what requirements are commonly incorporated in justice sharing initiatives.

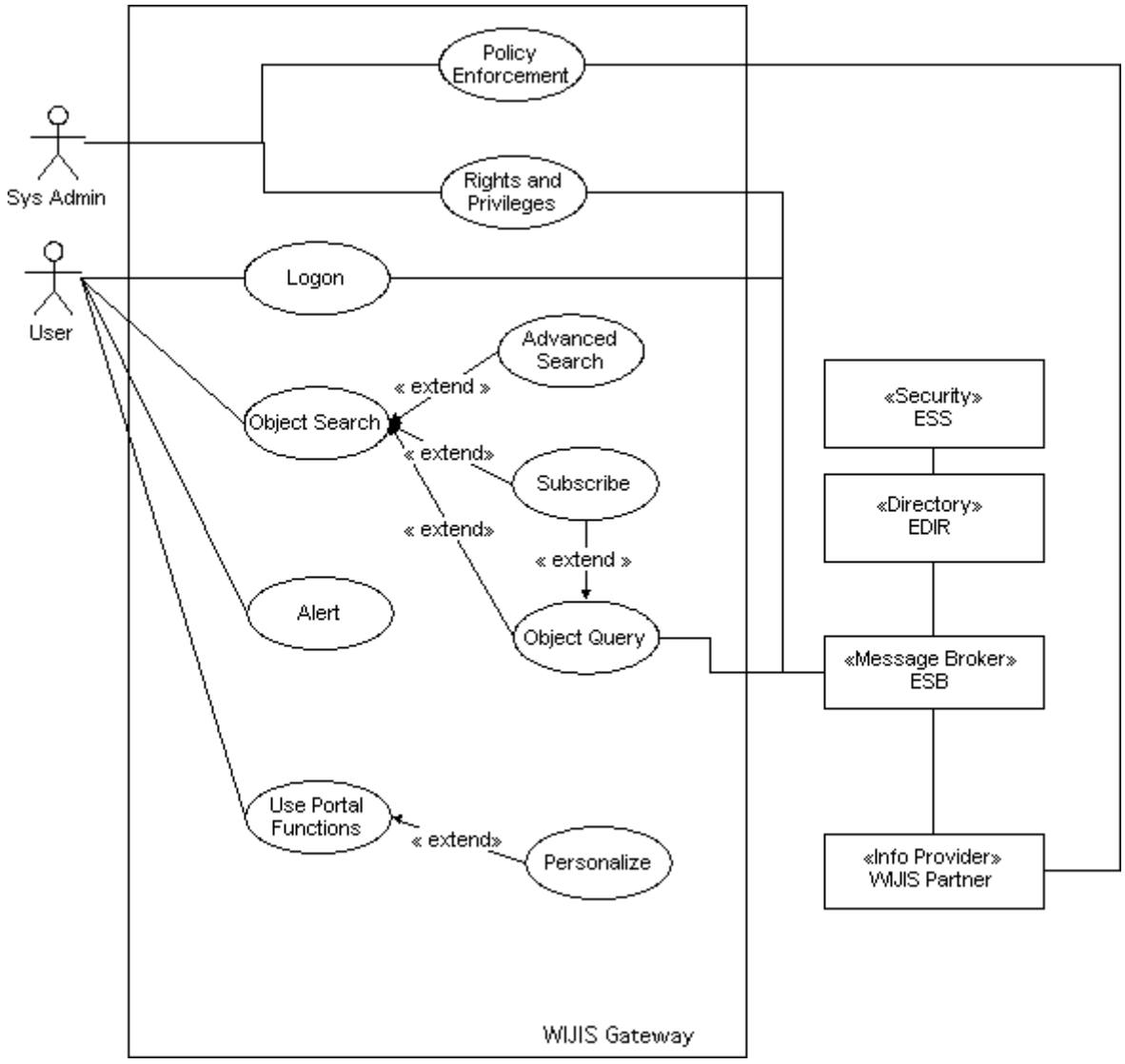


Figure 3. WIJIS Gateway

The above diagram is modeled after the Wisconsin justice information-sharing concept. It shows administrative users establishing policies, rights, and privileges. The gateway users are searching the information sharing GJXML object index, querying into

information sharing partner systems for detailed information. The user than subscribes to content updates on the information sharing GJXML objects of interest, using extended portal functions.

The efficient sharing of data among justice entities is at the very heart of modern public safety and law enforcement. It is the essential core of preventing another terrorist attack on our homeland. The technology is available through the use of GJXML, Web Services and the use of Enterprise Security Buses. It is imperative that each state moves forward with an information sharing model that adopts the national requirements so that vital information can be shared by all users.

Information sharing should extend beyond just law enforcement to all public safety agencies. The administrators of an information sharing enterprise must work with leaders from with the public safety community incorporating the necessary requirements to maintain a beneficial enterprise. The information gateway should be open to agency participation regardless of agency size, records management vendor or access to the enterprise regardless of whether they choose to share information with the Gateway. The Gateway should be built on open standards that allow for the extraction of data from any source. The Gateway should adopt the global justice reference model to ensure participation in a nationwide system of systems network and it should ensure data providers maintain control over data being shared.

The long term goals should be the prevention of terrorism, protect citizen privacy, provide real time access to data, maintain the security of the enterprise and allow access form wireless devices.

V. POLICY ANALYSIS/CONCLUSION

Previous case studies have suggested options available to Wisconsin for managing information flow and the sharing of information to prevent terrorism. These alternatives ranged from creating a single TEW in Milwaukee, to creating one state fusion center or creating both and in doing so, create a statewide information sharing network. This broad menu of policy choices suggests the need for a structured process for determining which alternative would be most preferred for addressing the existing information sharing need in Wisconsin.

The approach in this thesis is to involve the systematic weighing of benefits and drawbacks of each of the alternatives according to a set of selected criteria. These criteria will serve as measurement tools that will collectively account for all of the issues and considerations anticipated to impact the feasibility of a policy's implementation and the achievement of the policy's intended outcomes. The different criteria used to evaluate each alternative will be assigned varying levels of importance and determine the final outcome.

Seven basic criteria will be used to assess the efficacy of each alternative. The analysis will take into account both practical and evaluative criteria in selecting the preferred policy alternative. The criteria selected are as follows:

1. Efficiency
2. Information flow
3. Jurisdictional authority
4. Sustainability
5. Political and legal feasibility
6. Trust/Relationships
7. Administration

The Efficiency (Benefit to Cost Ratio) of a proposed policy measures the extent to which a policy maximizes the net benefits of all individuals in the market system, including both producers and consumers. The efficiency criterion assesses the extent to which the alternative achieves the policy objective relative to the cost of implementation

as compared to other potential options. Alternatives that rate higher on measures of efficiency would be deemed more cost-effective than other competing alternatives. The issue of sustainability refers to the potential for a given policy to sustain its beneficial impact beyond the scope of the immediate intervention. More specifically, the question of sustainability asks whether the future social or economic environment will continue to reap the benefits of a policy once that policy has ended. Sustainability is of special concern when the public policy under scrutiny must design a way to become self sustaining within a two year period.

A major practical concern involving the future promise of a given policy is the extent to which the policy receives political support from key decision-makers. Even policies with clearly demonstrated benefits might fail to be adopted in the face of strong political opposition. The political climate functions as a major policy constraint that will strongly influence the feasibility of implementing a given alternative. In addition to political feasibility, existing legal mandates governing information sharing and intelligence fusion may serve as constraints to proposed policies. For example, Minnesota statutes do not allow for the maintaining of and/or housing of intelligence.

A measure of jurisdictional authority refers to the extent to which the ability to implement the various policy components falls within the realm of authority of the entity. The extent of jurisdictional authority directly dictates the types of strategies and activities that the governing agency can accomplish and to what extent they can outreach to consumers.

Trust and relationships focus on working in a collaborative effort through a multi-jurisdictional and multi-disciplined approach. Agencies come together for the greater good and work side by side with one another. This allows people to build relationships through trust. The cohesiveness of a diversified group that relies on one another to share information is fostered. A new paradigm of need to share begins to form and relationships are strengthened in the process.

Administrative criteria focuses on the relative ease of implementation and cost associated with administering a program or policy. Policies that rate highly in satisfying evaluative criteria, for example, may be cost-prohibitive to implement or may not be

realistic in terms of the administrative effort required to carry out the policy functions effectively. For this reason, policies that are designed to operate within an existing administrative structure or at low administrative cost would be more practically feasible than those requiring major organizational restructuring or high levels of spending.

A. ANALYSIS CRITERIA

This set of selected criteria provides the necessary tools for determining the most preferred policy option with regard to both outcome and feasibility of implementation; however, each of the criteria presented may differ with regard to its relative importance to the outcome or process. In other words, one criteria or set of criteria may represent a more critical determinant of the policy's potential value than another, based on some value judgment. For this reason, it is useful to assign relative weights to each of the criteria in order to establish the degree of influence that the criteria will be allowed to exert over the final policy decision. These weights, assigned as fractions adding to "1" across the seven criteria, are listed below:

$$20\ (EF) + .20(IF) + .20(J)\ .15(S) + .15\ (PL) + .05\ (T/R) + .05\ (A)$$

From the seven criteria, the three assigned the highest degree of influence (weighting =.20) for the policy outcome, was efficiency, information flow and jurisdiction. The efficiency criteria is viewed as one of the most critical to the policy process because it captures the potential for the alternative to maximize net benefits to those impacted in the system. The stronger relative rating assigned to this criteria allows for the prioritization of maximally efficient approaches to accomplishing policy goals, which might be implemented in an "ideal" world unconstrained by practical limitations, such as political environment or administrative concerns. The second criteria, viewed equally important, is one of the direct outcomes of the policy, information flow. The stronger the potential to reduce stovepipping and share information with others the more ideal the outcome. The third criteria viewed as a top tier is jurisdiction. The larger the jurisdiction and the more consumers they serve the stronger the rating.

The second tier in terms of influence was comprised of both the sustainability and the political and legal feasibility criteria (weighting = 0.15). Sustainability received a

slightly lower weighting based on the argument that it would only be central to the policy process in the face of strong pressure to eliminate the legislation that finances preparedness program activities through Grants & Training (G&T). Within G&T's current policy environment, funding to support the information sharing program are assessed yearly and each program is a two year program. In addition, the current trend does not suggest any immediate demand to halt funding legislation. Nevertheless, it has been assigned a high relative rating in order to reflect the philosophy of the G&T preparedness program, which emphasizes the development of sustainable funding through other means.

Political and legal feasibility also received a high weight indicating the importance of political support to successful adoption and implementation of policies. Without the support of the Governor's office and the state legislature, future sustainability would clearly be an uphill battle. However, having the support of key players is vital to the long term success of the policy.

The third tier is composed of the remaining two of the practical criteria for assessing policy preferences, each assigned an equal weighting of 0.05. This tier includes measures of trust and building relationships and administrative burden. The criteria were prioritized slightly lower than the practical criteria of sustainability and political and legal feasibility, and are considered to be both desirable and necessary for successful implementation. Trust and building collaborative relationships is essential for information sharing to succeed.

B. ANALYSIS METHODOLOGY

The approach for assessing the optimal policy alternative, or package of policy options, involves the development of a simple process for evaluating each option according to a uniform set of criteria. The method of evaluating the alternatives involves the creation of both a qualitative and quantitative alternative criterion (outcomes) matrix, which together provides an assessment of how each policy option fares when evaluated

against each of the designated criteria. Each alternative-criterion matrix is structured as a table of cells with alternatives listed as row headings and individual criteria listed as column headings.

The qualitative version of the matrix provides a brief description of the projected outcome, or likely consequence of each policy, with regard to a given criteria, allowing for a straightforward comparison of advantages and drawbacks across alternatives. This qualitative discussion of each alternative will be used as the basis for creating a quantitative matrix, where a numeric rating is assigned to each cell in the table as a quantitative measure how the alternative fares on each criterion. This quantitative measure will be based on a four-point scale with point values ranging from Very Strong, indicating the policy is optimal in terms of that specific criterion, to Very Weak, indicating the policy fails to satisfy the criteria in any aspect. The following table provides a key for interpreting the range of ratings for each proposed criteria.

Key for Interpreting Criteria Rating Scale

Interpretation of Ratings

1- Very Strong

2- Strong

3- Weak

4- Very Weak

0.20 (EF) + 0.20(IF) + 0.20(J) 0.15(S) + 0.15 (PL) + 0.05 (T/R) + 0.05 (A)

Interpretation of Ratings – TEW Policy Option				
Criteria	**1. Very Strong**	**2. Strong**	**3. Weak**	**4. Very Weak**
Efficiency		X		
Information flow			X	
Jurisdictional Authority			X	

Sustainability		X		
Political & Legal Feasibility		X		
Building Trust			X	
Administration		X		

Table 1. TEW Policy Option

TEW Policy Option = 0.40 + 0.60 + 0.60 + 0.30 + 0.30 + 0.15 + 0.10 = **2.45**

0.20 (EF) + 0.20(IF) + 0.20(J) 0.15(S) + 0.15 (PL) + 0.05 (T/R) + 0.05 (A)

Interpretation of Ratings – Fusion Center Policy Option				
Criteria	**1. Very Strong**	**2. Strong**	**3. Weak**	**4. Very Weak**
Efficiency		X		
Information flow		X		
Jurisdictional Authority		X		
Sustainability		X		
Political & Legal Feasibility	X			
Building Trust		X		
Administration		X		

Table 2. Fusion Center Policy Option

Fusion Center Policy Option = 0.40 + 0.40 + 0.40 + 0.30 + 0.15 + 0.10 + 0.10 = **1.85**

0.20 (EF) + 0.20(IF) + 0.20(J) 0.15(S) + 0.15 (PL) + 0.05 (T/R) + 0.05 (A)

Interpretation of Ratings – Fusion Center & TEW Network Policy Option				
Criteria	**1. Very Strong**	**2. Strong**	**3. Weak**	**4. Very Weak**
Efficiency		X		
Information flow	X			
Jurisdictional Authority	X			
Sustainability		X		
Political & Legal Feasibility	X			
Building Trust	X			
Administration	X			

Table 3. Fusion Center & TEW Policy Option

Information Network Policy = 0.40 + 0.20 + 0.20 + 0.30 + 0.15 + 0.05 + 0.05 = **1.35**

C. RECOMMENDATION & CONCLUSION

The previous tables clearly show that the information-sharing network enterprise created by the implementation of a statewide intelligence fusion center in conjunction with a local TEW in the largest metropolitan area (Milwaukee) is the best policy option. The TEW in itself is weak in the areas of jurisdiction, information flow and building trust and relationships. This is primarily because the TEW although a great concept, is functional at the local level. Wisconsin has over 6 hundred law enforcement agencies and hundreds more public safety and first responder agencies. A single TEW located in Milwaukee cannot cover the entire jurisdiction of the state of Wisconsin. The state could not require the city of Milwaukee to service the entire state's needs. Even the slightest attempt would not be political conducive to those in elected office.

The TEW policy option is evaluated as weak on information flow because it can not be fluid on its own. With no state fusion center there is no concrete information flow

from the local level to the state and then into the national intelligence community. A TEW would simply work in conjunction with the federal level of government; however, there would be no state level participation in the intelligence process. A stand alone TEW cannot build trust and relationships statewide within the public safety community. Even though the TEW can accomplish nearly all goals and objectives for information sharing, it can only do so on a local level. A local TEW cannot track trends and readily gather information from throughout the rest of the state. It needs to be integrated with a statewide intelligence fusion center. The TEW concept also does not normally lend itself to hard intelligence analysis. The TEW is more of a support system and provides infrastructure assessment, red teaming and playbooks for specific response procedures during a crisis.

The state fusion center concept overall is a more thorough policy option. The statewide fusion center policy option was rated strong in every category except for political and legal feasibility where it scored very strong. In comparison with the TEW policy option, the statewide fusion center would have greater jurisdictional authority by covering the entire state. This would provide a better value to the thousands of stakeholders that will benefit firm information sharing. The information flow would be more robust because a statewide center would be directly tied into the state's entire public safety community. The direct result of these to effects would play a significant role in allowing the statewide center to foster and build more trust with local jurisdictions which will then lead to more information sharing. The statewide fusion center was rated very strong in political feasibility because it has the support of the State Department of Justice, Homeland Security Office, Governor's Office, Department of Military Affairs and several additional entities.

Combining the two policy options into an information sharing network is by far the most compressive policy option and the overall recommendation of this thesis.

In order to proactively participate in the prevention of terrorism it is clear that Milwaukee needs a TEW, because the Milwaukee urban area is home to the state's most critical infrastructure and provides a greater percentage of overall intelligence. The State needs to work with the City of Milwaukee in a collaborative effort to leverage resources

to provide workable intelligence information to users throughout the State. Milwaukee, a major urban area as defined by the Urban Area Security Initiative should move forward with a TEW and upon completion should be interlinked with the state fusion process. The city of Milwaukee Police Department and Fire Department has the resources and the commitment of both chief's. Currently homeland security funding and UASI funding is available to purchase equipment and cover any start up costs. A scaled-down version of the LA TEW would be cost effective and allow for future expansion as additional funding becomes available. The combined policy option was rated very strong in every category and strong in efficiency and sustainability. In taking these two criteria together, the primary reason for the ranking is simply the start up cost of the combined policy option and sustainability of both entities are more expensive than either the TEW or stand alone fusion center policy options. Table 4 shows the yearly operating cost of the statewide fusion center. The yearly budget was constructed using the actual true cost of each category. A similar table would have to be created to capture the yearly operating cost of a TEW for Milwaukee.

Item	Number	Cost
Personnel		
Analysts	5	$ 266,455
Agents	4	$ 352,780
Operational		
Phone		$ 8,862
Postage/Shipping	4	$ 2,000
Promotional Items		$ 2,500
Computers/Software		$ 6,500
Building		
Lease	1	$ 108,612
Alarm Monitoring		$ 1,100
Satellite News Feeds	1	$ 1,300

Miscellaneous		$31,500
TOTAL PER YEAR		**$ 781,609**

Table 4. Wisconsin Fusion Center Annual Budget

Although it would initially begin out as a small operation, future funding would allow TEW expansion. The resources to begin operations would consist of police, fire & EMS and public health. The TEW concept is flexible and allows for expansion. Long term, the TEW will be able to provide more products for the UASI area and the support will grow causing more agencies to commit resources and/or personnel to the TEW. A governance structure would be put in place to have administrative oversight over the TEW. The group will be responsible for the operational policies of the TEW. A governance structure will create a supported environment that frames the ability for the TEW to function and operate, assign task, allocate and manage resources and develop and enforce policy. In addition, the governance structure shall ensure an equal opportunity for all participating agencies and users to have ownership in the decision making process.

The TEW concept allows for inter-agency coordination. On a national level, the intelligence community must evolve and truly become both a top down and bottom up information sharing enterprise. The local TEW feeds information into the state fusion center and the statewide fusion center pushes that information up to the National Counter Terrorism Center (NCTC). The proper dissemination of information from the federal level would provide intelligence to the state fusion center and the state will disseminate that information to the local police. Fostering a collaborative environment builds trust among participating entities, strengthens partnerships and provides individual as well as collective ownership in the mission and goals of the TEW. The purpose of collaboration is to increase capacity, communication and continuity of service while decreasing duplication.

Area public safety agencies will be encouraged to participate in the TEW and Wisconsin Statewide Intelligence Center (WSIC) Terrorism Liaison Offer (TLO) and private sector entities, the Infrastructure Liaison Officer (ILO) programs. Both programs

will ensure that the TEW and WSIC have a trained primary point of contact that can be counted on to actively work with both entities. Terrorism Liaison Officers develop and maintain critical human networks throughout the community that can provide early warning to terrorist activity. Infrastructure Liaison Officers provide the same function, only they are employed in the private sector. ILOs help build the public-private partnership within the intelligence community.

The TEW system will be more than the one-time collection of law enforcement and/or terrorism related intelligence and will allow for a constant on-going process that involves the delineation of roles and responsibilities, the creation of requirements, and the collection, blending, analysis, timely dissemination and reevaluation of critical data, information and intelligence derived from a variety of sources. A TEW will leverage information and intelligence through processes and systems to support the rapid identification of patterns and trends that may be indicative of an emerging threat condition.

Although the primary emphasis of intelligence fusion is to identify, deter and respond to terrorism related incidents, threats and risks, a fundamental benefit to the Milwaukee urban area, tribal and local entities is that it will support ongoing efforts to address non-terrorism related issues such as; allowing for better identification and forecast of emerging crime, public health and quality of life trends and supporting law enforcement proactive, risk based, community focused problem solving activities.

The WSIC state fusion center will be linked to the Milwaukee (UASI-TEW) and the Joint Terrorism Task Force (JTTF). The statewide fusion center will serve as a central hub for information sharing and directly link into the NCTC and HSOC, thus leveraging national intelligence. A strategy for sharing information nationwide is creating a network. The information sharing network is essential to preventing another terrorist attack. A process will be initiated that will allow for the proper dissemination of intelligence and information sharing throughout Wisconsin.

The strategy canvas is both a diagnostic and an action framework for building a compelling valued innovative approach. Its primary purpose is it captures the current state of action in the known market space. This allows you to understand where the

current system is investing time and resources and what its products, services and delivery are. The primary problems of traditional information sharing are listed below, followed by the advantages of an information sharing network and collaborative information sharing.

Traditional Approach Problems

- Stove piping
- Intelligence community culture
- Need to know
- Failure to share
- Poor information flow
- Poor relationships and reputation

Information Sharing Network Advantages

- Need to share philosophy
- Collaborative
- Information flow
- Building of trust
- Relationships
- Reputation
- Overarching jurisdictional authority

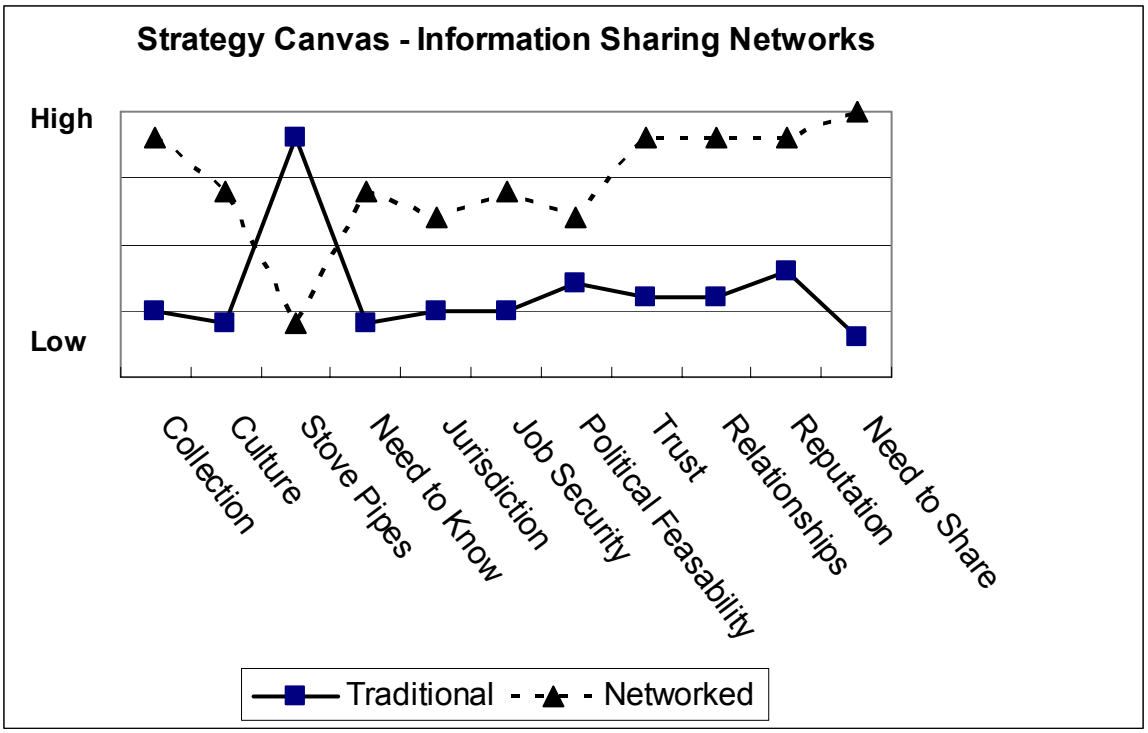
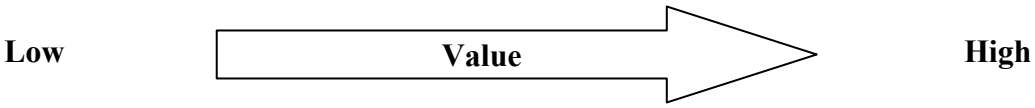


Figure 4. Traditional versus Information Sharing Networks Canvas

A comparison of the traditional versus networked method of intelligence sharing is illustrated in Figure 4. The categories of difference are as follows: collection; more enhanced via the information sharing network than traditional methods); culture (multi-agency and much improved via network compared to traditional, the friction of culture is reduced in an information sharing network); stove pipes (virtually eliminated in an information sharing network due to cultural shift from need to know to need to share attitude); need-to-know (traditional method operates strictly on need-to-know that is not conducive to the information sharing network theory, which is based on need-to-share and is thus rated much lower in intelligence sharing in the traditional method); jurisdiction; (an information sharing network covers the major urban areas and the state level. The network is than integrated into the national intelligence structure); job security (personnel in the traditional system feel they must maintain status quo to keep jobs versus personnel in the information sharing network in which networking and relationships would reduce fear of job security and thus increase perception that job security exists); Political feasibility (is enhanced in the information sharing network, there is strong

support from DHS and state & local government for information sharing and to support a methodology that can prevent another 9/11; trust (working closely together with a common goal, although from different agencies builds stronger trust factors than isolationist/elitist attitude of the traditional system thus, the mutual trust factor is greatly improved, coordination and collaboration builds this trust); relationships (relationships become stronger in a networked atmosphere, resulting in enhanced sharing, the need to share becomes evident in a collaborative environment) – an example is the JTTF, although little improvement has been made or at least has not spread nationally; reputation (within a networked sharing system it is perceived highly likely that agencies will be more forthcoming and not want to bear the brunt of the "agency" that held out in event of a scenario similar to 9/11 — cooperation will foster enhanced reputation); need-to-share (the development of an information sharing network is purely based on need-to-share intelligence, collaboration and coordination eliminating many barriers compared to the Department of Defense-based need-to-know attitude that the intelligence community operates under thus, information sharing is greatly enhanced). The strategy canvas shows the added value of an information sharing network.



Traditional Methods **Information Sharing Network**

The development and exchange of intelligence is not easy. Information sharing not only requires strong leadership; it also requires the commitment, dedication and trust of a diverse group of men and women that agree in the power of collaboration. 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, state and prevent criminal activity. TEWs embody the core of collaboration and as resources decrease, TEWs will become even more of an effective tool to maximize available resources and build trusted relationships. The fusion process should be organized and coordinated on a statewide level between the Milwaukee TEW and the statewide fusion center.

States planning to implement a statewide fusion center should learn from those states that have already set up and are operating intelligence fusion centers. A fusion center is a physical location where officials receive, process, and analyze all-source information and synthesize their analyses into intelligence products for dissemination to relevant agencies and officials. Fusion centers can also serve as primary mechanisms for information sharing at the state and local levels. Fusion center analysts process and analyze information from state and local public safety agencies. The center shares it with relevant federal, state, or local agencies. A fusion center also can process information from federal sources, determine its relevance within the state or local jurisdiction, and disseminate it as necessary.

The mission of any information sharing network should be to protect the citizens and critical infrastructures of the individual state by enhancing and coordinating counter terrorism intelligence and other investigative support efforts among local, state and federal law enforcement and public safety agencies. The goal is to prevent terrorism and related crimes and play a crucial support role in an all hazards event, thereby providing a safe environment for the citizens of that state. It is imperative to have intelligence and investigative priorities. Information sharing networks should prioritize by utilizing the following specific categories:

- Terrorism and related crimes
- Threats to critical infrastructure
- Threats to government and law enforcement officials
- Transnational organized crime
- Traditional organized crime
- Threats to special events
- Identity theft / Document fraud
- Narco terrorism
- Transportation related incidents
- Major arsons
- Weapons, alcohol, tobacco
- Hazmat/WMD related incidents
- Explosive related incidents

- International incidents with potential for local impact
- Border related crimes

As more fusion centers begin to start up operations around the U.S. we must make sure that they are fully integrated with local TEW's and the statewide fusion center is directly interconnected with the federal intelligence community. Over time, information sharing networks at the state and local level should see expansion not only in the form of space, but more importantly in the form of diversified personnel. An optimum local information sharing network in Wisconsin would have personnel from the following agencies assigned to the statewide fusion center, this list would include:

- Wisconsin State Patrol
- Milwaukee Police Department
- Madison Police Department
- Dane County Sheriff's Office
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Milwaukee Fire Department
- Madison Fire Department
- USDHS Border Patrol
- USDHS Immigration & Customs Enforcement
- Federal Bureau of Investigation
- U.S. Secret Service
- U.S. Postal inspection Service
- Wisconsin Department of Corrections
- Wisconsin Department of Public Health (DHFS)
- Wisconsin Department of Agriculture
- Wisconsin Department of Natural Resources
- Wisconsin Attorney General Office
- Wisconsin Department of Military Affairs
- USDHS Intelligence & Analysis

Wisconsin and additional states that have fusion centers or those that are in the conceptual stage for a statewide intelligence center and/or a local TEW should reach out

to the High Intensity Drug Trafficking Areas (HIDTA) and become partners in information sharing. Milwaukee, Wisconsin has a HIDTA office and they should be integrated into the information sharing network. The HIDTA program provides additional federal resources to those areas to help eliminate or reduce drug trafficking and its harmful consequences. Law enforcement organizations within HIDTAs assess drug trafficking problems and design specific initiatives to reduce or eliminate the production, manufacture, transportation, distribution and chronic use of illegal drugs and money laundering. One of the key priorities of the Program is to assess regional drug threats and facilitate coordination between federal, state and local efforts; to improve the effectiveness and efficiency of drug control efforts to reduce or eliminate the harmful impact of drug trafficking. Figure 5 shows the HIDTAs located throughout the U.S. that can be integrated into the intelligence community.[55]

Figure 5. High Intensity Drug Trafficking Areas

The Milwaukee HIDTA makes it clear in their mission statement that they apply enhanced intelligence processes, a high level of enforcement coordination, and

55 Office of National Drug Control Policy, "High Intensity Drug Trafficking Areas," http://www.whitehousedrugpolicy.gov/hidta/index.html. (accessed July 22, 2006).

prosecution too substantially and measurably reduce organized drug distribution, drug related violent crime, and money laundering, and to reduce the demand for illegal drugs within the Milwaukee HIDTA. The Milwaukee HIDTA would be a great asset to the information sharing network in Wisconsin and many other states that are in the process of creating and/or operating a fusion center and/or TEW.

Fusion centers provide a clear link between local and federal public safety agencies. This enables fusion centers to coordinate interagency information sharing more effectively than could be done with the traditional approach. Fusion centers also take an all-source, multidisciplinary approach that facilitates the collection of information from a wide range of sources and perspectives. Fusion centers can be structured differently and have different missions and some similar obstacles may have to be overcome through different methods. Fusion centers should support several general principles:

- States should identify the legal and bureaucratic obstacles to effective communications sharing and ensure their state fusion centers are designed in way that addresses those obstacles.
- States should ensure that fusion center officials are familiar with the federal privacy regulations governing the use and protection of criminal intelligence information and that center operations at a minimum, comply with those regulations.
- States should ensure that fusion centers are formalized through legislation or binding interagency agreements and that their governance structure includes representation from all participating agencies.
- States should determine early in the planning process whether the fusion center will have the authority to carry out its own investigations, play purely an analytical role, or have both functions.
- States should ensure the center integrates staff from diverse agencies, including public safety, public health, energy, transportation, technology and the state national guard. All agencies need not be a part of an intelligence fusion center, but the center should have provisions to incorporate liaisons from agencies with homeland security interest.

- States should ensure that the site selected for the fusion center is bureaucratically neutral, is designed to encourage collaboration, and can accommodate analysts from all agencies that are expected to contribute to its operations.
- Early in the process of establishing fusion centers states should identify and allocate state resources to complement federal grant money. This is essential to the long term viability of state fusion centers.

The operation of a fusion center can have several standards be put into place in many different ways to achieve the outcomes desired. However, in order to be successful the center should incorporate the following operational guidelines for the effective fusion of intelligence and information:

- Use of common terminology, definitions and lexicon by all entities involved.
- A clear understanding of the links between terrorism-related information and non-terrorism related information.
- Clearly defined intelligence and information requirements from the intelligence community that prioritize and guide planning, collection, analysis, dissemination, and reevaluation efforts.
- An all hazards, all crimes approach to defining information collection, analysis and dissemination.
- Reliance on existing information pathways and analytic processes to the extent possible.
- Clear delineation of roles, responsibilities and requirements of each level and sector of government involved in the fusion process.
- A capacity to convert information to operational intelligence.
- The use of subject matter experts in the analytical process.
- Extensive and continuous interaction with the private sector and with the public.

Intelligence fusion centers and terrorism early warning systems provide an opportunity for states and locals to break down the informational silos created by historical legal and bureaucratic impediments to information sharing. The intelligence reform efforts continuously underway at the federal level are contributing to an atmosphere that encourages information sharing. However, states must also be key leaders in this area. State and local leaders are positioned to mobilize state homeland security resources and design truly integrated information sharing networks.

Despite the federal government making intelligence analysis and information sharing a national preparedness priority, to create such an enterprise is challenging. Turf wars will continue to mark the relationship among state and federal agencies; privacy issues must be addressed; states must operate, at least for the time being with only limited national standards for the design and operation of fusion centers and TEWs; and restrictions on the use of federal homeland security funding, necessitate state funds for long term operations.

D. FUTURE RESEARCH ISSUES

Information sharing networks will continue to grow through the development of statewide fusion centers and local urban area terrorism warning systems. The success of such endeavors is currently unknown. The question becomes how can the success of these networks be measured? Future research should look at the fusion center information sharing concept and whether or not the intelligence centers put into place around the country have been successful or not and to what level have they been successful. There needs to be a consistent and systematic series of metrics that measure the success and/or failure of fusion centers. At this time it appears that nearly all jurisdictions exploring the intelligence fusion center and/or TEW concepts are not focusing on having an effective system in place that measures the outcomes and success of operating an information sharing entity. In addition, the issue of security clearances also needs to be addressed. The current military model should be studied and research conducted with stakeholder input on how to effectively solve the issue of security clearances. The current process is ineffective that is administered by the FBI and as the

lead domestic intelligence agency, it is a conflict of interest to be the collectors of intelligence and also be the approving authority for security clearances to share that information.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Borch, Frederic L. "Comparing Pearl Harbor to 9/11." *The Journal of Military History* (July 2003): 845-860.

Brennan, John. Director, Terrorist Threat Integration Center. "Our First Line of Defense for Homeland Security." In Testimony before the Committee on the Judiciary, U.S. Senate, held in Washington, DC, September 23, 2003.

Bureau of Justice Assistance. "Fusion Center Guidelines." *U.S. Department Of Justice*, July 2005. http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf. (accessed March 21, 2006).

Candiotti, Susan. "Another Hijacker Was Stopped For A Traffic Violation." *CNN*, January 9, 2002. http://edition.cnn.com/2002/US/01/09/inv.hijacker.traffic.stops (accessed October 12, 2005).

Carafano, James J. "Terrorist Intelligence Centers Need Reform Now." *The Heritage Foundation*, May 10, 2004. http://www.heritage.org/Research/HomelandDefense/em930.cfm/ (accessed November 15, 2005).

Criminal Intelligence Coordinating Council. "National Criminal Intelligence Sharing Plan." *Bureau Of Justice Assistance*, June 2005. http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf. (accessed September 26, 2005).

Embley, Paul. "Information Technology Standards." *The Police Chief*, June 2004, 37-39.

Johnson, Loch K. and James J. Wirtz. *Strategic Intelligence*. Los Angeles: Roxbury Publishing Company, 2004.

———. *Intelligence Collection*. Los Angeles: Roxbury Publishing Company, 2004.

Kendall, Paul F. *Justice Information Privacy Guideline*. Washington, D.C.: National Criminal Justice Association, September 2002.

Krikorian, Greg. "Terrorism Early Warning Group Works To Keep L.A.'s Guard Up." *Police One*, November 8, 2004. http://www.policeone.com/policeone/frontend/parser.cfm?object=News&tmpl=&operation=full_news&id=93416/ (accessed November 10, 2005).

Lipowicz, Alice. "Justice Issues Fusion Center Guidelines." *Washington Technology*, August 30, 2005. http://www.washingtontechnology.com/news/1_1_/daily_news/26893-1.html. (accessed October 26, 2005).

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington, D.C.: CQ Press, 2003.

Markel Foundation. *Creating a Trusted Information Network for Homeland Security-Second Report of the Markle Foundation Task Force.* December 2, 2003. http://www.markletaskforce.org/Report2_FullReport.pdf. (accessed September 22, 2005).

McCarter, Mickey. "Info-sharing Evangelists." *HS Today*, September 2005, 10-12.

McKay, Jim. "XML Out of the Shadows." *Government Technology*, June 2005, 18-20.

McNeil, Phyllis, Provost. *The Evolution of the U.S. Intelligence Community*. Edited by Loch K. Johnson and James J Wirtz. Los Angeles: Roxbury Publishing Company, 2004.

Modaferri, Peter A. "Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards." *The Police Chief* 72, no. 2 (February 2005): 24-28.

National Association of State and Chief Informational Officers. "Concept for Operations For Integrated Justice Information Sharing." July 2003. http://axle.doit.wisc.edu/~gwp/WIJIS/ConOps2003.pdf. (accessed September 25, 2005).

_____. "Justice Information." *Nascio*, May 2005. http://www.search.org/programs/info/jiem.asp/ (accessed November 12, 2005).

National Commission on Terrorist Attacks upon the United States. Thomas H. Kean and Lee H. Hamilton. *The 911 Commission Report*. Washington, D.C.: 2004.

Nunnally, Derrick and Linda Spice. "Evidence Found in Towers' Collapse." *JS Online*, October 11, 2004. http://www2.jsonline.com/news/metro/oct04/265866.asp/ (accessed March 18, 2006).

Office of Domestic Preparedness. "2006 Homeland Security Grant Program." December 2005. http://ojp.usdoj.gov/odp/docs.fy2006hsgp.pdf. (accessed December 29, 2005).

Office of Justice Programs. "Global Justice Information Sharing Initiative." September 2004. http://www.it.ojp.gov/topic.jsp?topic_id=8/ (accessed November 6, 2005).

———. "Guiding Principles and Strategic Vision of the Global Justice Sharing Initiative." September 14, 2004. http://www.it.ojp.gov/documents/200409_GAC_Strategic_Plan.pdf. (accessed November 16, 2005).

———. "Implementing Xml for Maximum Interoperability." *U.S. Department of Homeland Security*, 2005. htpp://www.ojp.gov/ (accessed September 6, 2005).

Office of National Drug Control Policy, "High Intensity Drug Trafficking Areas," http://www.whitehousedrugpolicy.gov/hidta/index.html. (accessed July 22, 2006).

Office of State and Local Coordination and Preparedness. "Terrorism Early Warning Group." 2005. http://www.ojp.usdoj.gov/odp/docs/TEWBrochure.pdf. (accessed November 17, 2005).

Pierce County, WA Department of Emergency Management. *Developing Threat Response Strategies and Information Systems for Local Government.* January 1, 2003. https://www.llis.dhs.gov/member/secure/getfile.cfm/TEW%20White%20Paper%2Epdf?id=9870. (accessed September 23, 2005).

President George W. Bush. "Executive Order: Strengthened Management of the Intelligence Community." August 27, 2004. http://www.whitehouse.gov/news/releases/2004/08/20040827-6.html. (accessed September 15, 2005).

Rech, Lee. "Patch Management." *IT Security*, March 2005, 6-9.

Reed, Ed and Matthew G. Devost. "Utilizing Terrorism Early Warning Groups to Meet the National Preparedness Goal." *Terrorism Research Center*, May 11, 2005. http://www.terrorism.com// (accessed March 6, 2006).

State of Illinois. "Statewide Intelligence Fusion Center." *Illinois Homeland Security*. http://www.illinoishomelandsecurity.org/ittf/terrorismreport19.htm. (accessed February 20, 2006).

Sullivan, John. "Building a TEW Network." Los Angeles, CA, 2005. Unpublished PowerPoint presentation.

Troy, Thomas F. *The Quaintness of the U.S. Intelligence Community*. Edited by Loch K. Johnson and James J. Wirtz. Los Angeles: Roxbury Publishing Company, 2004.

U.S. Department of Homeland Security. "The National Strategy for Homeland Security." The Whitehouse, July 16, 2002. http://whitehouse.gov/homeland/book/index/html/ (accessed September 4, 2005).

———. *Terrorism Early Warning Group*. 2005.

U. S. Department of Justice. "The National Criminal Intelligence Sharing Plan." October 2003. http://it.ojp.gov/documents/NCISP_Plan.pdf. (accessed February 15, 2006).

U.S. Department of State. "Fact Sheet: Bush to Create Terrorist Threat Integration Center." January 28, 2003. usinfo.state.gov/topical/pol/terror/03012806.htm. (accessed February 15, 2006).

United States v. Truong Dinh Hung, 629 F.2d 908, 913-14 (4th Cir. 1980).

Welsh, William. "Fusion Forward." *Washington Technology*, February 21, 2005. http://www.washingtontechnology.com/news/20_4/statelocal/25616-1.html. (accessed November 30, 2005).

_____. "Wisconsin Rides Enterprise Bus to Savings." *Washington Technology*, July 5, 2004, http://www.washingtontechnology.com// (accessed September 2, 2005).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Robert Simeral
   Naval Postgraduate School
   Center for Homeland Security & Defense
   Monterey, California

4. Nadav Morag
   Naval Postgraduate School
   Center for Homeland Security & Defense
   Monterey, California